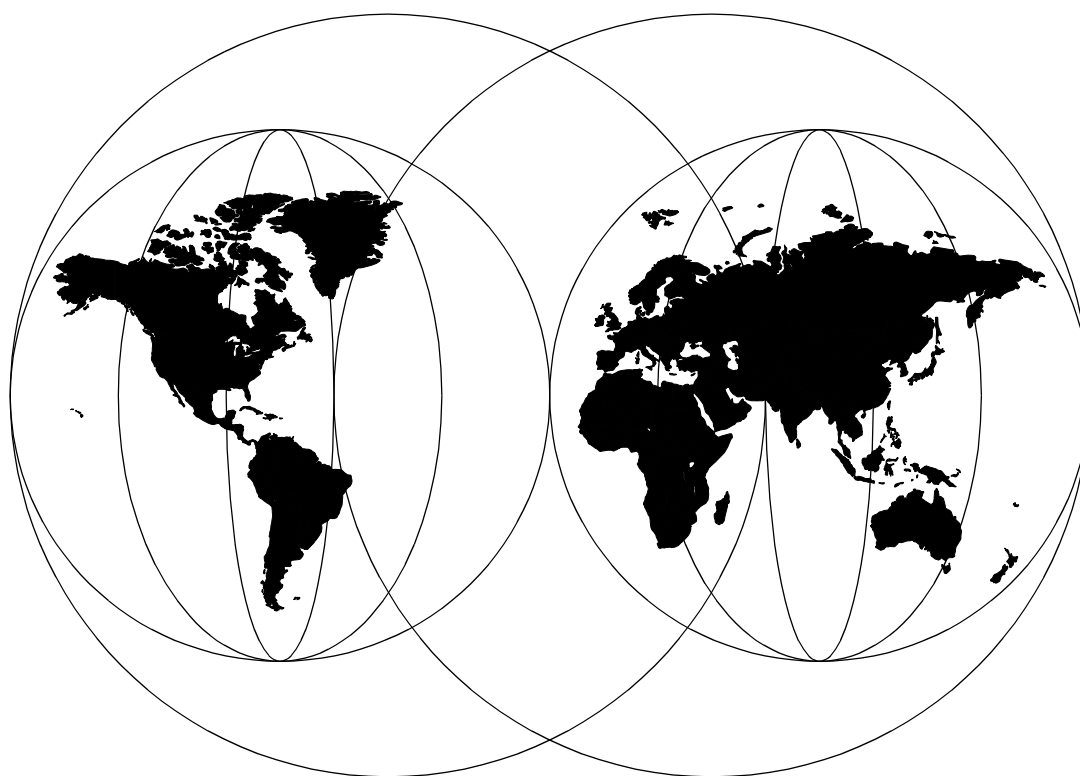




# **IBM Network Station Manager Release 3 Guide for Windows NT**

*Claude Bechard*



**International Technical Support Organization**

<http://www.redbooks.ibm.com>





International Technical Support Organization

SG24-5221-00

**IBM Network Station Manager Release 3**

**Guide for Windows NT**

November 1998

**Take Note!**

Before using this information and the product it supports, be sure to read the general information in Appendix C, "Special Notices" on page 421.

**First Edition (November 1998)**

This edition applies to Release 3 of the IBM Network Station Manager for use with Windows NT.

Comments may be addressed to:  
IBM Corporation, International Technical Support Organization  
Dept. HZ8 Building 678  
P.O. Box 12195  
Research Triangle Park, NC 27709-2195

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 1998. 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

<b>Figures</b> .....	xi
<b>Tables</b> .....	xix
<b>Preface</b> .....	xxi
<b>Chapter 1. Overview</b> .....	1
1.1 What Is New in Release 3? .....	1
1.2 Release 3.02 Additional Functions .....	3
1.2.1 Touch Screen Support .....	3
1.2.2 Multiple Serial Port Adapter .....	4
1.2.3 Flash Boot Support .....	6
1.2.4 Series 1000 Type II PCMCIA Feature .....	7
1.3 IBM Network Station Overview .....	7
1.3.1 What Is an IBM Network Station? .....	8
1.3.2 What Software Does It Run? .....	11
1.3.3 How Does It Work? .....	12
1.3.4 Server Software .....	16
<b>Chapter 2. Installation</b> .....	19
2.1 Obtaining the Code .....	19
2.2 Differences with the Installation Process of Previous Releases .....	20
2.3 Prerequisites Products .....	20
2.4 Disk Space Requirements .....	22
2.5 A Sample Installation .....	22
2.5.1 Main Installation Selection Panel .....	23
2.5.2 Installation of Netscape Navigator 4.0 .....	24
2.5.3 Installation of Lotus Domino Go Webserver .....	25
2.5.4 Installation of IBM Network Station Manager .....	28
2.6 Installation Notes .....	34
2.6.1 Installation Verification .....	34
2.6.2 Types of Windows NT Server Installations .....	35
2.6.3 Creation of NSMAdmin and NSMUser Groups .....	36
2.6.4 Re-Installation and Update .....	38
2.6.5 Desktop Shortcut for the IBM Network Station Manager .....	39
2.6.6 Lotus Domino Go Webserver Startup .....	40
2.6.7 The Lotus Domino Go Webserver Configuration File .....	42
2.6.8 Microsoft IIS 4.0 Web Server .....	44
2.7 Documentation .....	46
2.7.1 IBM Network Station Manager .....	46
2.7.2 eNetwork On-Demand Servers .....	47
2.7.3 Lotus Domino Go Webserver .....	48
2.7.4 Microsoft's IIS 4.0 .....	50
2.8 Installed Directory Structure .....	50
2.9 Installing NSM on Windows NT Server 4.0, Terminal Server Edition .....	53
2.10 Uninstalling Products .....	53
2.10.1 Netscape Browser and Lotus Domino Go Webserver Uninstall .....	53
2.10.2 IBM Network Station Manager Uninstall .....	53
2.10.3 IBM Intermediate Support Driver Uninstall .....	53
2.10.4 NSMAdmin and NSMUser User Groups .....	54
2.10.5 Remaining Files and Directories .....	54

2.11	Installing Products Individually . . . . .	54
2.12	Batch Mode Installation . . . . .	55
2.12.1	Recording an Automated Install . . . . .	55
2.12.2	Using the Automated Install . . . . .	56
2.12.3	Changing the Install Drive in the Response File . . . . .	57
2.13	Boot Server Special Install . . . . .	57
2.14	Authentication Server Special Install . . . . .	59
2.15	Windows NT Server 4.0, Terminal Server Edition Installation . . . . .	62
2.16	MetaFrame from Citrix Systems Inc. . . . .	62
2.16.1	MetaFrame Installation . . . . .	62
2.16.2	Licensing . . . . .	63
2.16.3	Administration . . . . .	64
2.16.4	MetaFrame Documentation . . . . .	65
2.17	UNIX Integration Services (UIS) for MetaFrame . . . . .	66
2.17.1	UIS Installation . . . . .	66
2.17.2	UIS Configuration . . . . .	67
2.17.3	UIS Documentation . . . . .	69
<b>Chapter 3.</b>	<b>Migration from Release 2 . . . . .</b>	<b>71</b>
3.1	Migration Overview . . . . .	71
3.2	Migration Methods . . . . .	72
3.2.1	The Single Server Migration . . . . .	72
3.2.2	The Dual Server Migration . . . . .	73
3.3	What Actually Needs to Be Migrated? . . . . .	75
3.4	Dual Server Migration Example . . . . .	77
3.4.1	Server Migration . . . . .	78
3.4.2	Client Retargeting . . . . .	80
3.4.3	Retargeting Clients That Boot Using NVRAM . . . . .	80
3.4.4	Retargeting Clients That Boot Using DHCP . . . . .	84
3.5	Single Server Migration Example . . . . .	86
3.5.1	Server Migration . . . . .	87
3.5.2	Retargeting Clients that Boot Using NVRAM . . . . .	90
3.5.3	Retargeting Clients That Boot Using DHCP . . . . .	92
3.6	Migration/Installation Problems . . . . .	92
3.6.1	Migration Tasks . . . . .	93
3.6.2	Using the NSMMIGR.EXE Utility . . . . .	94
3.6.3	Using the NTNSMRR2.EXE Utility . . . . .	95
3.7	Migrating Custom R2 Configuration Files . . . . .	97
3.8	Migrating the Boot Monitor Prom . . . . .	99
3.9	Changing to DHCP Remotely . . . . .	100
<b>Chapter 4.</b>	<b>Separation of Servers . . . . .</b>	<b>101</b>
4.1	What Is Separation of Servers? . . . . .	101
4.2	Objectives of Using Separate Servers . . . . .	102
4.2.1	Load Balancing . . . . .	103
4.2.2	Centralized Administration . . . . .	104
4.2.3	Roaming . . . . .	104
4.3	Types of Servers - Definitions . . . . .	106
4.3.1	DHCP Server . . . . .	106
4.3.2	Boot Server . . . . .	107
4.3.3	Terminal Configuration Server . . . . .	107
4.3.4	Authentication Server . . . . .	108
4.4	Other Server Types . . . . .	109

4.4.1	Application Server . . . . .	109
4.4.2	File Server . . . . .	109
4.4.3	Print Server . . . . .	109
4.4.4	Summary . . . . .	110
4.5	An Example of Separation of Servers . . . . .	111
4.5.1	Configuration . . . . .	112
4.5.2	DHCP Options . . . . .	115
4.6	Implementing Separation of Servers . . . . .	117
4.6.1	Access to Server Directories . . . . .	118
4.6.2	A Sample File Service Table . . . . .	119
<b>Chapter 5.</b>	<b>Using the IBM Network Station . . . . .</b>	<b>123</b>
5.1	The Menu Bar . . . . .	123
5.2	The IBM Network Station Console . . . . .	124
5.2.1	Statistics . . . . .	125
5.2.2	Setup . . . . .	127
5.2.3	Utilities . . . . .	131
5.2.4	Window Manager . . . . .	132
5.2.5	Terminals . . . . .	132
5.2.6	Login . . . . .	133
5.2.7	Console . . . . .	135
5.2.8	Messages . . . . .	135
5.3	The Command Pop-Up Menu . . . . .	135
<b>Chapter 6.</b>	<b>Configuring the IBM Network Station . . . . .</b>	<b>137</b>
6.1	Physical Installation . . . . .	137
6.2	Setup/Configuration Methods . . . . .	137
6.3	Configuration of the IBM Network Station . . . . .	137
6.3.1	Setting Up for a Boot Using NVRAM . . . . .	139
6.3.2	Logging On . . . . .	143
6.3.3	Setting Up for a Boot Using DHCP . . . . .	145
<b>Chapter 7.</b>	<b>Using the IBM Network Station Manager Application . . . . .</b>	<b>147</b>
7.1	What Is IBM Network Station Manager? . . . . .	147
7.2	How to Access the IBM Network Station Manager . . . . .	148
7.3	A Few NSM Typical Configuration Examples . . . . .	152
7.3.1	Creating a 3270 Menu Bar Item . . . . .	152
7.3.2	Autostarting an Application . . . . .	153
7.3.3	Adding a Remote Program Menu Item . . . . .	153
7.3.4	Adding a Local Program Menu Item . . . . .	154
7.3.5	Adding a Terminal Menu Item . . . . .	155
7.3.6	Starting a Java Applet . . . . .	155
7.3.7	Adding a Java Application Menu Item . . . . .	156
<b>Chapter 8.</b>	<b>Emulators, Browser and Java . . . . .</b>	<b>159</b>
8.1	5250 and 3270 Emulators . . . . .	159
8.1.1	Converged 3270 and 5250 Emulators . . . . .	159
8.1.2	Additional 3270/5250 Emulator Enhancements . . . . .	159
8.1.3	Additional NLS Enhancements . . . . .	161
8.1.4	Emulators and Java . . . . .	161
8.1.5	Terminal (VT320) Emulator . . . . .	161
8.2	NC Navigator Browser . . . . .	163
8.3	Java . . . . .	164

<b>Chapter 9. NFS, TFTP and Time Servers</b> .....	165
9.1 Trivial File Transfer Protocol (TFTP) Server .....	165
9.1.1 TFTP Configuration .....	165
9.1.2 TFTP Tracing and Logging .....	167
9.1.3 TFTP Help .....	167
9.2 Time Server .....	169
9.2.1 Time Server Configuration .....	169
9.2.2 Time Server Logging/Tracing .....	170
9.3 Networking File System (NFS) Server .....	171
9.3.1 NFS Configuration .....	171
9.3.2 NFS Logging/Tracing .....	174
 <b>Chapter 10. Dynamic Host Configuration Protocol (DHCP)</b> .....	175
10.1 What Is DHCP? .....	175
10.1.1 Static vs. Dynamic IP Address Allocation .....	177
10.2 How a Client Obtains Information via DHCP .....	178
10.2.1 DHCPDISCOVER .....	178
10.2.2 DHCPOFFER .....	178
10.2.3 DHCPREQUEST .....	178
10.2.4 DHCPACK .....	179
10.2.5 DHCPDECLINE .....	179
10.3 What Are DHCP Options? .....	181
10.4 How to Configure the DHCP Server .....	183
10.4.1 Default DHCP Configuration File .....	185
10.4.2 Server Parameters .....	186
10.4.3 Global Definitions .....	187
10.4.4 Subnet Definition .....	188
10.4.5 Client Definition .....	189
10.4.6 Class Definitions .....	190
10.5 DHCP Server Administration .....	191
10.6 Online Documentation .....	193
10.7 Using DHCP with IBM Network Stations .....	194
10.7.1 Summary .....	194
10.7.2 Why Is Using DHCP Better Than NVRAM? .....	194
10.7.3 IP Configuration of a Typical PC .....	195
10.7.4 IP Configuration of an IBM Network Station .....	195
10.7.5 Case 1- Permanent IP Address .....	196
10.7.6 Case 2 - Variable IP Address - Fixed IP Name .....	197
10.7.7 Case 3 - Variable IP Address - No Host Name .....	197
10.7.8 Using Multiple DHCP Servers .....	198
 <b>Chapter 11. Dynamic Domain Name Services (DDNS)</b> .....	199
11.1 What Is a Domain Name Server (DNS)? .....	199
11.2 Why Is a DNS Required? .....	200
11.3 Why Is a Dynamic DNS Required? .....	200
11.4 Can There Be Multiple DNS Servers? .....	200
11.5 How Does It Work? .....	201
11.6 How to Configure for DDNS? .....	202
11.6.1 Configuring the DNS Information on the IBM Network Station ...	203
11.6.2 Choosing between DHCP or NSM DNS Data .....	204
11.6.3 Configuring the DHCP Server to Perform DDNS Updates .....	205
11.7 The DDNS Server Administrator .....	208
11.8 DDNS Logging/Tracing .....	211



<b>Chapter 12. Full-Screen Solutions</b> . . . . .	215
12.1 Full-Screen Solutions in Release 2.5. . . . .	215
12.2 Full-Screen Solutions in Release 3 . . . . .	215
12.2.1 How Are Full-Screen Solutions Implemented in R3? . . . . .	216
12.2.2 A 3270 Full-Screen Example . . . . .	217
12.2.3 Security Considerations . . . . .	219
<b>Chapter 13. Configuration Files Structure</b> . . . . .	221
13.1 Types of Configuration Parameters . . . . .	222
13.2 Types of Configuration Files . . . . .	222
13.3 Configuration Files Directories . . . . .	224
13.4 Configuration Files . . . . .	226
13.4.1 Hardware Configuration Files . . . . .	226
13.4.2 Application Configuration Files . . . . .	229
13.4.3 Startup Configuration Files . . . . .	231
13.5 Configuration Files Download Sequence . . . . .	233
13.5.1 Hardware Files Download . . . . .	234
13.5.2 Client Initialization (Pre-Authentication) . . . . .	235
13.5.3 Preference Files (Post-Login) . . . . .	235
13.5.4 Startup Files . . . . .	237
13.5.5 NC Navigator Start . . . . .	238
13.6 User Editable Files - Summary . . . . .	238
<b>Chapter 14. Printing</b> . . . . .	239
14.1 History . . . . .	239
14.2 Release 3 Print Support . . . . .	239
14.3 Particularities of the IBM Network Station . . . . .	243
14.4 Configuration Using the IBM Network Station Manager . . . . .	243
14.5 Additional Details . . . . .	245
<b>Chapter 15. The Lotus eSuite Workplace</b> . . . . .	247
15.1 Prerequisites . . . . .	247
15.2 Installation . . . . .	247
15.3 Configuration/Administration . . . . .	249
15.3.1 Configure the DNS in IBM Network Station Manager . . . . .	249
15.3.2 Configure the Desktop in IBM Network Station Manager . . . . .	250
15.3.3 Starting the eSuite WorkPlace Administrator . . . . .	254
15.3.4 Configuring eSuite WorkPlace Applications . . . . .	256
15.3.5 Starting the eSuite Workplace Desktop . . . . .	259
<b>Chapter 16. National Language Support (NLS)</b> . . . . .	263
16.1 Installation Language . . . . .	263
16.2 Summary - Rule of Thumb . . . . .	263
16.2.1 The Installation Dialog Language . . . . .	264
16.2.2 The Application Language . . . . .	265
16.2.3 The Windows NT Regional Settings . . . . .	266
16.2.4 The Windows NT Input Locales . . . . .	267
16.3 The Startup Language . . . . .	268
16.3.1 What Does It Affect? . . . . .	268
16.3.2 How Is It Configured? . . . . .	268
16.4 The Keyboard Language . . . . .	270
16.4.1 What Does It Affect? . . . . .	270
16.4.2 How Is It Configured? . . . . .	270
16.5 The Login Panel Language . . . . .	271

16.5.1	What Does It Affect?	271
16.5.2	How Is It Configured?	272
16.6	The Kernel Environment Language	272
16.6.1	What Does It Affect?	272
16.6.2	How Is It Configured?	273
16.6.3	Japanese Language Input Method	274
16.6.4	The NC Navigator	275
<b>Chapter 17.</b>	<b>Connecting to Windows Applications Servers</b>	<b>277</b>
17.1	Windows Applications Servers	277
17.2	What Is WinFrame?	279
17.3	What Is WinCenter Connect?	280
17.3.1	What Is WinCenter?	280
17.4	Windows NT 4.0 - Terminal Server Edition (WTSE)	281
17.5	Connecting an IBM Network Station to Windows Terminal Server	282
17.5.1	Using Microsoft's Remote Desktop Protocol (RDP)	282
17.6	Connect Using ICA	287
17.6.1	Define a Menu Bar Item for an ICA Connection	287
17.6.2	Using an Autostarted Session	289
17.6.3	Using the ICA Chooser Application	289
17.6.4	Using the Kiosk Mode	292
17.6.5	Keyboard Support - ICA	292
17.7	Using NCD's UNIX Integration Services (UIS) for X.11 Connections	293
17.7.1	Using a Remote Program Menu Item (RSH Command)	293
17.7.2	Local Window Manager or WinCenter Window Manager?	299
17.8	Issuing IBM Network Station Commands from a Windows Desktop	299
17.8.1	From a WinCenter Desktop	300
17.8.2	From a MetaFrame Desktop	301
<b>Chapter 18.</b>	<b>Installing Applications on WTSE</b>	<b>303</b>
18.1	Objectives	303
18.2	Overview	304
18.3	Sources of Information	305
18.4	Application Compatibility Issues	306
18.4.1	What Is the Cause of the Problem?	306
18.4.2	Application Compatibility Problems	307
18.4.3	Solutions, Tools and Techniques	307
18.4.4	Registry Settings Problems	309
18.4.5	File Problems	310
18.4.6	Object Problems	311
18.5	Home Directories and Home Drives	311
18.5.1	What Is a Home Directory	311
18.5.2	Creating a Home Directory	311
18.5.3	What Is a Home Drive?	314
18.6	Logon Scripts	318
18.7	User Profiles	319
18.7.1	Location of the User Profile Settings	320
18.7.2	Initial Creation of a User Profile	320
18.7.3	Example - Creating and Copying a User Profile	321
18.7.4	Specifying a User Profile Path in the User Account	322
18.7.5	Local, Roaming and Mandatory User Profiles	323
18.7.6	User Profile in a Multi-User Environment	324
18.7.7	User Profiles in WinFrame	324

18.8	The change user Command	325
18.8.1	The change user /install Command	325
18.8.2	The change user /execute Command	327
18.8.3	The change user /query Command	330
18.9	A Few Practical Examples	331
18.9.1	An Application Using Only an INI File	331
18.9.2	An Application Using Registry Entries and User Files	333
18.9.3	An Application Using Registry Entries That Require Modifications	340
18.9.4	Summary - Examples	346
18.10	Controlling the Execute Mode	346
18.10.1	Applications Compatibility Flags	347
18.10.2	IniFiles Compatibility Flags	349
18.10.3	Registry Entries Compatibility Flags	349
18.11	Networking Applications Limitations	350
18.12	Updating INI Files and Registry Entries	350
18.13	Using the Registry Editor	351
18.14	Summary	352
18.15	Application Notes in Windows NT Server 4.0, Terminal Server Edition	354
18.16	WinCenter's Multi-User Application Manager	355
18.16.1	What Is Multi-User Application Manager (MAM)?	355
18.16.2	MAM Templates	355
18.16.3	MAM Policies	356
18.16.4	MAM Edit and Execution Mode	356
18.16.5	Should I Use MAM or Not?	356
18.16.6	Sample MAM User Interface	357
<b>Chapter 19.</b>	<b>Problem Determination - Tools, Tips and Techniques</b>	<b>363</b>
19.1	The IBM Network Station Message Log	363
19.1.1	On-Screen Messages during the Boot Process	363
19.1.2	Messages on the IBM Network Station Console	364
19.1.3	Message Log via TELNET from the IBM Network Station	365
19.1.4	Message Log from a Remote Host Using TELNET	367
19.1.5	Sample Message Log	369
19.2	The Network Station Console	370
19.3	NT's Event Viewer	370
19.4	Controlling Access to the IBM Network Station	372
19.4.1	X Server Access	373
19.4.2	Console Access	374
19.4.3	Configuration and User Preference Information Access	374
19.4.4	Diagnostic Access	375
19.4.5	File Manager Password	375
19.4.6	Screen Lock Password	375
19.4.7	Unit Global Password	375
19.4.8	Remote Command Execution Access	376
19.5	Launching Commands from a Remote Host	376
19.5.1	Commands	377
19.5.2	Help on Commands	379
19.6	Accessing the Setup Panels from Another Network Station	382
19.7	Using the Config Daemon from a Remote Location	382
19.8	Using the Boot Monitor Commands	386
19.9	Getting Additional File Diagnostics	386
19.10	Uploading Dump Files	388
19.10.1	Using TFTP to Upload a DUMP File	388

19.10.2 Using NFS to Upload a DUMP File . . . . .	388
19.11 Resetting NVRAM Defaults . . . . .	390
19.12 Resetting the IBM Network Station Password . . . . .	390
19.13 Avoiding Reboots . . . . .	391
19.14 Rebooting IBM Network Stations Remotely . . . . .	392
19.15 Getting Additional Messages with Java . . . . .	393
19.16 Service Information Tool . . . . .	393
19.17 Lotus Domino Go Webserver Logging/Reporting . . . . .	394
19.18 DHCP Server Logging/Tracing . . . . .	395
19.19 Windows NT Network Monitor . . . . .	400
19.19.1 Installing the Network Monitor Tool . . . . .	402
19.19.2 Using the Network Monitor Tool . . . . .	403
<b>Appendix A. Useful Control Key Sequences . . . . .</b>	<b>417</b>
<b>Appendix B. Boot Monitor Commands . . . . .</b>	<b>419</b>
<b>Appendix C. Special Notices . . . . .</b>	<b>421</b>
<b>Appendix D. Related Publications . . . . .</b>	<b>423</b>
D.1 International Technical Support Organization Publications . . . . .	423
D.2 Redbooks on CD-ROMs . . . . .	423
D.3 Other Publications . . . . .	423
D.4 Web Sites . . . . .	424
<b>List of Abbreviations . . . . .</b>	<b>425</b>
<b>How To Get ITSO Redbooks . . . . .</b>	<b>427</b>
<b>Index . . . . .</b>	<b>431</b>
<b>ITSO Redbook Evaluation . . . . .</b>	<b>439</b>

## Figures

1. Touch Screen Hardware Setup . . . . .	4
2. A Sample Multiple Serial Port Adapter . . . . .	5
3. set serial-interfaces-table Parameter . . . . .	5
4. IBM Network Station Model 100 . . . . .	9
5. Ports and Connections . . . . .	10
6. IBM Network Station Architectural Overview . . . . .	12
7. IBM Network Station Components . . . . .	13
8. Network Station vs. PC . . . . .	14
9. Boot Sequence Summary . . . . .	16
10. Boot Servers vs. Application Servers . . . . .	17
11. Summary of Components . . . . .	18
12. Readme Files on the CD-ROM . . . . .	21
13. Error Message When Installing on a FAT Drive . . . . .	21
14. First Install Screen (Language) . . . . .	23
15. Install Task Selection Screen . . . . .	23
16. The Install Additional Products Panel . . . . .	24
17. Installation Type and Destination Directory . . . . .	24
18. Lotus Domino Go Webserver- Select Components . . . . .	25
19. Choose Component Directories (1) . . . . .	26
20. Choose Component Directories (2) . . . . .	26
21. Choose Configuration Parameters . . . . .	27
22. Lotus Domino Go Webserver Completion Message . . . . .	27
23. IBM Network Station Main Install Screen . . . . .	28
24. Language Selection for NSM . . . . .	28
25. DHCP Selection Panel . . . . .	29
26. Migration Panel . . . . .	30
27. Destination Directory for the eNetwork On-Demand Server . . . . .	31
28. NC Navigator Question . . . . .	31
29. Summary of Products to Be Installed . . . . .	32
30. Desktop Shortcut Creation Question . . . . .	33
31. Installation Progress Feedback . . . . .	33
32. Install Completion Screen . . . . .	33
33. Add/Remove Programs after Installation . . . . .	34
34. Installed Services . . . . .	35
35. Creating an NSMACCT Global Group on a PDC . . . . .	36
36. Local Group Properties . . . . .	37
37. Add Users and Groups . . . . .	37
38. NSMUser Group on Local Server . . . . .	38
39. Service Update Message . . . . .	39
40. Service Update Message (2) . . . . .	39
41. The IBM Network Station Manager Desktop Shortcut Properties . . . . .	40
42. Lotus Domino Go WebserverService Startup . . . . .	40
43. Lotus Domino Go Webserver Status Panel . . . . .	41
44. Lotus Domino Go Webserver Error Log . . . . .	42
45. Adding NSM Configuration Entries to HTTPD.CNF . . . . .	43
46. Restart the Lotus Domino Go Webserver after Altering httpd.cnf . . . . .	43
47. Updating Microsoft's IIS 4.0 . . . . .	44
48. Properties for the networkstation Virtual Directory . . . . .	45
49. Default Document - IIS 4.0 . . . . .	45
50. IBM Network Station Manager Online Help Facility . . . . .	47

51. eNetwork On-Demand Server Online HTML Documentation . . . . .	48
52. The Lotus Domino Go Webserver Main Page . . . . .	49
53. Lotus Domino Go Webserver Documentation. . . . .	50
54. Directory Structures (R3 and R2.5). . . . .	51
55. Main Directories Expanded. . . . .	52
56. eNetwork On-Demand Server Directory Structure . . . . .	52
57. Sample setup.iss Response File. . . . .	56
58. Install Type Registry Entry . . . . .	58
59. Authentication Server Installation . . . . .	61
60. Authentication and Configuration Server . . . . .	62
61. MetaFrame Installation Autorun Panel . . . . .	63
62. MetaFrame Tools and Applications Folder . . . . .	63
63. MetaFrame Licenses. . . . .	64
64. MetaFrame Administration . . . . .	65
65. MetaFrame Online Documentation . . . . .	65
66. UIS Installation Panel . . . . .	66
67. UIS Applications Folder. . . . .	67
68. UIS Configuration Manager. . . . .	68
69. UIS Group Definition . . . . .	68
70. Enabling X.11 Connections. . . . .	69
71. Single Server Migration Method . . . . .	72
72. The Dual Server Migration Method . . . . .	74
73. Dual Server Migration - Example 1 . . . . .	78
74. Migration Path Prompt during NSM Install . . . . .	79
75. Release 2 Boot Parameters . . . . .	81
76. Summary - Retargeting NVRAM Clients - Dual Server Method . . . . .	82
77. Changing the Pilot Client's NVRAM for Retargeting . . . . .	83
78. Defaults.dft in \nstation\configs\ on the R3 Server . . . . .	84
79. Defaults.dft in \nstation\configs\ on the R3 Server . . . . .	85
80. Single Server Migration Example . . . . .	87
81. Detection of Old Versions . . . . .	88
82. Progress Display - Uninstalling . . . . .	88
83. Removal Confirmation Panel . . . . .	89
84. unInstallShield Removal Display. . . . .	89
85. Location of User Preference Files to Be Migrated . . . . .	90
86. Single Server Migration - Retargeting NVRAM Clients . . . . .	91
87. Defaults.dft from \nstation\configs on R3 Server. . . . .	91
88. Detection of Old Versions, after an Interruption . . . . .	93
89. Running the NSMMIGR.EXE Utility . . . . .	94
90. The \userbase\home and \users Subdirectories . . . . .	95
91. Output of the NTNSMRR2.EXE Utility . . . . .	97
92. Boot Parameters - Enabling Boot Using DHCP . . . . .	100
93. A Sample Separation of Servers Scenario . . . . .	102
94. Load Balancing . . . . .	103
95. Roaming . . . . .	105
96. Server Types - Summary . . . . .	111
97. Separation of Server Example . . . . .	112
98. The Setup Utility Panels . . . . .	113
99. Using the Roam Button on the Login Panel . . . . .	114
100. Specifying an Authentication Server. . . . .	115
101. DHCP Options for Separate Servers . . . . .	116
102. DHCP Options and Equivalent Configuration Parameters . . . . .	117
103. Accessing Directories on Servers. . . . .	119

104.Display of the File Service Table on the IBM Network Station . . . . .	121
105.IBM Network Station Console . . . . .	125
106.IBM Network Station Console - Show Version . . . . .	125
107.IBM Network Station Console - Memory . . . . .	126
108.IBM Network Station Console - X Connections . . . . .	126
109.IBM Network Station - Statistics . . . . .	127
110.IBM Network Station Console - Quick Setup . . . . .	128
111.IBM Network Station Console - Setup Parameters . . . . .	129
112.IBM Network Station Console - Setup - File Pull-Down. . . . .	130
113.IBM Network Station Console - User Preferences. . . . .	131
114.IBM Network Station Console -Test Network . . . . .	132
115.IBM Network Station Console - Terminal/Telnet . . . . .	133
116.The set term-default-host Parameter. . . . .	133
117.The set login-default-host Parameter . . . . .	134
118.IBM Network Station Console - Login Host Chooser. . . . .	135
119.The set exec-command-menu Parameter . . . . .	136
120.Main Network Station Setup Utility Panel . . . . .	138
121.Set Network Parameters - NVRAM - IBM Network Station Setup Utility . . . .	139
122.Set Boot Parameters . . . . .	141
123.Set Configuration Parameters Panel . . . . .	142
124.Kernel Loading Process. . . . .	143
125.IBM Network Station Login Screen . . . . .	144
126.Password Change Panel . . . . .	144
127.Using the Roam Function . . . . .	145
128.Set Network Parameters - Network . . . . .	146
129.Accessing the IBM Network Station Manager . . . . .	147
130.The IBM Network Station Manager Main Panel. . . . .	149
131.Tasks Available to the User Authority Level . . . . .	150
132.IBM Network Station Manager - Workstation Defaults . . . . .	151
133.Adding a Menu Item. . . . .	152
134.Adding a 3270 Menu Item - Additional Parameters. . . . .	153
135.Autostarting an Application . . . . .	153
136.Adding a Remote Program Menu Item . . . . .	154
137.Adding a Local Program Menu Items . . . . .	155
138.Adding a Terminal Menu Item . . . . .	155
139.Adding a Java Applet Menu Item. . . . .	156
140.Adding a Java Application Menu Item . . . . .	157
141.Using TN3270 from the Browser . . . . .	160
142.Terminal Menu in NSM . . . . .	162
143.The Terminal (VT320) Emulator Command Options. . . . .	162
144.TFTPD Configuration Panel - Service . . . . .	166
145.TFTPD Configuration Panel - Directories . . . . .	166
146.TFTPD Configuration Panel - Trace . . . . .	167
147.eNetwork On-Demand Server Product Documentation. . . . .	168
148.TFTP Server Documentation. . . . .	168
149.The Time Server . . . . .	169
150.Timed Configuration Panel - Adjust to Local Time . . . . .	170
151.Time Settings on the IBM Network Station . . . . .	170
152.Time Server Restarting Message . . . . .	170
153.Time Server Log File . . . . .	171
154.NFS Server Configuration - Main Panel . . . . .	171
155.NFS Server Configuration - Directories . . . . .	172
156.NFS Server Configuration - Directories - Edit . . . . .	173

157.NFS Server Configuration - Users .....	174
158.NFS Server Configuration - Trace .....	174
159.DHCP Overview .....	176
160.DHCP Boot Sequence Summary .....	180
161.An Example Trace of DHCP Discover/Offer Activities .....	181
162.A DHCP Frame/Record .....	182
163.New R3 DHCP Options .....	183
164.The Main DHCP Configuration Panel .....	184
165.DHCP Server - Miscellaneous Parameters .....	186
166.Configuring Global DHCP Options .....	187
167.The Subnet Configuration Panel .....	188
168.DHCP Client Configuration Panel .....	189
169.DHCP Class Definition .....	190
170.DHCP Server Administration - IP Addresses .....	191
171.DHCP Server Administration - Clients .....	192
172.The dadmin -i Command .....	192
173.DHCP Server Administration - Server .....	193
174.eNetwork On-Demand Server Online HTML Documentation .....	193
175.What Is a DNS Server? .....	199
176.A Dynamic Domain Name Server .....	201
177.DHCP Server Updating DDNS on Behalf of Client .....	202
178.DHCP Configuration - DNS Information .....	203
179.A Sample hosts.nsm File .....	204
180.Domain Name Server Configuration Panel in IBM Network Station Manager	204
181.Configuring NDS in NSM .....	205
182.The DDNS A Records Panel on DHCP Server Configuration .....	206
183.Requesting DDNS A Record Update .....	206
184.The DDNS PTR Records Panel on DHCP Server Configuration .....	207
185.DDNS Server for PTR Record Updates in Subnet Definition .....	207
186.NSUPDATE Monitor Window .....	208
187.The DDNS Server Administrator Main Panel .....	209
188.NSLOOKUP Command Output .....	210
189.DDNS Server Administration - Reverse Address Details .....	211
190.DDNS Logging .....	212
191.DDNS Trace Enabling .....	213
192.RUNWM Environment Variable .....	217
193.Removing Menu Bar .....	217
194.Autostart a 3270 Session in Kiosk Mode .....	218
195.Setting Background to Black .....	218
196.Types of Configuration Parameters .....	222
197.Configuration File Types .....	223
198.Configuration File Types .....	224
199.Prodbase Directories per Platform .....	225
200.Userbase Directories per Platforms .....	225
201.Shipped Hardware Configuration Files .....	226
202.System-Wide Defaults Hardware Configuration Files .....	227
203.Individual Terminal Hardware Configuration File .....	228
204.Group Hardware Configuration File .....	228
205.User Hardware Configuration File .....	228
206.Product-Owned Application Configuration Files .....	229
207.Shipped Application Configuration Files .....	229
208.System-Wide Application Configuration Files .....	230
209.Group Application Configuration Files .....	231



210.Individual User Application Configuration Files . . . . .	231
211.Shipped Startup Configuration Files . . . . .	232
212.System-Wide Startup Configuration Files . . . . .	232
213.Group Startup Configuration Files . . . . .	233
214.Individual User Startup Configuration Files . . . . .	233
215.Startup File Sourcing . . . . .	237
216.Print Capabilities Overview . . . . .	240
217.A Sample Print Dialog . . . . .	241
218.The Printer Selector. . . . .	242
219.The IBM Network Station Manager Printer Settings Configuration . . . . .	244
220.Printer List Parameters - System Defaults. . . . .	245
221.Destination Directory - Lotus eSuite WorkPlace Installation . . . . .	248
222.NT Services for Lotus eSuite WorkPlace. . . . .	249
223.DNS Configuration in IBM Network Station Manager . . . . .	249
224.Creating a New NT Group . . . . .	250
225.Setting Group Defaults . . . . .	250
226.Desktop and Menu Bar Options. . . . .	251
227.Setting an Environment Variable . . . . .	251
228.Setting the TZ Environment Variable. . . . .	252
229.Members of the esuite Group . . . . .	252
230.Selecting a Users Group . . . . .	253
231.Choosing a Group for a User. . . . .	254
232.Starting the eSuite Workplace Administrator. . . . .	254
233.Lotus eSuite WorkPlace Administrator Starting. . . . .	255
234.Lotus eSuite WorkPlace Administrator Main Configuration Panel. . . . .	256
235.Adding a User to eSuite WorkPlace Administrator . . . . .	257
236.The All Users Group in eSuite WorkPlace Administrator. . . . .	258
237.The Customize Workplace Panel in eSuite WorkPlace Administrator. . . . .	259
238.The Lotus eSuite WorkPlace Standard Desktop . . . . .	260
239.The Lotus eSuite WorkPlace Browser Application . . . . .	261
240.The First Installation Panel . . . . .	265
241.The NSM Release 3 Setup Language Selection Panel. . . . .	265
242.The Windows NT Regional Settings . . . . .	266
243.The Windows NT Input Locales. . . . .	267
244.The Main Setup Utility Panel . . . . .	269
245.Setup Utility - Set Language Parameters . . . . .	269
246.Setting the Startup Language . . . . .	270
247.Setting the Keyboard Language . . . . .	271
248.Login Panel, in French, for Wrong Password . . . . .	272
249.Sample Menu Bar, Prompt Panels and Error Messages in French. . . . .	273
250.The Language Settings for a User. . . . .	274
251.Japanese Language Input Method . . . . .	275
252.Local vs. Remote Application Execution . . . . .	278
253.The WinFrame Product . . . . .	279
254.WinCenter Connect . . . . .	280
255.Windows NT 4.0 - Terminal Server Edition . . . . .	281
256.Terminal Server Client Creator . . . . .	283
257.Installed Terminal Server Client Shortcuts . . . . .	283
258.MS Terminal Server Client Panel . . . . .	284
259.Client Connection Manager. . . . .	284
260.Connection Details. . . . .	285
261.Connection Options . . . . .	286
262.Application Selection . . . . .	286

263.	Configuring an ICA Client . . . . .	288
264.	The icacInt Command Usage . . . . .	288
265.	ICA Chooser Panel. . . . .	290
266.	Defining an ICA CHooser Menu Item . . . . .	290
267.	ica-chooser-entries Parameter in defaults.dft. . . . .	290
268.	ICA Chooser - Properties . . . . .	291
269.	Existing Disconnected Sessions. . . . .	291
270.	Defining an X.11 Connection . . . . .	293
271.	The X11 Command Options . . . . .	294
272.	The wincenter Command . . . . .	295
273.	A WInCenter Menu Item . . . . .	295
274.	Geometry Parameter Example . . . . .	296
275.	Resolution Parameter Example . . . . .	297
276.	Resolution Parameter Example 2. . . . .	298
277.	Creating Icons for wcpsh Commands . . . . .	301
278.	Specifying a Home Directory for a User . . . . .	312
279.	Home Directories . . . . .	313
280.	Permissions Set on the Home Directory. . . . .	313
281.	How a Home Drive Is Used . . . . .	315
282.	Making the Home Directory a Shared Drive . . . . .	316
283.	Using the Connect To Option for a Home Directory . . . . .	317
284.	Specifying a Logon Script in the User Profile . . . . .	319
285.	A User Profile . . . . .	320
286.	System Properties - User Profiles . . . . .	321
287.	The Copy To Panel while Copying a User Profile . . . . .	322
288.	User Environment Profile - User Profile Path . . . . .	323
289.	User Profile Editor in WinFrame . . . . .	325
290.	Copying Registry Entries to a Central Location . . . . .	327
291.	Copying Registry Entries to HKEY_CURRENT_USER . . . . .	328
292.	Copying INI Files to the User's Home Directory . . . . .	329
293.	Summary - Change User Process . . . . .	330
294.	Creating a pfe32.ini File . . . . .	333
295.	The SmartSuite Files Installed by the Server Install Process. . . . .	335
296.	SmartSuite Entries in HKEY_LOCAL_MACHINE after Server Install . . . . .	335
297.	User Files for SmartSuite in the User's Home Directory . . . . .	337
298.	HKEY_CURRENT_USER Registry Entries after SmartSuite Node Install . . . . .	338
299.	Terminal Server\Install\Software Registry Entries . . . . .	339
300.	WTSE Application Notes for MS Internet Explorer 3.x . . . . .	341
301.	Application Installation and Logon Scripts . . . . .	342
302.	The msie30.cmd File . . . . .	343
303.	The msie30.key File . . . . .	344
304.	Registry Entries after the msie30.cmd Script Execution. . . . .	345
305.	WTSE Registry Compatibility Keys . . . . .	347
306.	Example - Compatibility Flags for the REGEDIT Application . . . . .	349
307.	REGEDT32 Version of the Registry Editor. . . . .	352
308.	REGEDIT Version of the Registry Editor . . . . .	352
309.	Summary . . . . .	353
310.	The MAM Template Editor - Main Panel . . . . .	357
311.	MAM Templates - Directories Actions . . . . .	358
312.	MAM Templates - File Actions . . . . .	359
313.	MAM Templates - Edit File Action . . . . .	359
314.	MAM Templates - Registry Actions . . . . .	360
315.	MAM Templates - INI Files Actions . . . . .	360

316.MAM Templates - Command Actions . . . . .	361
317.A Sample Policy. . . . .	361
318.IBM Network Station Setup Utility - Diagnostic Verbose Option . . . . .	364
319.IBM Network Station Console Messages . . . . .	365
320.IBM Network Station Console Messages via Diag Port. . . . .	366
321.IBM Network Station Console - Options . . . . .	367
322.Accessing Messages Remotely. . . . .	368
323.IBM Network Station Console Messages via Telnet 5998. . . . .	368
324.Sample Messages in the Message Log. . . . .	369
325.NT Event Viewer . . . . .	371
326.NT Event Viewer - Details of an Event . . . . .	371
327.NT Event Viewer - Specifying a Display Filter . . . . .	372
328.X Server Access Control . . . . .	374
329.Setting the Administrator Password. . . . .	375
330.Help on the Navio Command. . . . .	380
331.Help on the ns3270 Command . . . . .	380
332.Help on the ns5250 Command . . . . .	381
333.Help on telnet or term . . . . .	381
334.Help on Miscellaneous Other Commands . . . . .	382
335.Connecting to a Remote Station . . . . .	382
336.Config Daemon Commands for Read-Only . . . . .	383
337.Config Daemon Commands for Read-Write . . . . .	384
338.Sample Partial get all Parameters List. . . . .	385
339.Boot Monitor Commands. . . . .	386
340.Message Log with File Extended Diagnostics Enabled. . . . .	387
341.NFS Service Directory . . . . .	389
342.Resetting Password. . . . .	391
343.NSREBOOT Command Sample Output . . . . .	393
344.Executing ntnsmver through a Web Browser . . . . .	394
345.Lotus Domino Go Webserver Logging and Reporting. . . . .	395
346.DHCP Server - Logging Parameters . . . . .	396
347.Error MESSage - Log File Name . . . . .	397
348.DHCP Server Sample Message Log. . . . .	399
349.The ForcePmode Registry Entry . . . . .	401
350.The Linkage Registry Entries. . . . .	402
351.Network Monitor Tool Installation . . . . .	403
352.Network Monitor Tool - Main Panel while Capturing Data. . . . .	404
353.Network Monitor Tool - Capture Filters . . . . .	405
354.Network Monitor Tool - Filtering on Addresses . . . . .	406
355.Network Monitor Tool - Display Panel . . . . .	407
356.Network Monitor Tool - Display Filters. . . . .	408
357.Network Monitor Tool - Selecting the DHCP Frames Only . . . . .	409
358.Network Monitor Tool - Display of DHCP Frames Only. . . . .	410
359.Network Monitor Tool - Displaying the Details of Each Frame . . . . .	411
360.Network Monitor Tool - Printing Selected Frames. . . . .	412
361.Network Monitor Tool - Printing Selected Frames - Advanced Options . . . .	412
362.Frame 23 - A DHCPDISCOVER Frame - Page 1 . . . . .	413
363.Frame 23 - A DHCPDISCOVER Frame - Page 2 . . . . .	414
364.Frame 31 - A DHCPOFFER Frame - Page 1 . . . . .	415
365.Frame 31 - A DHCPOFFER Frame - Page 2 . . . . .	416



## **Tables**

1. IBM Network Station Models . . . . .	10
2. Size of Installed Directories . . . . .	22
3. Size of Remaining Directories after Uninstall. . . . .	54
4. Migrating Manual Changes from Release 2.5 to Release 3. . . . .	99
5. File Service Table Contents after Boot and Login . . . . .	120
6. Exports File on the Boot Server . . . . .	121
7. DHCP Classes - IBM Network Station . . . . .	191
8. Summary of Type 3 (User Editable) Files . . . . .	238
9. Applications Compatibility Flags Settings . . . . .	347
10. IniFiles Compatibility Flags Settings . . . . .	349
11. Registry Entries Compatibility Flags Settings . . . . .	349
12. Useful IBM Network Station Control Key Sequences . . . . .	417



---

## Preface

This redbook describes all of the major functions available with Release 3 of the IBM Network Station Manager, the differences from the previous version and how to migrate from the previous release.

It is meant as a complete guide to installing both the server and the IBM Network Station. It shows how to configure the server, use the IBM Network Station Manager to configure the IBM Network Station clients and how to use the facilities and applications on an IBM Network Station. It also helps you to understand how the migration facilities work, understand what separation of servers is and how to configure for it, understand what DHCP/DDNS are and how they can be used with IBM Network Stations, what WinFrame, WinCenter, Windows Terminal Server Edition and MetaFrame are and how to set up connections to these servers, how to install applications on a Windows Terminal Server and finally how to use some of the tools to do problem determination.

---

## The Author

This redbook was produced by a member of the Systems Management and Networking Center, Raleigh.



**Claude Béchard** is a Senior Technical Marketing Support Representative at the Systems Management and Networking ITSO Center, Raleigh. He joined the ITSO seven years ago and wrote several redbooks on SNA and IBM Communications Server products. His responsibility in the last 18 months has been to produce documents on the IBM Network Station and Windows NT. He is an IBM Canada employee, with 29 years of service, and holds a degree in Mechanical and Industrial Engineering from the University of Montreal.

The author wishes to extend his gratitude to those individuals in the IBM Network Station development organization who spent time answering his questions.

---

## Comments Welcome

### Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in "ITSO Redbook Evaluation" on page 439 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

For Internet users <http://www.redbooks.ibm.com>

For IBM Intranet users <http://w3.itso.ibm.com>

- Send us a note at the following address:

[redbook@us.ibm.com](mailto:redbook@us.ibm.com)





---

## Chapter 1. Overview

The objective of this redbook is to discuss all the major functions available with Release 3 of the IBM Network Station Manager on Windows NT Server 4.0 and on Windows NT Server 4.0, Terminal Server Edition. We also discuss the differences and migration from the previous release.

The previous redbook on this subject was entitled *IBM Network Station Guide for Windows NT*, SG24-2127-01, and it discussed the functions available with Release 2.x of the IBM Network Station Manager software on both Windows NT 4.0 and Winfred/WinCenter servers.

Some of the information available in the previous redbook that was somewhat release-independent, such as problem determination, has been revised, updated and included here in order to make this document complete for anyone using only Release 3.

When appropriate, we refer you to other redbooks that might include a more complete description of a particular topic, such as printing. See Appendix D, "Related Publications" on page 423 for other redbooks and publications on the IBM Network Station.

---

### 1.1 What Is New in Release 3?

The objective of this section is to provide a brief list of the new features and functions available with Release 3 of the IBM Network Station Manager software for those readers that are already familiar with the previous release. Where necessary, more details are provided in the chapters that follow.

Some of the enhancements are:

- An improved integrated installation process

This release provides a very significant improvement in the ease of installation by providing a single integrated installation process. Installation can be done on either a Windows NT 4.0 Server or on Windows NT 4.0 Terminal Server Edition.

Some prerequisite products such as Netscape 4.04 Browser and Lotus Domino Go Webserver 4.6.1 are included on the CD along with the IBM Network Station Manager software. If Microsoft's Internet Explorer 4.0 and Internet Information Server 4.0 are desired, they can be downloaded from Microsoft's site.

The install process also includes a batch install capability as well as some special boot server and authentication server install modes.

- Extensive national language support
- Migration support from Release 2.x

Single and dual server migration methods are offered, and compatibility directories are provided to allow for an easier retargeting of clients from an R2 to an R3 system.

Please refer to Chapter 3, "Migration from Release 2" on page 71 for detailed migration examples.

- Separation of servers

This is the ability for an IBM Network Station to get its required operational files from multiple servers, instead of a single boot server, during the overall boot process.

For example, an IBM Network Station can get its network configuration data from a DHCP server, its base code (meaning its kernel and application modules) from a boot server, its hardware configuration data from a terminal configuration server, and its customized user configuration data from an authentication server.

Please refer to Chapter 4, "Separation of Servers" on page 101 for a detailed description of these facilities.

- Enhanced *IBM Network Station Guide for Windows NT*, SG24-2127

Release 3 provides support for the TCP/IP LPR/LPD protocol (RFC 1179), which allows the IBM Network Station to act as either a print client or print server. This includes also LPR/LPD streaming support, which is a draft extension to RFC 1179.

Chapter 14, "Printing" on page 239 provides only a brief overview of the printing functions available; please refer to *IBM Network Station Printing Guide*, SG24-5212 for a more complete and detailed description of the printing capabilities.

- 3270 and 5250 emulators

These have been converged and enhanced with additional features.

- A kiosk (full-screen) mode

Kiosk (full-screen) mode provides a way of suppressing the login panel and an encoding utility to encode the file containing the kiosk user IDs and passwords.

- IBM Network Station Manager

The NSM is common across all IBM server platforms. It now includes a lot more parameters, leaving very little need for back door configuration files.

Some of the additional parameters that are now supported are printers, the VTxxx emulator, user groups, DNS configuration, etc.

The NSM uses NT user ID and password both with the IIS and Lotus Go Webservers.

- A common configuration file structure

In order to facilitate the use of multiple server platforms, the configuration file structure has been modified to have more commonality across platforms.

- Java Virtual Machine (JVM) 1.1.4 and Just-in-Time (JIT) Compiler support

- An Independent Computing Architecture (ICA) Client

An ICA client is now included to establish sessions to WinFrame and Windows Terminal Server Edition with MetaFrame.

- Lotus eSuite 1.1 WorkPlace support

- NC Navigator Browser

The 40-bit version is integrated in the product install. (That is, it is installed automatically.) The 128-bit version is an optional install on the North American version of the CD.

- **Change password capability**

The user can now change his or her password in the IBM Network Station Login panel if the user account has been configured to require a change of password at the next logon.

- **Use of NFS for kernel download**

Using NFS for downloading the kernel is now the default protocol in Release 3 instead of TFTP which was the previous default.

- **NT event log messages**

The IBM Network Station Manager and Network Station Login server now write their error messages to the NT event log.

- **A new utility, called nsreboot, for remotely rebooting one or more IBM Network Stations.**

- **The product publication, in PDF format, is included on the CD with Adobe Acrobat reader.**

---

## **1.2 Release 3.02 Additional Functions**

A few additional functions to NSM Release 3 have been made available, through PTFs, shortly after GA. These are:

- Touch screen support
- Multiple serial port adapter support
- PCMCIA and flash boot

We only include a brief summary here, with pointers to Web sites containing more information, because we did not have the opportunity to really test these new features before publication.

### **1.2.1 Touch Screen Support**

Please see <http://www.pc.ibm.com/networkstation/whitepapers/touch.html> for a white paper on this particular function.

#### **1.2.1.1 What Is it?**

A touch screen is a CRT or flat panel monitor that has been enabled with a transparent, touch-sensitive surface.

This touch surface can be used in environments where a mouse or other pointing device is inconvenient, environmentally unsuitable, or not intuitive for the user. Touch screens are operated using a selection device, typically the user's finger, rather than a mouse.

A touch screen attached to an IBM Network Station functions as a one-button mouse and provides all of the operations normally performed by the left mouse button, including single-click selection, drag and drop, and double-click. The application program receives and interprets the input as if it were seeing a mouse with only a left button. Tasks normally associated with a right mouse button cannot be performed via a touch screen unless the application is reprogrammed.

### 1.2.1.2 Hardware Setup

The touch screen monitor's video input is connected to the standard video output of the IBM Network Station just like any other monitor while the touch sensor itself connects to the IBM Network Station via the RS-232C serial communication connection.

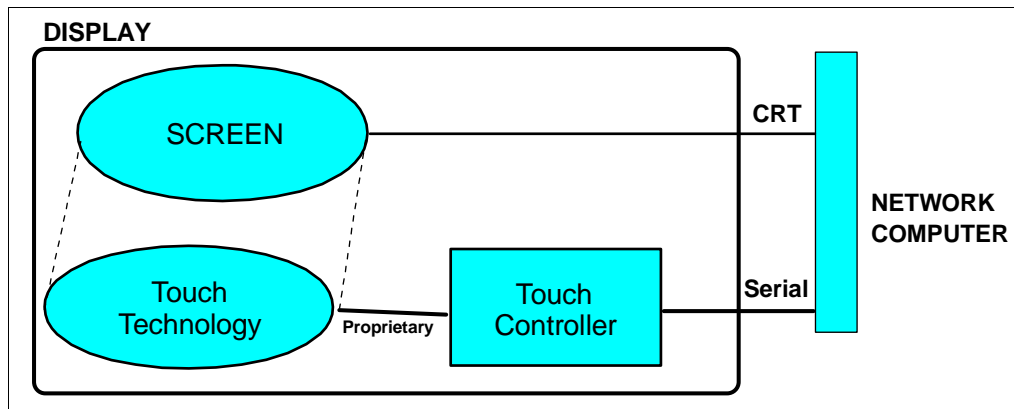


Figure 1. Touch Screen Hardware Setup

### 1.2.1.3 Software Setup

To add the support for touch screen, add the following lines to the defaults.dft configuration file.

```
set serial-interfaces-table = { { 1 input-device input-device 9600 8 1 none  
none none } }  
set xserver-input-extension-device = ibm-touchscreen  
set pref-xserver-current-pointing-device = mouse-and-extension-device  
set xserver-retain-x-settings = true
```

The touch screen initially also needs to be calibrated; to calibrate, use the Console as follows. (Note: Access to the Console Setup functions must have been enabled to be able to calibrate.)

1. Select **Console=>Setup=>Change Setup Parameters=>Input Devices=>Calibrate**.
2. At the prompt, touch lower left and upper right corners of the screen
3. Select **File=>Save to NVRAM**.

See <http://www.pc.ibm.com/networkstation/whitepapers/touch.html> for additional and up-to-date details.

## 1.2.2 Multiple Serial Port Adapter

Please see <http://www.pc.ibm.com/networkstation/solutions/interface.html> for a white paper on this particular function.

### 1.2.2.1 What Is it?

The multiple serial port adapter increases the serial interface of the Network Station from a single native serial port to multiple serial ports through the use of a Type II PCMCIA Card.

The multiple serial port card allows a range of serial devices to be attached to the IBM Network Station such as printers, scanners, plotters, etc. These can be enabled through the interfaces, extending the capability of the IBM Network Station to a fuller range of specialized application solutions.

Figure 2 on page 5 is the representation of a typical adapter card:



Figure 2. A Sample Multiple Serial Port Adapter

#### 1.2.2.2 Programming Support

While many types of serial devices, such as MICR readers, pole displays, cash drawers, etc., can be connected to the IBM Network Station serial port, IBM does not provide any device drivers for these devices.

Application programming is required to send and receive data to these ports/devices. This is done through a TCP/IP socket interface. Since the interfaces use TCP/IP, the application to access the ports can run on any server in the network.

The application can also be written in Java to run natively on the Network Station. The programming interface to these additional ports is identical to that used to address the built-in serial port.

#### 1.2.2.3 Software Setup

Add the following lines to the defaults.dft configuration file. The initial line (port 1) is required for the native serial port. Add lines for ports 2 to 5 depending on how many ports are present on the adapter card.

```
set serial-interfaces-table = {  
  { 1 <mode> <mode> <baud-rate> <data-bits> <stop-bits> <parity> <handshake> none }  
  { 2 <mode> <mode> <baud-rate> <data-bits> <stop-bits> <parity> <handshake> none }  
  { 3 <mode> <mode> <baud-rate> <data-bits> <stop-bits> <parity> <handshake> none }
```

Figure 3. set serial-interfaces-table Parameter

See <http://www.pc.ibm.com/networkstation/solutions/interface.html> for further details and for a programming example.

### 1.2.3 Flash Boot Support

Release 3.0 IBM Network Station Manager has been enhanced to provide flash memory card support.

This function is available in U.S. English for IBM Network Stations connected to any of the IBM servers supported by Release 3.0. It is offered in North America and Europe/Middle East/Africa only. North America Request for Price Quote (RPQ) orders are subject to NCD approval; Europe/Middle East/Africa RPQs will be generally available upon request.

For a complete description of this feature, please refer to the following Web site:

[www.pc.ibm.com/networkstation/whitepapers/flash.html](http://www.pc.ibm.com/networkstation/whitepapers/flash.html)

#### 1.2.3.1 What Is It?

A flash memory card is a PCMCIA adapter card on which data can be recorded. When the card is inserted into the IBM Network Station PCMCIA adapter slot, the local file system can access the data recorded on the card. This is somewhat equivalent (with restrictions) to inserting a diskette in a PC for example.

These cards vary in storage capacity from 10 MB for a C-Series card to 40 MB for a D-series card.

By storing the IBM Network Station software (operating system, application modules, etc.) on the flash memory card, the IBM Network Station can actually be triggered to boot from the flash memory card instead of a server.

This function blends very well with the separation of server functions provided by NSM Release 3. Indeed, the flash memory card provide the functions normally provided by a boot server (base code server) while the terminal configuration server and the authentication server can still be located across a wide area network.

The main benefits are a significant reduction in the network traffic caused by an IBM Network Station boot, which is especially valuable in a network with reduced bandwidth availability.

#### 1.2.3.2 Peer Booting

In an environment where many stations are on a local high-speed LAN, without a boot server on the LAN, and a WAN connection to the rest of the network, the flash card in one IBM Network Station can be used to boot other IBM Network Stations on the local area network using the NFS protocol. This is known as *peer booting*. The other IBM Network Stations need only be set up as if they were booting from any other server. The peer booting capability is built in to the Network Station and requires no additional software.

#### 1.2.3.3 Cautions

Even though using flash memory cards can be advantageous in certain cases, there are a few potential disadvantages and facts that must be taken into consideration when considering their use.

The Web site [www.pc.ibm.com/networkstation/whitepapers/flash.html](http://www.pc.ibm.com/networkstation/whitepapers/flash.html) makes the following points:

- Customers should not assume that the flash boot capability detailed in this document via PCMCIA cards will necessarily persist as future models of the IBM Network Station are announced. The C and D series cards may not be supported, the PCMCIA slot may not be available, and/or IBM may devise a better way to provide this capability such as through internal memory or media.
- It takes approximately two minutes per megabyte to copy data to the flash card. If the copy process is interrupted, the flash card may be left in such a state that the Network Station cannot be booted from it.
- It is recommended that PCMCIA flash be treated as read-only memory. While it can be written to by applications (such as a browser), the fact that space is not easily recoverable means that the card will fill up and be unusable for further updates until space is reclaimed manually.
- Management of a flash card equipped IBM Network Stations is time-consuming and not yet automated. No tools are provided to synchronize the files on the flash card with those on the server or even to indicate when the files on the flash card are down-level from some designated configuration. In fact, the files on the flash card (local) file system have no time stamps so it is not easy to tell which version of each software module is on the card.

#### **1.2.4 Series 1000 Type II PCMCIA Feature**

A new option now available for the IBM Network Station Series 1000 is a hardware feature which provides one type II Personal Computer Memory Card Industry Association (PCMCIA) slot.

Software support for this adapter is contained in the latest level of Network Station Manager Release 3.

Customers can now utilize the PCMCIA feature of the Series 1000 to implement flash boot or multiple serial port support.

A few of the early IBM Network Station Series 1000 had a pre-installed PCMCIA adapter slot and only need the appropriate Network Station Manager software to support a PCMCIA card.

For those IBM Network Station Series 1000s without a pre-installed PCMCIA adapter slot, the adapter is now available on all models.

For ordering and information about obtaining the PCMCIA adapter, please contact your IBM representative or an IBM Business Partner and refer to part number 07L8336. The PCMCIA adapter can be ordered in the GEMS ordering system in the U.S. and Canada or in the UPOS ordering system in EMEA.

See <http://www.pc.ibm.com/networkstation/solutions/s1000.html> for details.

---

### **1.3 IBM Network Station Overview**

This section is an introduction to the IBM Network Station for those readers who may not already be familiar with what the product is and how it works. It is definitely not meant as a detailed description of all the features and functions but only as a very high-level and summarized overview necessary for anyone with a

general background in information processing technology to get a general idea of what an IBM Network Station is and how it functions.

### **1.3.1 What Is an IBM Network Station?**

The IBM Network Station is what is known as a network computer or a thin client.

You can think of it as a PC, except that this PC does not have any local disk storage. Therefore, due to the absence of local storage, it must obtain all of its operational software from a remote server.

If we compare the IBM Network Station to a PC again, when you power up a PC, the boot process takes care of fetching the required software components, such as the operating system, from the local disk storage, and after having loaded the operating system in memory, control is passed to the operating system. The user can then start any application, and when he or she does so, further software components are fetched from the local storage and loaded into memory by the operating system.

The IBM Network Station basically goes through the same process. That is, the boot process takes care of fetching the required software components, but instead of fetching them from local storage, it has the ability to connect to a remote server and to fetch the components from that remote server. It is sort of equivalent to having a remote network drive attached to a PC and getting software components from that remote drive instead of a local drive.

The main advantage of this arrangement is that the software used by many IBM Network Stations resides in one central location and can therefore be maintained much more easily than if copies were distributed to every station.

#### **1.3.1.1 What Does It Look Like?**

Physically, the IBM Network Station is much smaller than a PC. A model 100 is illustrated in the figure below:





*Figure 4. IBM Network Station Model 100*

The basic IBM Network Station includes:

- A PowerPC RISC-based microprocessor, of varying speed dependent on the model
- RAM memory, up to 64 MB
- Network interface supports 10BASE-T Ethernet or 4/16 Mbps token-ring
- 8-bit audio speaker
- Standard PC type ports for:
  - Keyboard
  - Mouse
  - VGA or SVGA monitor
- Parallel port supports system printer connection
- Serial port for modem or peripheral device support
- Type 2 PCMCIA flash memory card for local storage (except for later models of the Series 1000)

Below is a graphical representation of these hardware components:

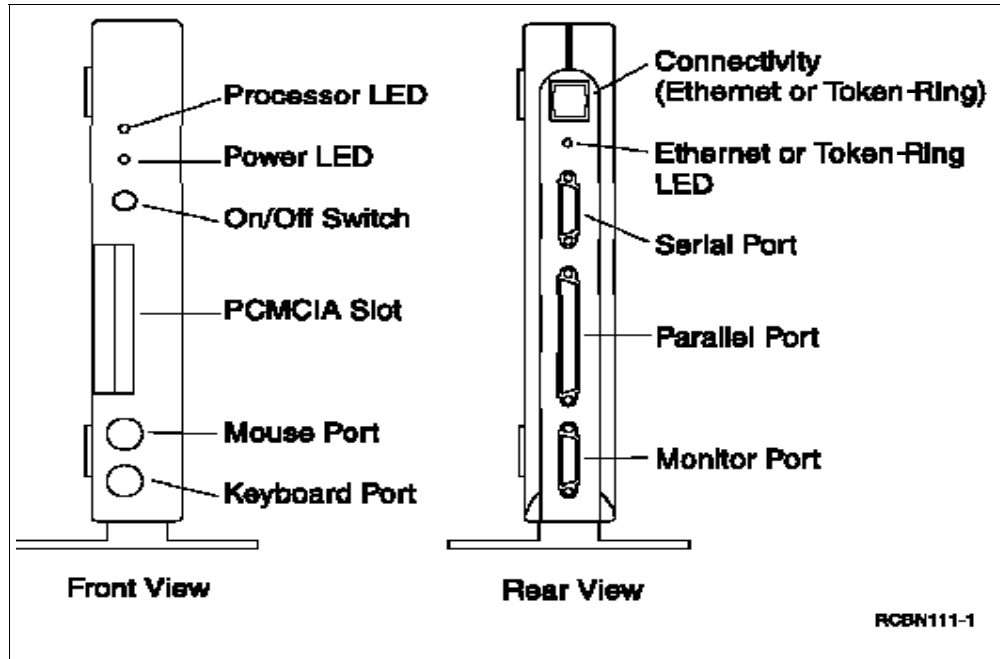


Figure 5. Ports and Connections

### 1.3.1.2 How Many Models Are There?

At this point in time, the available models are as follows:

Model	Description	Memory
8361-100	Series 100 Ethernet	8 MB
8361-200	Series 100 Token-Ring	8 MB
8361-110	Series 300 Ethernet	16 MB
8361-210	Series 300 Token-Ring	16 MB
8361-341	Series 300 Twinax	16 MB
8362-A22	Series 1000 Token-Ring	32 MB
8362-A23	Series 1000 Token-Ring	64 MB
8362-A52	Series 1000 Ethernet	32 MB
8362-A53	Series 1000 Ethernet	64 MB

Table 1. IBM Network Station Models

Generally, the model to use is mainly dependent on the type of applications that the user needs:

- The Series 100 is intended to be used as a network access computer. In this environment, the user is mainly concerned with accessing server-based applications through the emulators and the X-Windows or ICA support.
- The Series 300 is intended to be used for Internet access through a browser, in addition to accessing server-based applications.

- The Series 1000 is intended for using Java-based applications and office suites.

For more details and up-to-date information, please consult the IBM Network Station Web site (<http://www.pc.ibm.com/networkstation/>).

### 1.3.2 What Software Does It Run?

The IBM Network Station's processor is not an Intel-based processor but a Power PC RISC processor; therefore it runs a UNIX-like operating system.

This operating system is loaded into the IBM Network Station's memory from a server, during the boot phase.

After it gets control, it is ready to run applications. These applications can either be native applications, meaning that they actually execute on the IBM Network Station itself under the control of the local operating system, or they can be applications running remotely on application servers.

#### 1.3.2.1 Native Applications

Native applications that can execute on the IBM Network Station are as follows:

- A local 3270 or 5250 emulator

The application modules are loaded from the server at the time that the user starts the application for the first time. Actually, there is a way to pre-load these application modules, if desired, during the boot phase so that the load time is much quicker when the application is requested by the user.

- A local browser

The NC Navigator browser is provided as a native browser that runs locally, just like the emulators. This application is also loaded from the server the first time that it is invoked.

- Java applets or Java applications

Java applets or applications can be run locally on the IBM Network Station.

#### 1.3.2.2 Applications Running on Remote Servers

Applications can also be executed on remote servers (AIX servers or Windows NT servers) from the display of the IBM Network Station, which acts as an X station.

The X-Windows support can be used to connect into a remote AIX server for example, and the Common Desktop Environment (CDE) facility of AIX can be used to execute AIX applications from the display, keyboard and mouse attached to the IBM Network Station. In this case, all applications execute on the remote server(s); the only part that executes on the IBM Network Station is the code allowing the input and output to be redirected to the display of the IBM Network Station.

The same X-windows support can also be used to connect to a Windows application server such as a WinCenter host or a Windows Terminal Server running MetaFrame and UNIX Integration Services in order to execute Windows applications on the remote server and have the input/output redirected to the IBM Network Station's display. In that case, the ICA protocol can also be used (instead of X-windows) to connect into a WinFrame or MetaFrame server.

Please refer to Chapter 17, “Connecting to Windows Applications Servers” on page 277 for an explanation of what these Windows application servers are.

### 1.3.2.3 IBM Network Station Architecture

Figure 6 on page 12 illustrates all of these software components on the IBM Network Station:

- The Network Station Base Components at the bottom of the diagram represent those components that are always present on the station, meaning that they do not have to be loaded from a server.
- The top portion of the diagram labeled Applications Loaded During Boot or On-Demand represent the applications, including the base operating system, that need to be loaded from a server (or possibly a flash memory card).

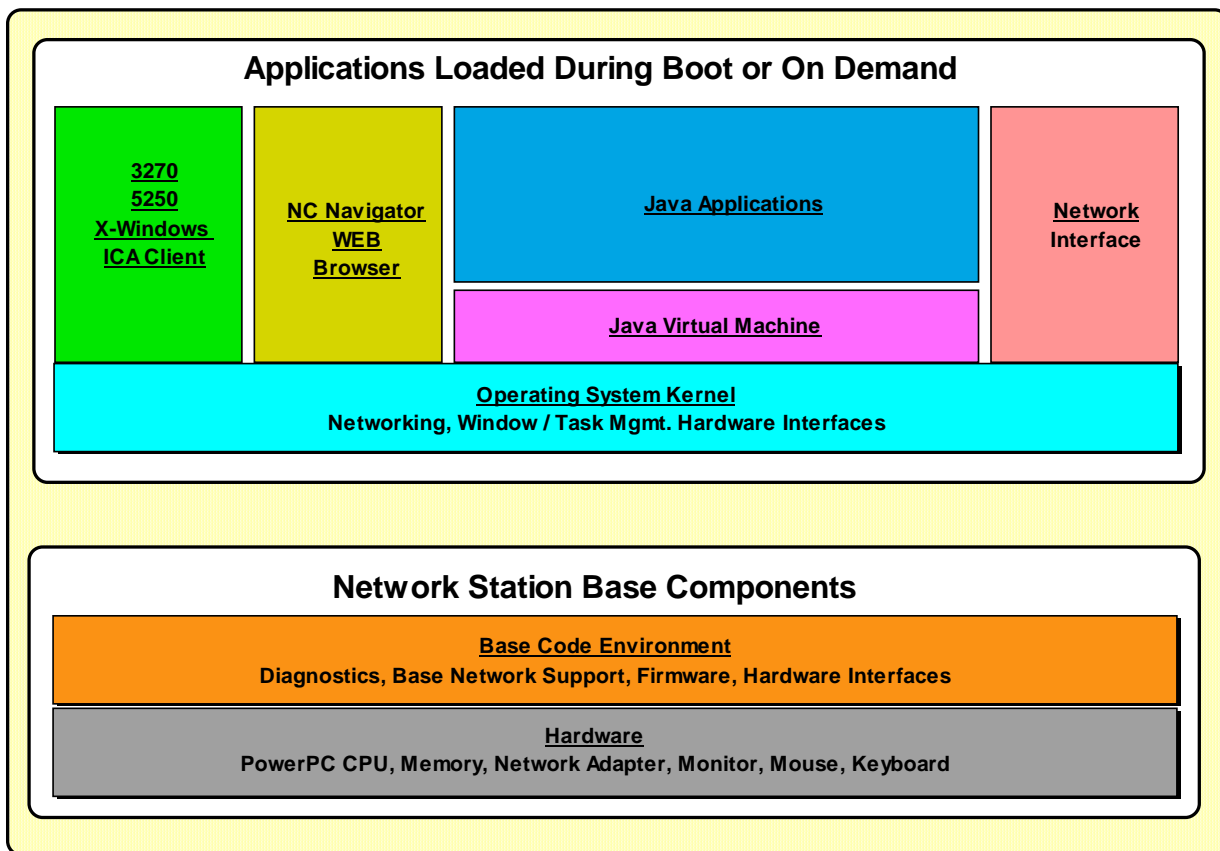


Figure 6. IBM Network Station Architectural Overview

### 1.3.3 How Does It Work?

Now that we know the basic components, how does this really work? How does the IBM Network Station come alive and succeed in getting what it needs to be operational when there is no local disk storage.

#### 1.3.3.1 Boot Phases

From the moment you power up the IBM Network Station, there are four phases we can identify:

1. The Power On Self Test (POST) phase, during which the station checks its components.
2. The Boot phase, during which it locates a boot server and downloads its operating system.
3. The Customization phase, during which it locates a configuration server and reads its terminal configuration files that determines how the station behaves.
4. The User Logon phase during which it locates an authentication server, obtains a user name and password, reads configuration files that are specific to the user logging on, and reads startup files that determines how the desktop looks and the applications, if any, that are to be automatically started.

### 1.3.3.2 IBM Network Station Components

Let's examine this in a bit more detail to understand how it works. To do this, we must first take a look at the IBM Network Station components. These are illustrated in the figure below:

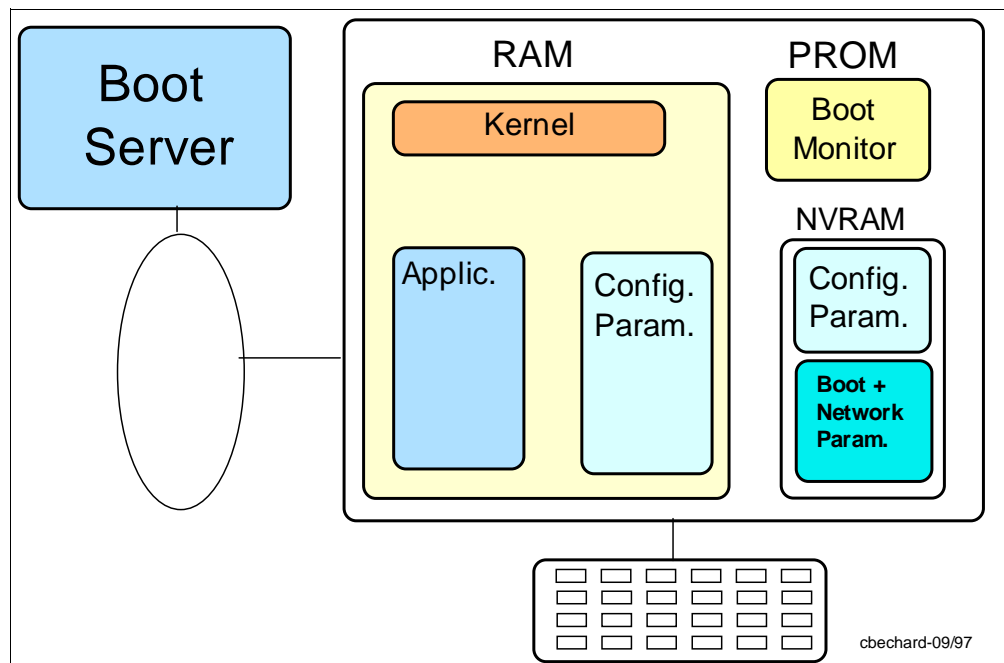


Figure 7. IBM Network Station Components

In the figure above:

- The Programmable Read Only Memory (PROM) contains a program called the Boot Monitor. This is the program that is given control after the power on is complete and is responsible for locating a boot server and downloading the operating system from that server.
- The Non-Volatile Random Access Memory (NVRAM) is memory that does not get erased when the station is powered off. It contains those configuration parameters that need to be retained after a power off; in particular, the address of a boot server for example.
- The Random Access Memory (RAM) is the main memory of the IBM Network Station in which the operating system and then some additional configuration parameters are loaded. (These are the configuration parameters that are

re-read after every boot and that do not need to remain permanently set.) Finally, any of the applications modules that the user requests are loaded.

This memory is real memory (not virtual) and therefore the amount of available memory must be sufficiently large enough to hold all applications that need to be resident simultaneously.

#### 1.3.3.3 What Is the Difference with a PC?

From a startup point of view, the main difference between a PC and an IBM Network Station is the fact that a PC has a local disk storage capability on which the operating system and other software components are stored.

Therefore, when the user powers on the PC, there is a component called the bootstrap that causes the retrieval of the required software components from the local disk storage, as illustrated in the next figure.

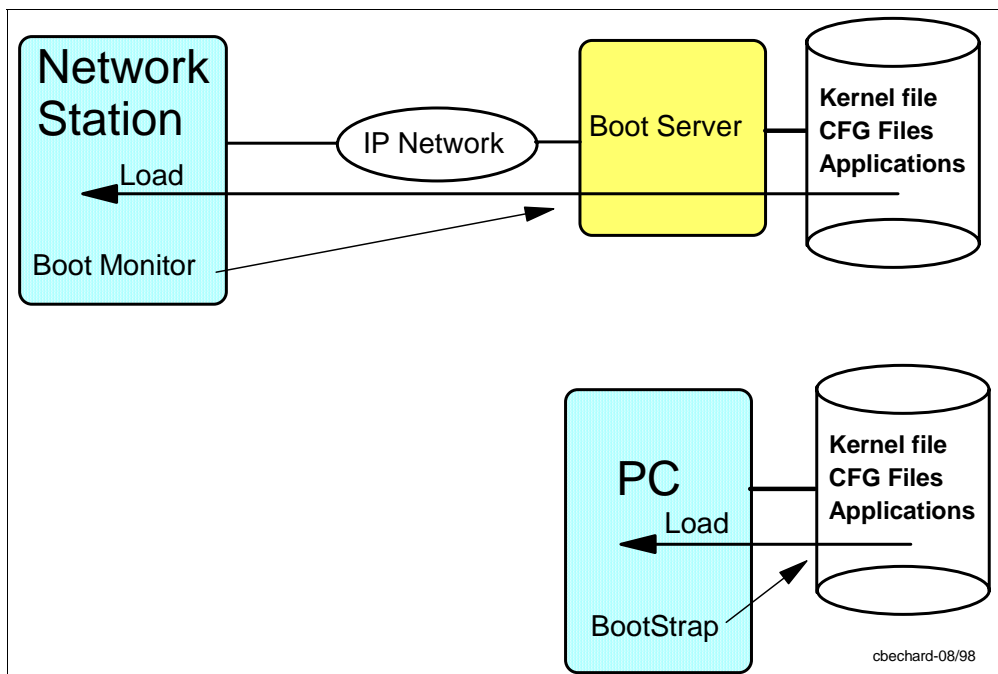


Figure 8. Network Station vs. PC

On the IBM Network Station, the equivalent of the bootstrap component is the boot monitor. The boot monitor is a program that has the ability to open the local network adapter, insert into the network, and contact a remote server from which to retrieve the required software components that it needs to boot. Therefore, the only difference actually is that the storage device that contains the software required for the machine to boot is local in one case and remote in the other.

#### 1.3.3.4 Boot Sequence of Events

What actually happens then after a IBM Network Station is powered on? In summary, the events are as follows:

1. The boot monitor program is given control. It examines the NVRAM network parameters to determine whether to use the network and boot parameters that are stored in NVRAM to contact a boot server, or whether it should use the

BOOTP/DHCP method of booting, which means getting this information from a server on the network instead.

2. If NVRAM indicates that it should get its network information from a server on the network, the boot monitor opens the network adapter and issues a broadcast on the network looking for a server that will supply it with the information it needs, such as an IP address, etc.

Assuming all goes well, a server responds and provides the boot monitor with the information it needs, such as an IP address, the address of a boot server, etc.

3. If NVRAM indicates that the required configuration information resides in NVRAM, the boot monitor reads this information locally from NVRAM.
4. The boot monitor then contacts the identified boot server and requests to download a copy of the kernel (operating system).
5. After the kernel is downloaded, it is given control. It queries the configuration information in NVRAM to determine the address of the configuration server. This information was either entered locally in NVRAM or was part of the information provided by the DHCP server.
6. The kernel contacts the configuration server (which can be the same as the boot server but does not have to be; please refer to Chapter 4, "Separation of Servers" on page 101 for details on using multiple servers) and reads the terminal configuration files that determine the behavior of the station.
7. One of the files obtained from the configuration server contains a configuration parameter called `exec-startup-commands` that determines which program is to be given control next. Normally, the next program to be given control is called `actlogin`, which is the login client. This login client is responsible for displaying a panel to the user and asking for a user name and password.

**Note:** There are ways of preventing the login panel from being displayed; this is called the kiosk mode. See Chapter 12, "Full-Screen Solutions" on page 215 for details.

8. The login client displays the login panel. The user enters a user name and password, and the login client locates the authentication server and then contacts the authentication server in order to validate the user.

**Note:** The authentication server is identified through either a configuration parameter or the user can enter a specific server by using the Roam button on the login panel.

Once the user has been verified, additional configuration files specific to this user and the group the user belongs to, are downloaded. Finally, startup files are also downloaded; these determine what items appear on the menu bar, which applications are to be started automatically and sets some environment variables.

The above steps are summarized in the diagram below:

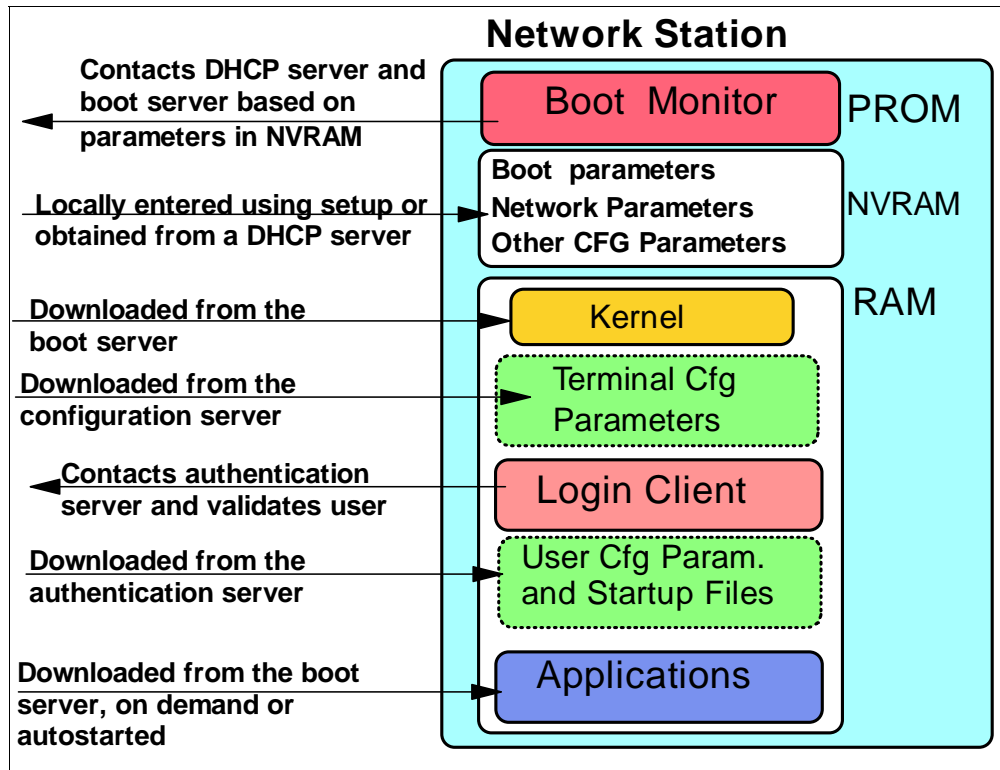


Figure 9. Boot Sequence Summary

In summary then, this is very similar to a PC starting its operation after a power up sequence, except that in this case, since there is no local disk storage, all the required components are fetched from a remote server. In addition, these components can be fetched from different physical servers when using the separation of servers functionality.

For details on the exact download sequence of all the files, please refer to 13.5, "Configuration Files Download Sequence" on page 233.

### 1.3.4 Server Software

What software runs on the on the servers and what operating systems can be used?

A boot server (or terminal configuration server or authentication server) can be based on any of the following hardware platforms:

- S/390
- AS/400
- RISC/6000
- PC Servers (Windows NT)

In fact, when using separate servers, servers can be mixed and matched. For example, the boot server can be a PC server, while the terminal configuration server can be a RISC/6000 and the authentication server can be an AS/400.

Application servers can also be based on any of these platforms.



The figure below illustrates the different servers. The term boot server in this diagram is used to indicate either a boot server, terminal configuration server, authentication server, or all three functions. In other words, the boot server function indicates the ability to download IBM Network Station software to the station as opposed to providing a user application capability.

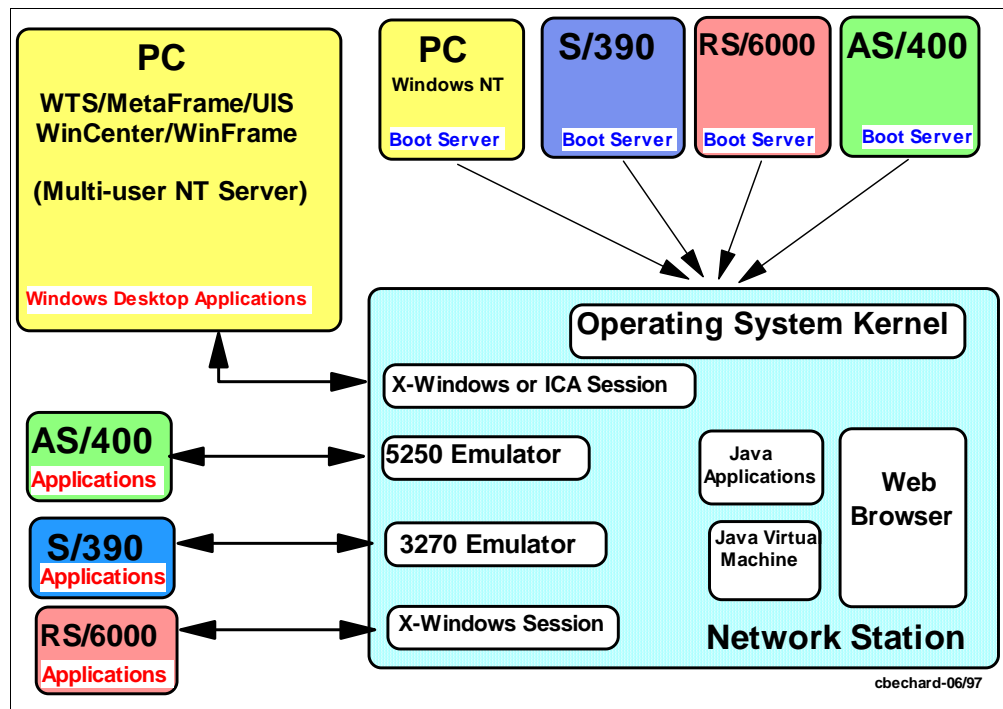


Figure 10. Boot Servers vs. Application Servers

#### 1.3.4.1 Server Components

Finally, what about the components required on the server?

Figure 11 on page 18 attempts to summarize the major components involved in interfacing with the IBM Network Station; they are as follows:

- The NFS server on the server handles all the requests for files to be downloaded to the IBM Network Station. It is used to download the kernel, the configuration files, the startup files and the application modules from the different directories on the server to the IBM Network Station.

Even though TFTP is not supported in Release 3 for the download of the kernel, the TFTP server is still installed. TFTP is still used for compatibility purposes during migration from previous releases, and can still be used by applications if desired.

- The NFS server is also tied into the Windows NT security subsystem to validate requests for files.
- The login server interfaces with the login client on the IBM Network Station and also ties in to the Windows NT security subsystem to authenticate users.
- The DHCP server can be, but does not have to be, on the same server as the boot server. In fact, the recommendation is that they not be on the same machine.

- The Network Station manager (NSM) is operated from any standard JavaScript-enabled browser, from anywhere on the Web. It is used to update the configuration files and startup files that are downloaded to the IBM Network Stations.

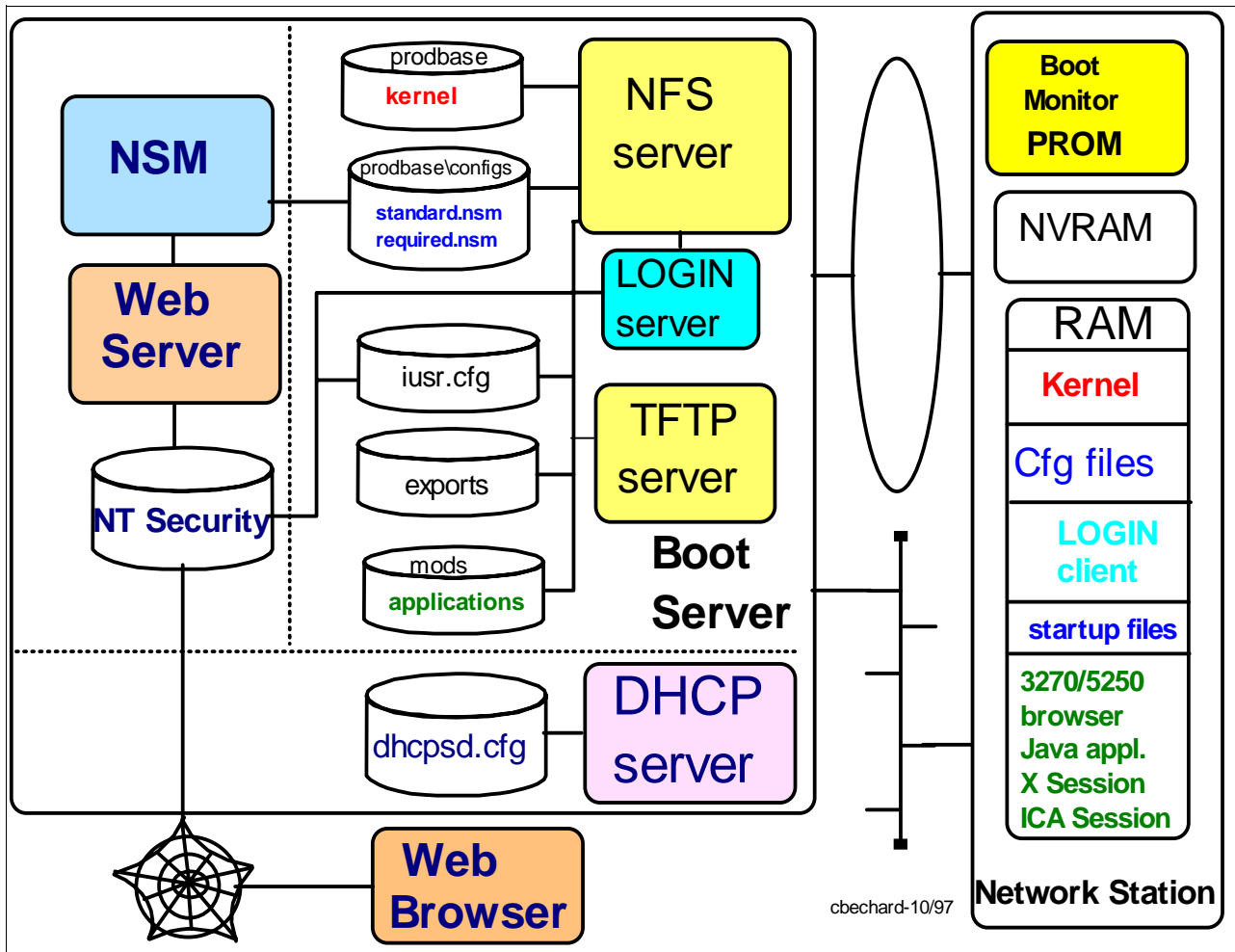


Figure 11. Summary of Components

---

## Chapter 2. Installation

This objective of this chapter is to discuss *installation-related* issues and to briefly illustrate a typical installation process.

The intent is not to provide detailed step-by-step installation instructions, because these are already provided in the *IBM Network Station Manager Installation and Use, SC41-0664* product publication, which also includes instructions to install a base Windows NT 4.0 system and the required Service Pack 3. We also recommend that you always read the README files as they include last minute details and corrections that are always useful to know.

Rather, the intent is to provide the reader with the result of our experience when we installed the product and to provide additional details and insight into the install process that might be of use in cases where the installation does not go exactly as planned.

In this chapter, we provide a sample installation for the additional components such as the Lotus Domino Go Webserver and for the IBM Network Station Manager.

In this first example, we install a brand new copy of the IBM Network Station Manager on a new server. For an installation example that includes a migration from a previous version, please refer to Chapter 3, "Migration from Release 2" on page 71.

---

### 2.1 Obtaining the Code

The IBM Network Station Manager code can be obtained, as with previous versions, either from the Web or by ordering a CD-ROM.

The Web site from which to obtain the code has not changed and is still:

<http://service.boulder.ibm.com/nc>

The CD-ROM can also be ordered from that Web site.

The CD contains the following code:

- The IBM Network Station Manager
- The eNetwork On-Demand Server
- The Lotus Domino Go Webserver
- The Netscape Navigator 4.04 Browser
- The NC Navigator Network Station Browser
- The Adobe Acrobat Reader

This CD can be ordered in either the North American version or the International Version.

If you wish to use Microsoft's Internet Explorer and Internet Information Server instead of the Netscape Navigator browser and Lotus Go Webserver, you need to download these products from Microsoft's Web site because these products are

not on the CD. The Web page has the required links to the appropriate sites for you to do this.

---

## 2.2 Differences with the Installation Process of Previous Releases

The installation process for Release 3 of the IBM Network Station Manager has been greatly improved over the previous versions.

Once the prerequisite products are installed (that is, Windows NT 4.0, Netscape or Internet Explorer browser, and Lotus Domino Go Webserver or Internet Information Server), the installation process for the IBM Network Station Manager and related products is a single stream integrated process that does not require a reboot until the end of the installation process.

You do not have to worry, as was previously the case, about installing individual components or about the specific sequence in which the products need to be installed.

Once the prerequisite products are installed, all that is required is to launch the IBM Network Station Manager install process and it takes care of installing the IBM NDIS Intermediate driver (previously known as the wedge) required by the IBM DHCP server, the eNetwork On-Demand Server (which includes the NFS server, TFTP server, DHCP server and TIMED server), the NC Navigator browser and the IBM Network Station Manager itself.

In fact, if you already have the base Windows NT 4.0 Server and Service Pack 3 installed (or Windows NT Server 4.0, Terminal Server Edition), and you wish to use the Netscape browser and the Lotus Domino Go Webserver that are on the CD as prerequisites, then all you need to do is to load the CD, install the prerequisite products, then launch the IBM Network Station Manager installation and reboot only once at the end of the installation sequence.

---

## 2.3 Prerequisites Products

Please remember to always consult the readme file that comes with the product for the latest information on prerequisites and last minute changes and instructions.

In this case, in addition to the general readme file, there are many other readme files that can be consulted. The figure below displays all the readme files we found by using Find.

The main one is the one at the top of the list, whereas the others are the individual product readme files.

Name	In Folder	Size
Readme.txt	M:\ntnsm\en	32KB
readme.txt	M:\ntnsm\en\products\adobe	2KB
readme.txt	M:\ntnsm\en\products\citrix	1KB
read.me	M:\ntnsm\en\products\enod\ndis	8KB
readme.txt	M:\ntnsm\en\products\enod\tcpip	12KB
readme.txt	M:\ntnsm\en\products\lotusgo	2KB
readme.txt	M:\ntnsm\en\products\Ncd	1KB
readme.txt	M:\ntnsm\en\products\netscape	2KB
readme.twn	M:\ntnsm\en\products\udc\dos	1KB
readme.txt	M:\ntnsm\en\products\udc\dos	2KB
readme.ipn	M:\ntnsm\en\products\udc\winnt	1KB
readme.twn	M:\ntnsm\en\products\udc\winnt	1KB
readme.txt	M:\ntnsm\en\products\udc\winnt	2KB
readme.txt	M:\ntnsm\en\pubs	2KB

Figure 12. Readme Files on the CD-ROM

Prerequisites are enforced by the installation process, meaning that the installation process does not proceed if a prerequisite is missing. In summary, the software prerequisites are:

1. Windows NT Server 4.0 with Service Pack 3, or Windows NT Server 4.0, Terminal Server Edition, and disk drives formatted with NTFS

**Please Note**

Microsoft Windows NT Service Pack 3 needs to be installed on the Windows NT Server 4.0 *only*; do *not* install Service Pack 3 on Windows Terminal Server Edition.

If the install drive is not formatted as NTFS, you see a message such as the one illustrated in the figure below:



Figure 13. Error Message When Installing on a FAT Drive

2. A Web browser, either Netscape Navigator 4.0.4 or Microsoft Internet Explorer 4.0.1
3. A Web server, either Lotus Domino Go Webserver 4.6.1 or Microsoft's Internet Information Server 4.0

---

## 2.4 Disk Space Requirements

The table below is a summary of the amount of disk space required by the components we install in the plain vanilla sample installation we describe below, using the General Availability version of NSM Release 3.

In summary, approximately 250 MB is required for Windows NT (includes page file space) and 200 MB for the NSM-related code. In total, 500 MB is the minimum amount of space required, and 800 MB is recommended for a Windows NT 4.0 Server environment.

In a Windows NT Server 4.0, Terminal Server Edition environment, 1 GB of space is the recommended size.

**Note:** This is the space required for the base system and the NSM-related products; it does not include the space required by the applications and related components.

*Table 2. Size of Installed Directories*

Component	Approximate Size
Windows NT 4.0 Server + SP 3	140 MB (Note)
Windows NT Server 4.0, Terminal Server Edition	220 MB (Note)
IBM Network Station Manager	150 MB
eNetwork On-Demand Server	18 MB
Lotus Domino Go Webserver	18 MB
Netscape Browser	10 MB
Note: Plus 100+ MB of pagefile space	

---

## 2.5 A Sample Installation

Insert the CD in the drive and you should get the first panel automatically through the autorun facility. If not, you can click on the autorun.exe file located in the ntasm\en\autorun directory.

The first screen allows the choice of the language of installation. This language selection is only for the installation dialogs, and does not represent a choice of the language that the product should use once installed, except in the case of the additional products.

Please refer to Chapter 16, "National Language Support (NLS)" on page 263 for details on language selection.



Figure 14. First Install Screen (Language)

### 2.5.1 Main Installation Selection Panel

The second panel allows you to choose to view the readme file, which you should always do before proceeding, to explore the contents of the CD, to install the IBM Network Station Manager or to install additional products.

These additional products are:

- Netscape Navigator 4.0
- Lotus Domino Go Webserver 4.6.1
- Adobe Acrobat Reader

Listed are also Citrix and NCD, but at the moment, these are only place holders until these products are made available.

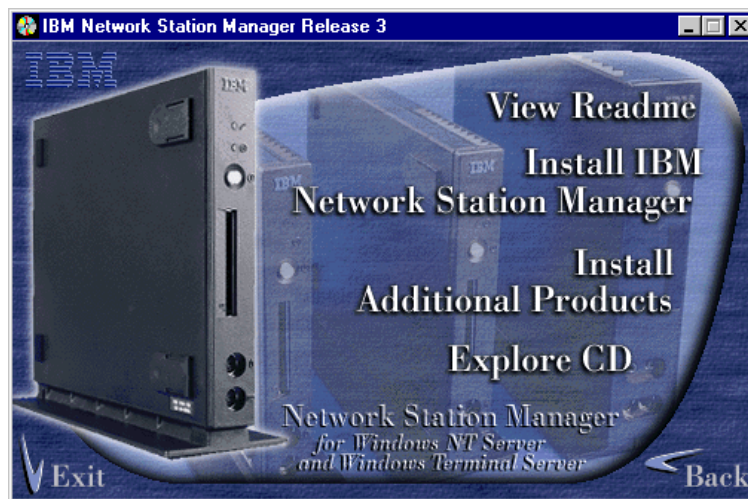


Figure 15. Install Task Selection Screen

We choose to install additional products first since we need the Web browser and Web server prerequisite products.

### 2.5.2 Installation of Netscape Navigator 4.0

On the Additional Products panel shown below, we select **Netscape Navigator 4.0**.

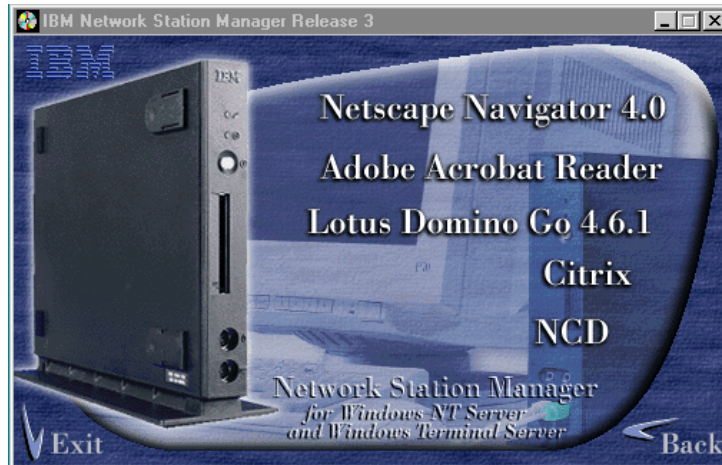


Figure 16. The Install Additional Products Panel

The installation process is very straightforward as there are few decisions to be made. The main decisions are the destination directory and the setup type as illustrated in the figure below:

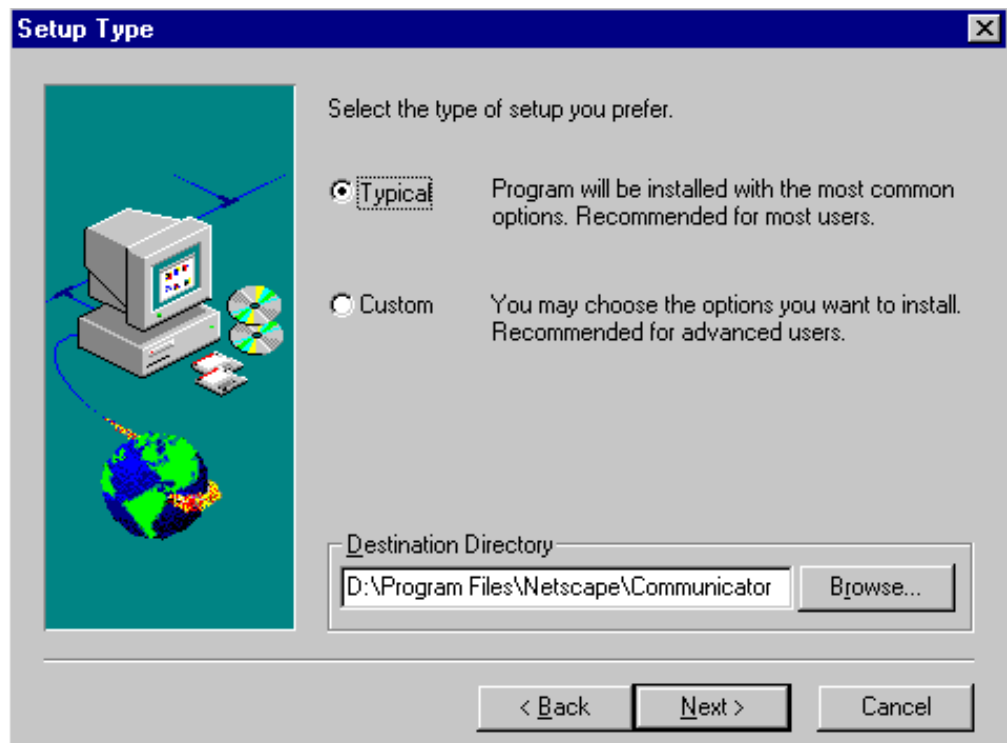


Figure 17. Installation Type and Destination Directory



Once the installation completes, the browser can be started immediately without the need for a reboot.

We suggest that you at least start the browser once before going on with the installation. This creates a profile and allows you to indicate that you want this browser to be the default browser. This is important if you later indicate that you want a shortcut to be created on the desktop for the IBM Network Station Manager because the default browser is the one that is used at the time that the shortcut is created.

### 2.5.3 Installation of Lotus Domino Go Webserver

We then come back to the additional products panel and select **Lotus Domino Go Webserver**.

On the Select Components panel shown below, the first three entries are already pre-selected. Add the Java Servlet selection and click on **Next**.

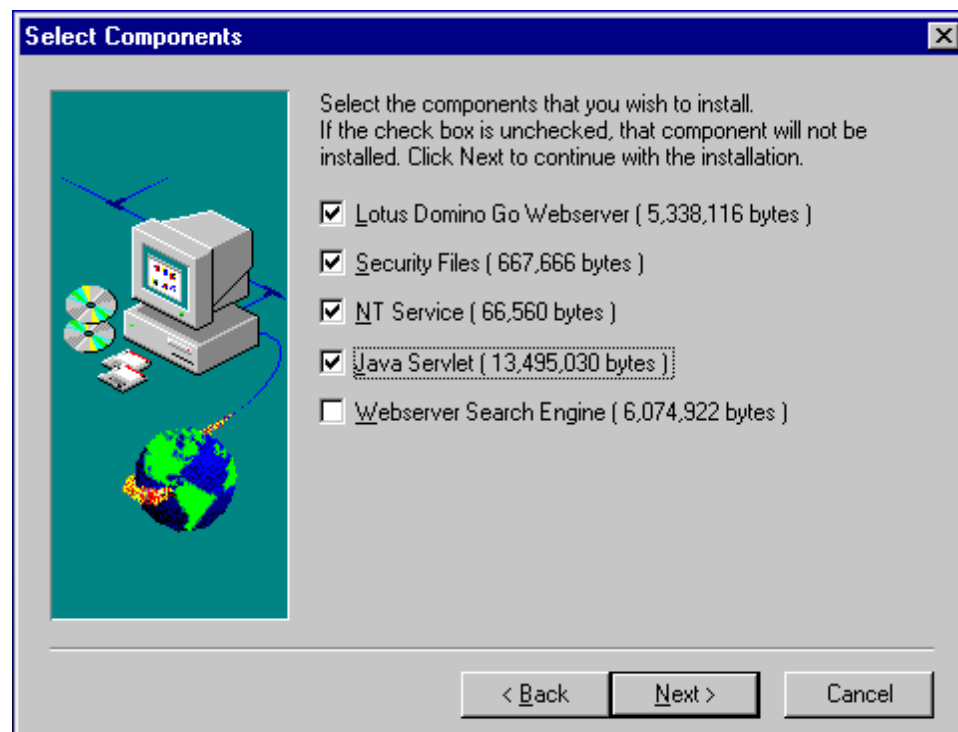


Figure 18. Lotus Domino Go Webserver- Select Components

You are then prompted for an installation directory. In our case, we choose to install on drive H.

The next two panels show the different directories being created, giving you the option to change their location if desired. We accepted the default locations.

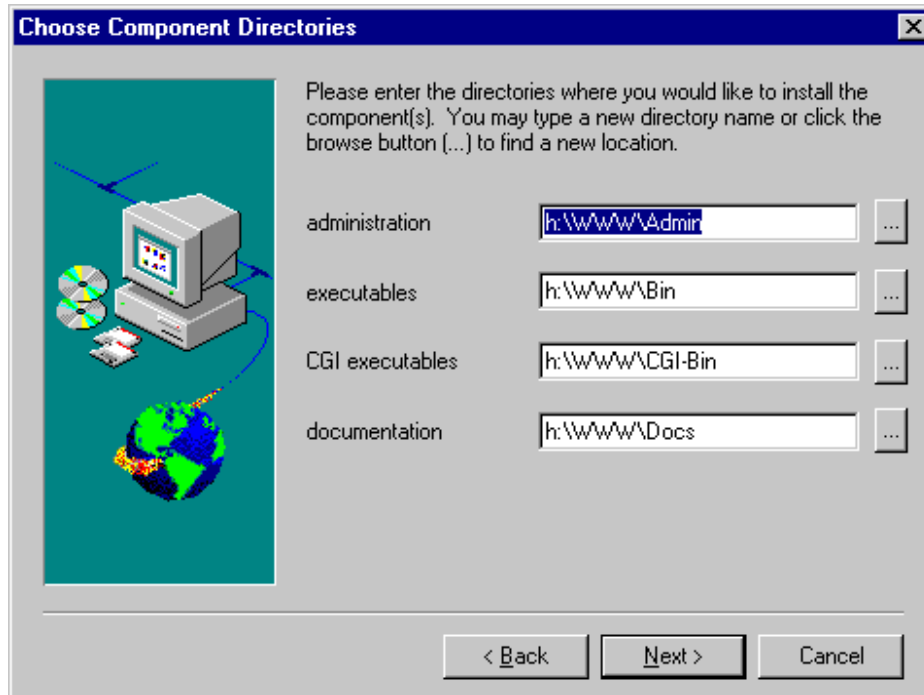


Figure 19. Choose Component Directories (1)

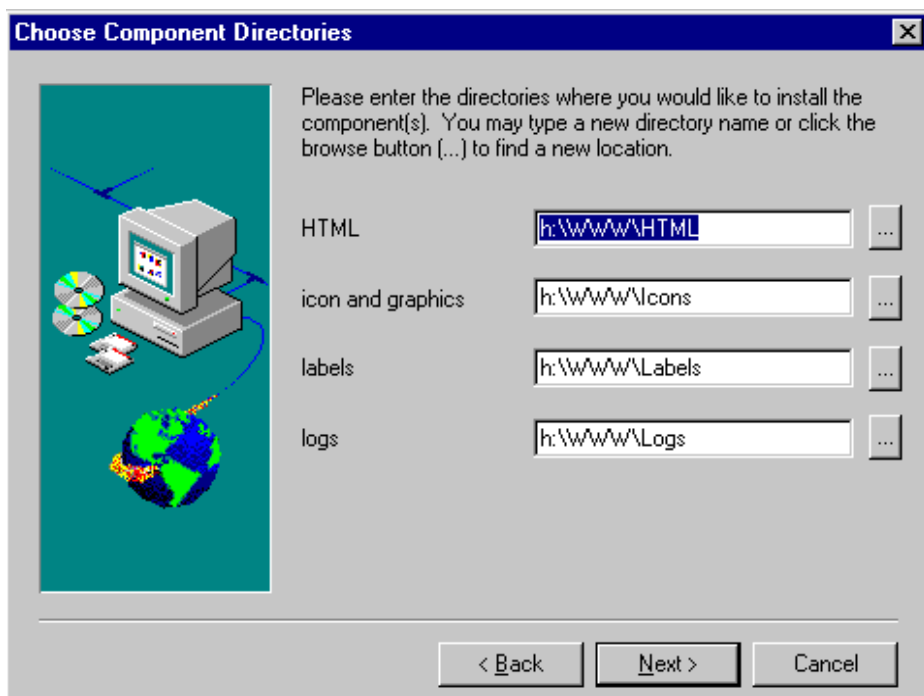


Figure 20. Choose Component Directories (2)

The next panel allows you to change some of the basic configuration data. We accept the defaults and enter our administrator ID and password.

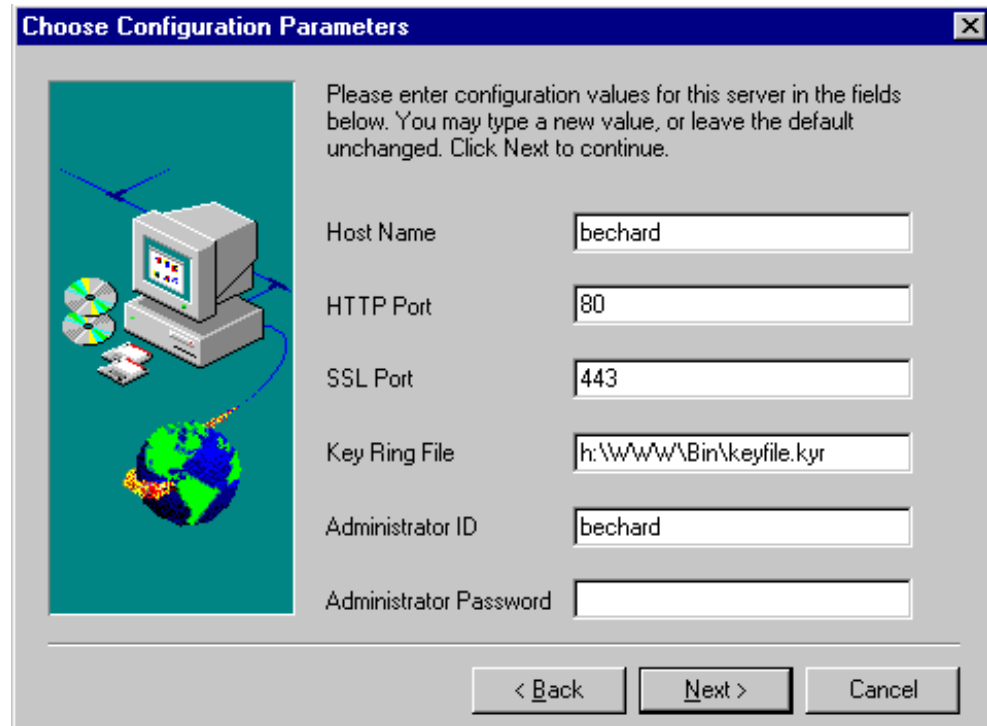


Figure 21. Choose Configuration Parameters

After files get copied, the following message is issued, indicating the completion of the installation.

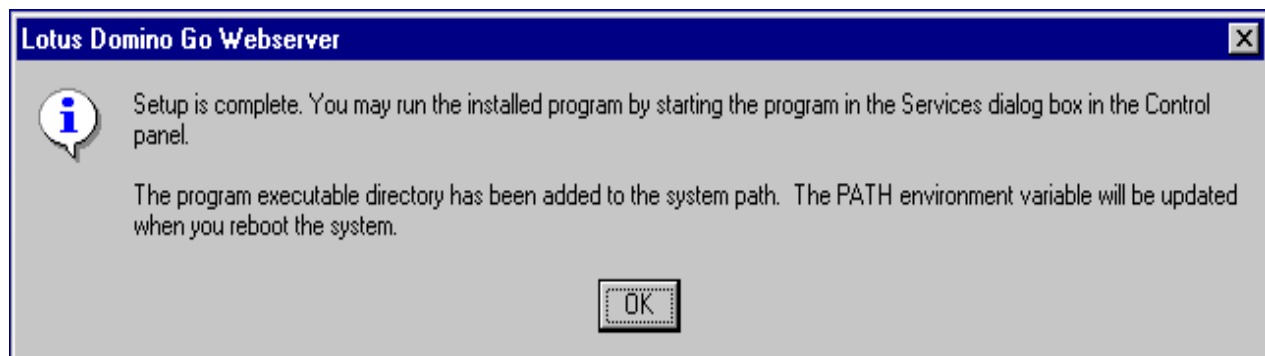


Figure 22. Lotus Domino Go Webserver Completion Message

Notice, as indicated in the message above, that the Lotus Domino Go Webserver is started using the Services dialog in the Control Panel (see 2.6.6, “Lotus Domino Go Webserver Startup” on page 40). In other words, there isn’t an icon in a folder somewhere that you can click to start the Web server; you can only start it by starting the corresponding NT service.

It is not necessary to start the Web server at this time. However, it can be started if you wish to do so.

There is no need to reboot at this time before going on with the other components to install.

## 2.5.4 Installation of IBM Network Station Manager

Back on the main installation screen, we then select **Network Station Manager**, and then **Run Installation** on the next panel.



Figure 23. IBM Network Station Main Install Screen

### 2.5.4.1 Installation Language Selection

The next panel asks for a language selection. This language selection is only for the language used during the installation process dialogs and *not* to select the language that the application will use once installed.

The language that the application uses after installation is automatically determined by the value of the default system locale in the Windows NT Regional Settings.

Please refer to Chapter 16, "National Language Support (NLS)" on page 263 if you require additional details on the subject of installation language.

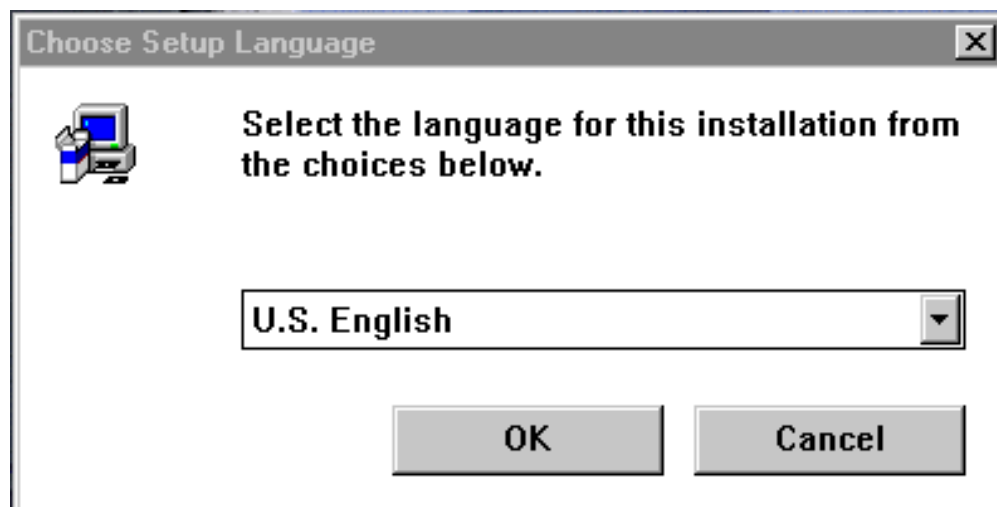


Figure 24. Language Selection for NSM

This is valid for the eNetwork On-Demand Server product as well as for the NSM product.

#### 2.5.4.2 DHCP Server Selection

The message illustrated in the next figure is then issued when the install process does not find the IBM Intermediate Support Driver (previously known as the wedge) required for the IBM DHCP Server.

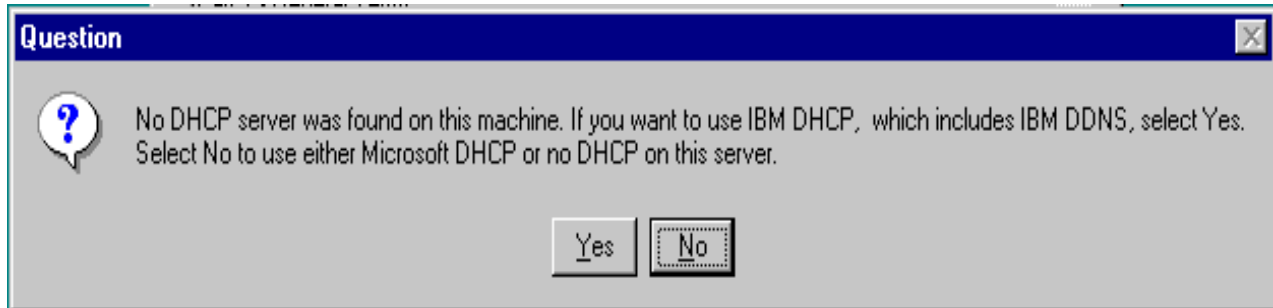


Figure 25. DHCP Selection Panel

You have a choice here of answering Yes if you want to use the IBM version of the DHCP server. Otherwise, answer No if you do not want to install a DHCP server on this machine or if you want to use Microsoft's DHCP server, which you need to install from the Windows NT 4.0 Server CD if it is not already installed.

This does not have to be installed at this time but can be done at any time since there is no direct installation relationship or dependency between NSM and DHCP.

**Note:** There is a read.me file specific to the IBM Intermediate Support Driver in the \ntnsm\en\products\enod\ndis directory on the CD-ROM.

#### 2.5.4.3 Migration Selection

The next panel is used only if you are migrating from a previous version and you need to indicate the location of the user preference files to be migrated. For example, you might specify x:\nstation where x: is a drive mapped to the server on which the old release is installed.

See Chapter 3, "Migration from Release 2" on page 71 for migration scenarios.

In this case, we are not migrating so we leave this blank.

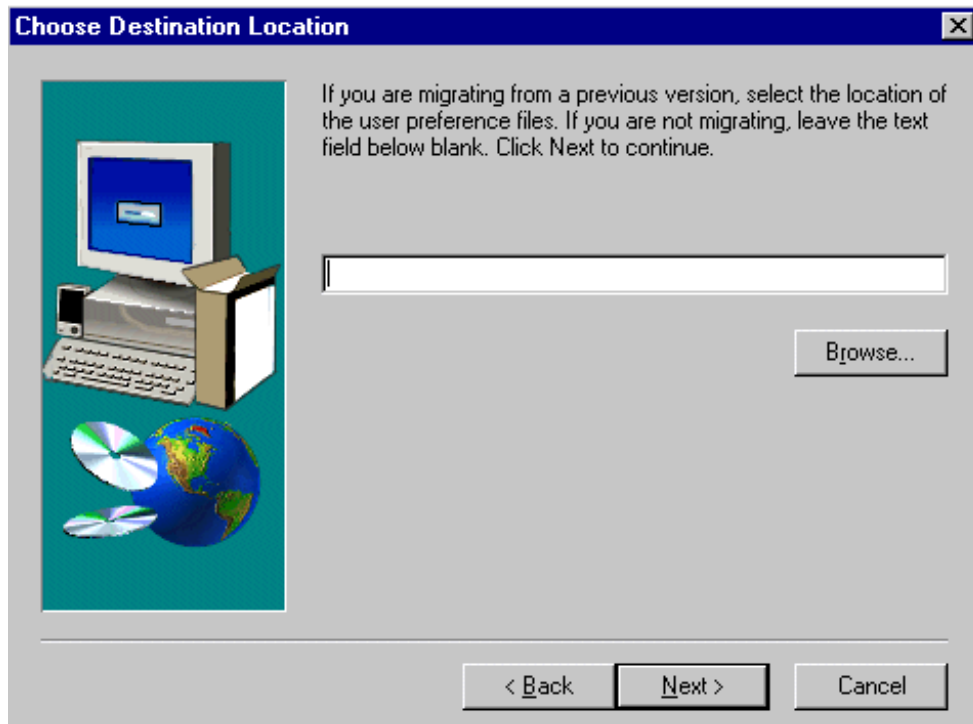


Figure 26. Migration Panel

#### 2.5.4.4 eNetwork On-Demand Server Destination Selection

The next panel indicates that the eNetwork On-Demand Server will be installed. Do not forget to change the drive letter here if you want to install the eNetwork On-Demand Server on a drive other than C:\.

The eNetwork On-Demand Server consists of many components, including the IBM Intermediate Support Driver (previously known as the wedge), the DHCP and DDNS servers, the TFTP server, the TIMED server, the network station login (NSLD) server, the NFS server and the RPC Portmapper server.

**Note:** These components can be installed individually as well by using the specific setup.exe file for the eNetwork On-Demand Server. See the readme.txt file in the \ntnsm\en\products\enod\tcpip directory on the CD-ROM for more details.

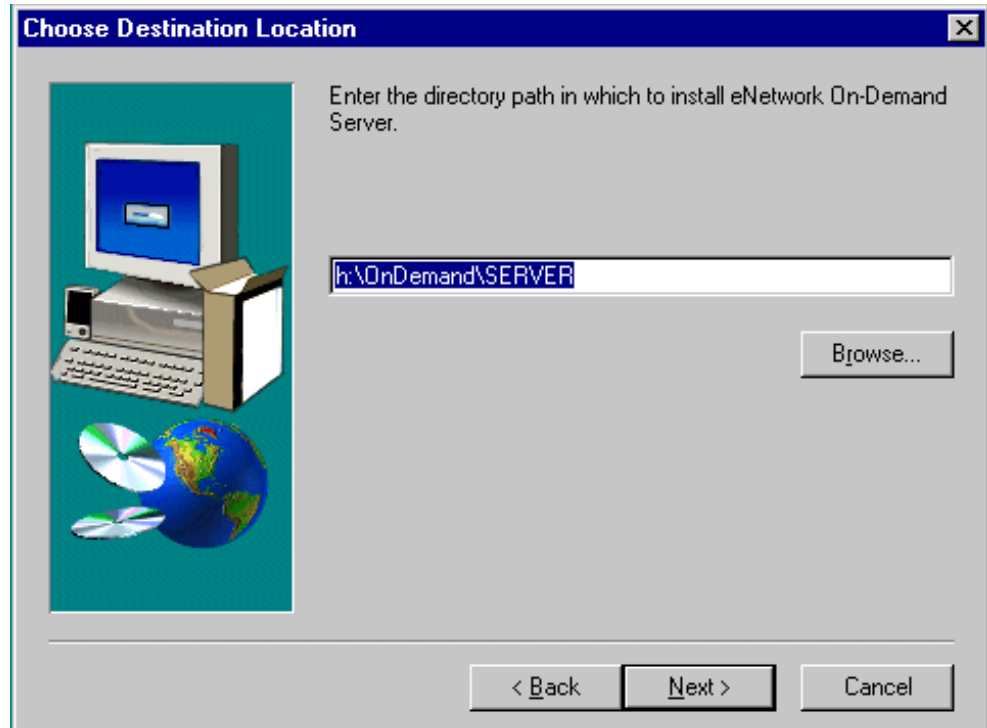


Figure 27. Destination Directory for the eNetwork On-Demand Server

#### 2.5.4.5 NC Navigator Selection

The next panel is presented only in the North American version of the CD-ROM. For the International version of the CD, this question is not asked and the 40-bit NC Navigator product is installed automatically.

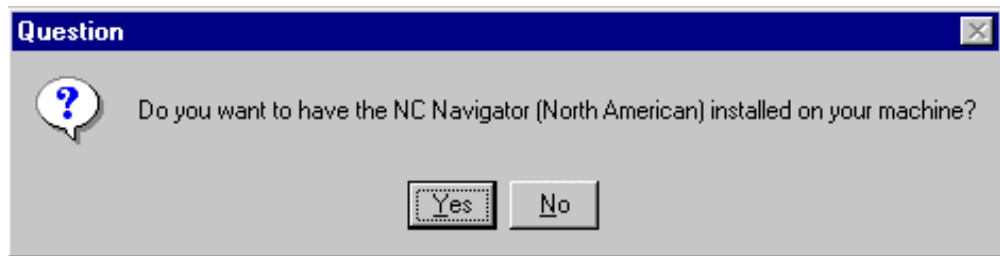


Figure 28. NC Navigator Question

On the North American version of the CD however, there are two choices:

1. Answer No if you only need the standard 40-bit NC Navigator browser, and therefore do not need to install the more secure version of the browser.

This is because the 40-bit NC Navigator browser is, by default, part of the IBM Network Station Manager install. (In other words, it is installed whether you want it or not.)

2. Answer Yes if you want to install the more secure version of the browser.

In other words, the more secure version is also present on the CD but is installed only if you answer Yes to the prompt illustrated in Figure 28 on page 31.

**Note:** For the International version of the CD, only the 40-bit version is present on the CD and therefore, this question is not asked.

If you answer Yes, the 128-bit version of the browser is installed (in addition to the 40-bit version) and it also needs to be manually enabled by adding an environment variable using the IBM Network Station Manager and setting its value to TRUE. The name of the environment variable to add is NAV\_128SSL.

Since the environment variable can be configured for the system, group or user, you can have certain users use the 40-bit version and you can have others use the 128-bit version if desired.

Remember that this is now the only browser available since the IBM Network Station browser that was available in the previous versions has been discontinued.

#### 2.5.4.6 Final Check

A final screen simply lists the components that are about to be installed as a final check before launching the copying of files.



Figure 29. Summary of Products to Be Installed

#### 2.5.4.7 Shortcut Icon Selection

You are then asked if you want the installation to create a shortcut for you on the desktop, which allows you to start the IBM Network Station Manager directly from the desktop on the server. You can always create this shortcut yourself later on if you need to.



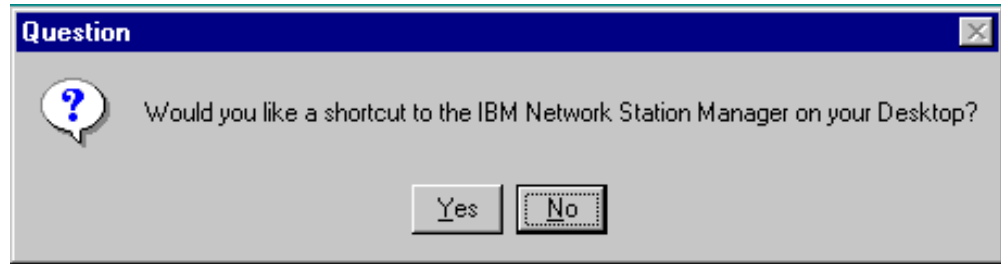


Figure 30. Desktop Shortcut Creation Question

#### 2.5.4.8 Progress Feedback

You then get a series of progress panels that provide feedback on the main actions that are taking place, such as the one illustrated below:

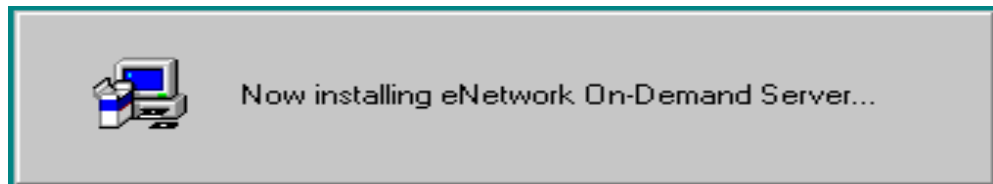


Figure 31. Installation Progress Feedback

#### 2.5.4.9 Completion

The last panel is the one shown below, identifying the completion of the install process, at which time you can click **Finish** to let the system reboot.

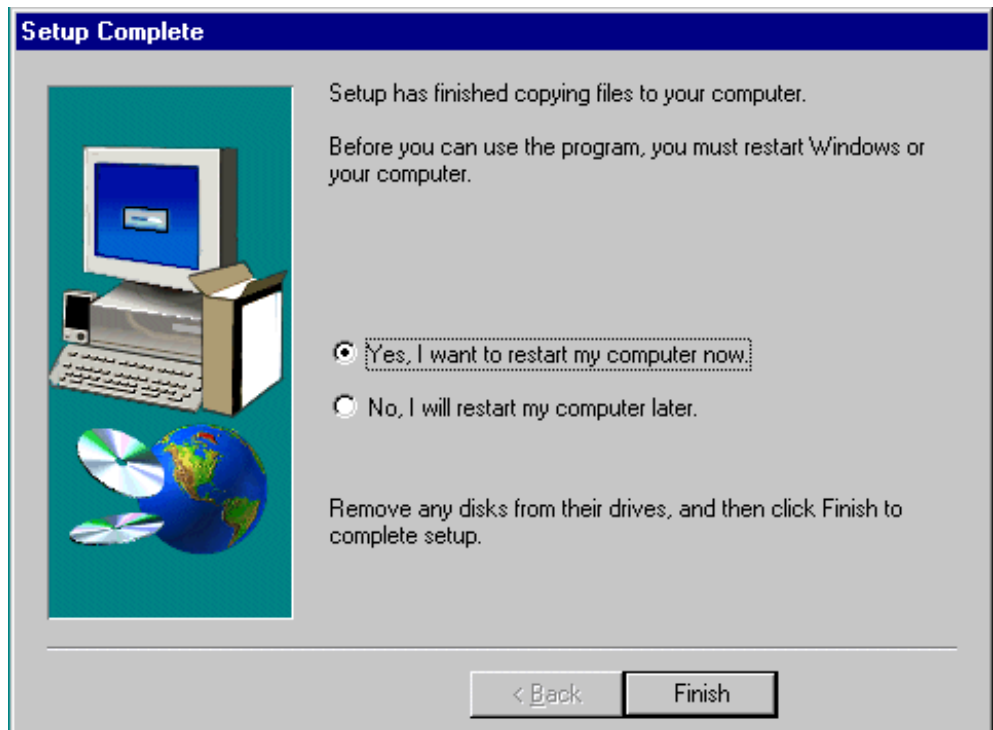


Figure 32. Install Completion Screen

## 2.6 Installation Notes

We provide here a few miscellaneous installation-related notes to provide additional insight into the installation process. These might be useful in cases where problems are encountered during or after installation.

### 2.6.1 Installation Verification

If you need a quick visual confirmation that your installation was done properly and that you have all the required components, the following sections discuss a couple of things that you can verify.

#### 2.6.1.1 The Add/Remove Programs Properties

The Add/Remove Program list should now show the following installed products:

- IBM eNetwork On-Demand Server
- IBM Network Station Manager
- Lotus Domino Go Webserver
- Netscape Navigator 4.04
- NC Navigator

The list is illustrated in the next figure. Some of the labels might be different if you do not have the North American version.

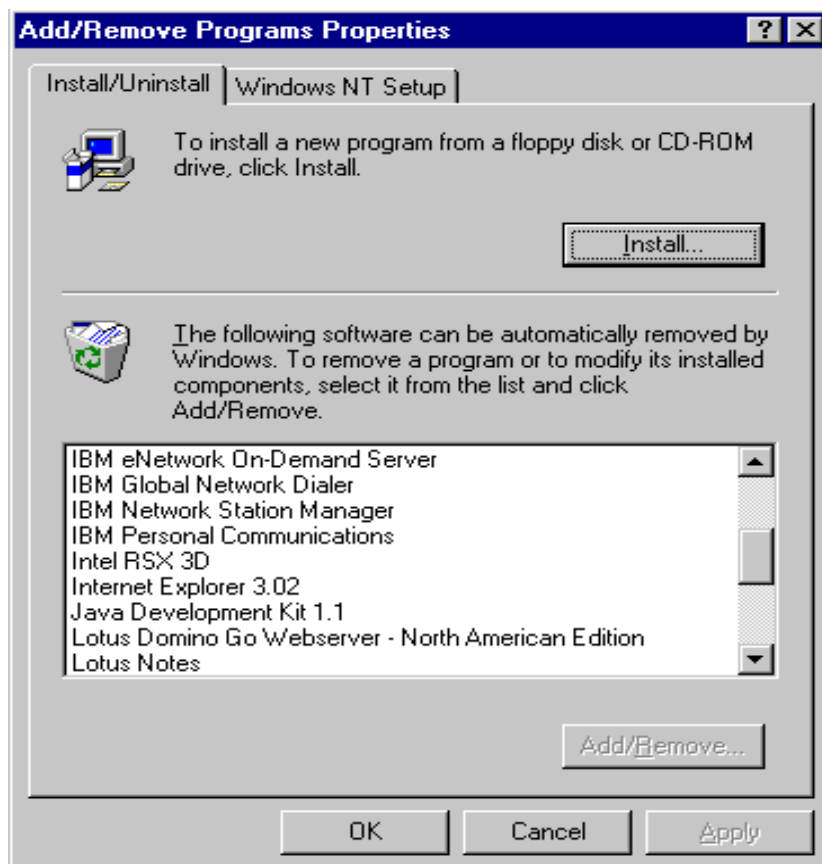


Figure 33. Add/Remove Programs after Installation

### 2.6.1.2 The Installed NT Services

The Services panel should display the NT services illustrated in the figure below:

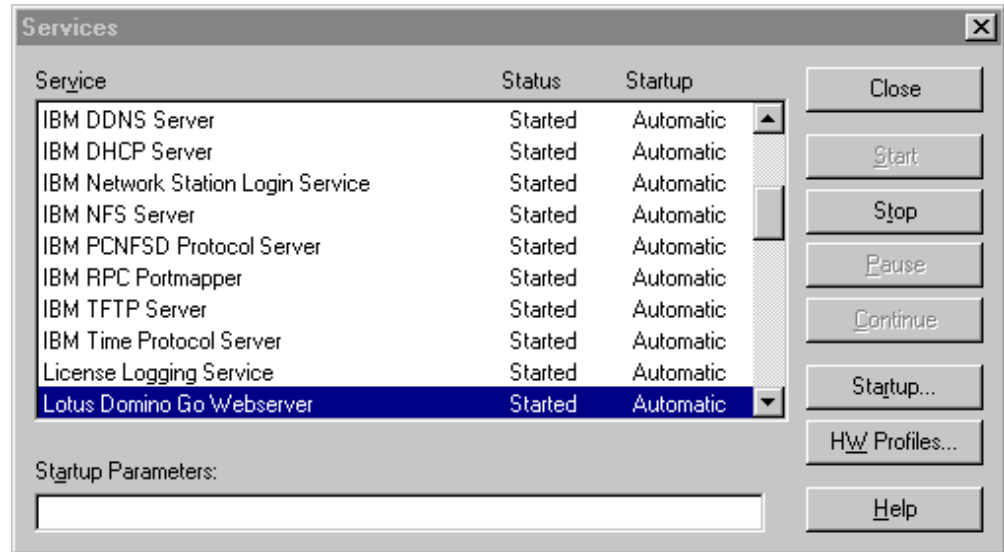


Figure 34. Installed Services

The fact that all these services have a status of Started is probably the best indication that the installation was successful. If there was a problem with the installation, it is probable that one or more of these services would not be able to start correctly.

The IBM DDNS and IBM DHCP Server services may not appear in this list if you chose to use the Microsoft DHCP Server instead of the IBM DHCP Server. However, all the other services whose names start with IBM in the above list are required.

## 2.6.2 Types of Windows NT Server Installations

With this release of the IBM Network Station Manager, you can install on:

- A primary domain controller (PDC) - This is not recommended.
- A backup domain controller (BDC) - This is not recommended.
- A stand-alone server attached to a domain (SAD) - Recommended.
- A stand-alone server - Recommended.

Installing on a PDC or BDC is not recommended because these types of servers should normally be dedicated to being domain controllers, and nothing else.

However, installing on a PDC remains possible since PDC was the recommended install (initially) for NSM Release 2, an existing PDC server that is migrated from Release 2 to Release 3 has to remain a PDC, since you can only change a system to a non-PDC or non-BDC system with a re-installation of the base Windows NT system.

### 2.6.3 Creation of NSMAdmin and NSMUser Groups

The NSMAdmin and NSMUser user groups created by the installation process are always created on the local server (except in one case, which is for an installation on a BDC, in which case these user groups are created on the PDC).

If your IBM Network Station users are already defined on a PDC, these users must be made members of the local NSMUser group on the server where they log on to.

If all these users are already part of a global group on the PDC, then the easiest and fastest way to include them in an NSMUser local group on a stand-alone server is to make the domain's global group a member of the stand-alone server's NSMUser local group.

For example, assume we have users user1 and user2 defined on the NSDOMAIN PDC as members of a global group called NSMACCT. We want to give these users the ability to log on to the server1 server.

When these users were defined on the PDC, they were made part of a global group called NSMACCT on the PDC, as illustrated in the next figure, which displays the Global Group Properties on the NSDOMAIN domain PDC:

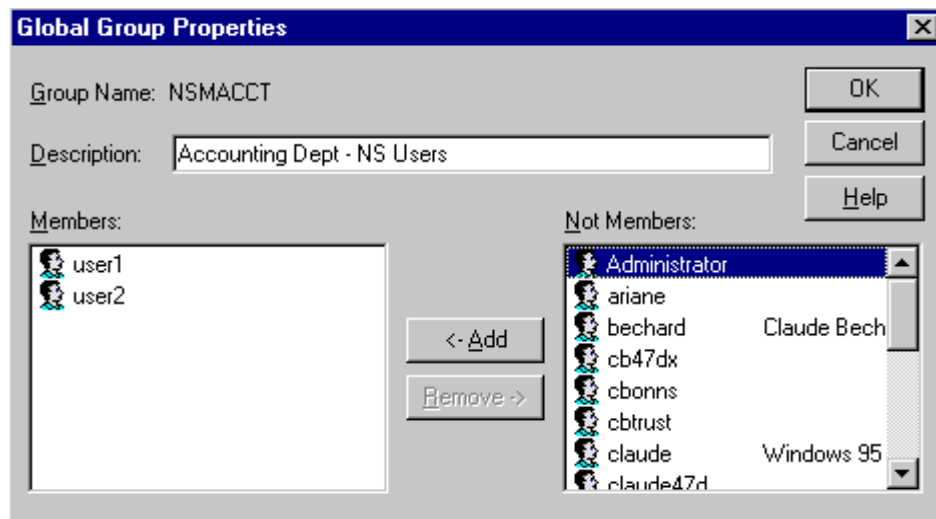


Figure 35. Creating an NSMACCT Global Group on a PDC

On the server1 server, we use the User Manager for Domains, and bring up the NSMUser group, which is a local group created on the server1 server, as shown below:

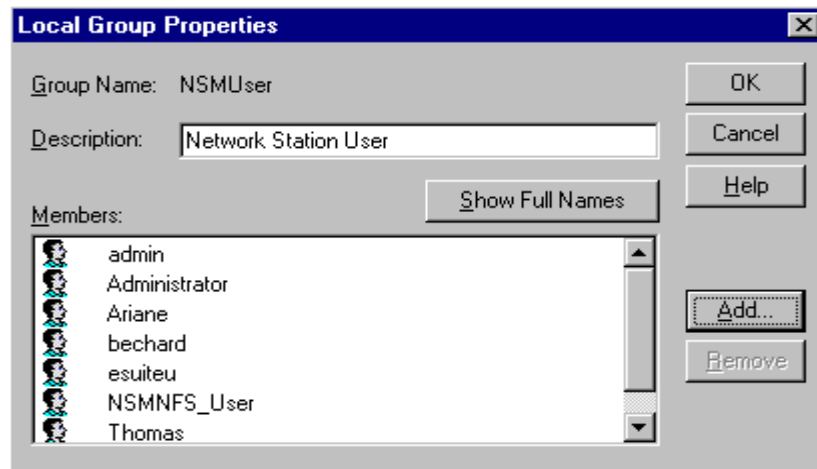


Figure 36. Local Group Properties

On the panel above, we then click on the **Add** button, which brings up the next panel entitled Add Users and Groups:

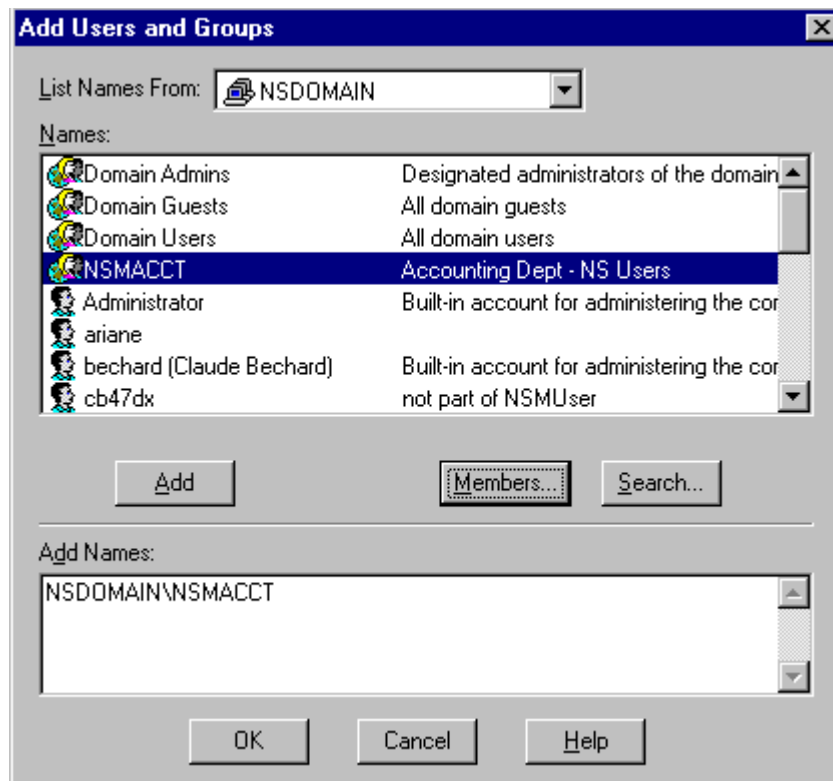


Figure 37. Add Users and Groups

On the above panel, notice that we have selected, in the field labeled List Names From: at the very top of the panel, **NSDOMAIN**. The list of names that gets displayed is from the NSDOMAIN PDC.

We select the **NSMACCT** group from the list and click on **Add** so that the \\NSDOMAIN\NSMACCT entry appears in the bottom portion of the window,

indicating that we are adding the NSMACCT global group from the NSDOMAIN to our local group NSMUser on the server1 server.

Instead of including the group, we could of course add the individual domain users \\NSDOMAIN\\user1 and \\NSDOMAIN\\user2.

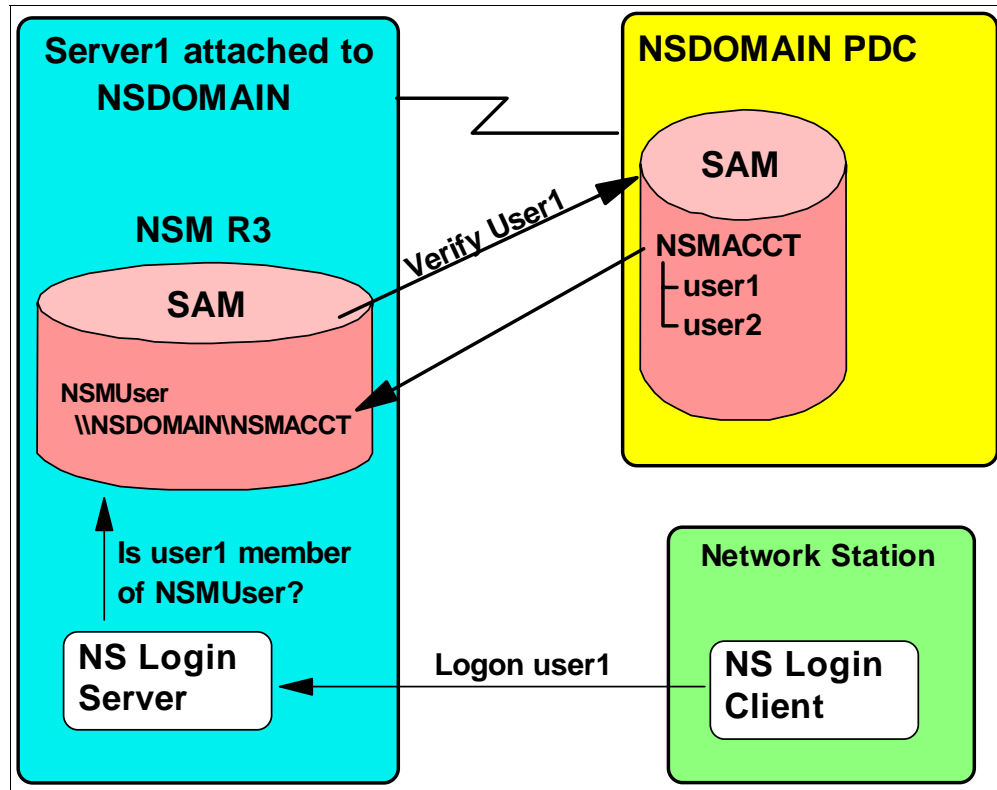


Figure 38. NSMUser Group on Local Server

## 2.6.4 Re-Installation and Update

If for some reason you need to re-install a fresh copy of the IBM Network Station Manager, you must first perform a full uninstall before initiating a re-install. There is no refresh capability such that you can ask for all the modules to be refreshed without having to do an install.

If you attempt to re-install without first uninstalling, the install process will notify you that you must uninstall first, and offer to launch the uninstall process.

**Note:** Launching the uninstall process from within the install process is not the same as doing a stand-alone uninstall from the Add/Remove programs. The reason is that the install process saves registry information and saves the location of destination directories before launching the uninstall and restores this information before resuming the install after the uninstall completes.

In the case of a service update, for example, installing NSM 3.02 (Service Update #2) on top of NSM 3.0 (the GA level), you initiate the process just as if you were re-installing; the install process detects the level that is installed and knows that it should only perform an update instead of an installation.

In that case, the install process informs the user that a service update needs to be applied by displaying a panel as illustrated in the next figure:

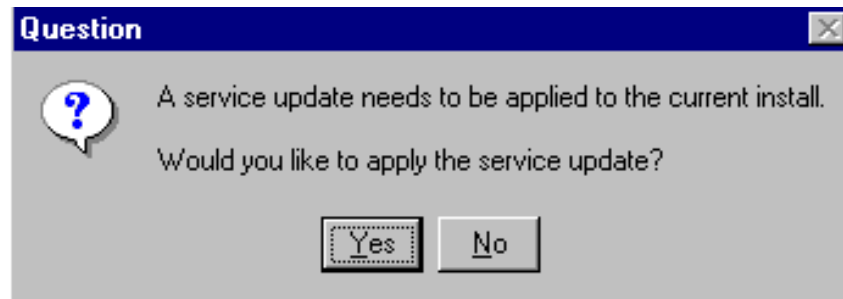


Figure 39. Service Update Message

After you answer **Yes** on this panel, the next panel displayed to the user shows the components that are to be installed as part of the service update.

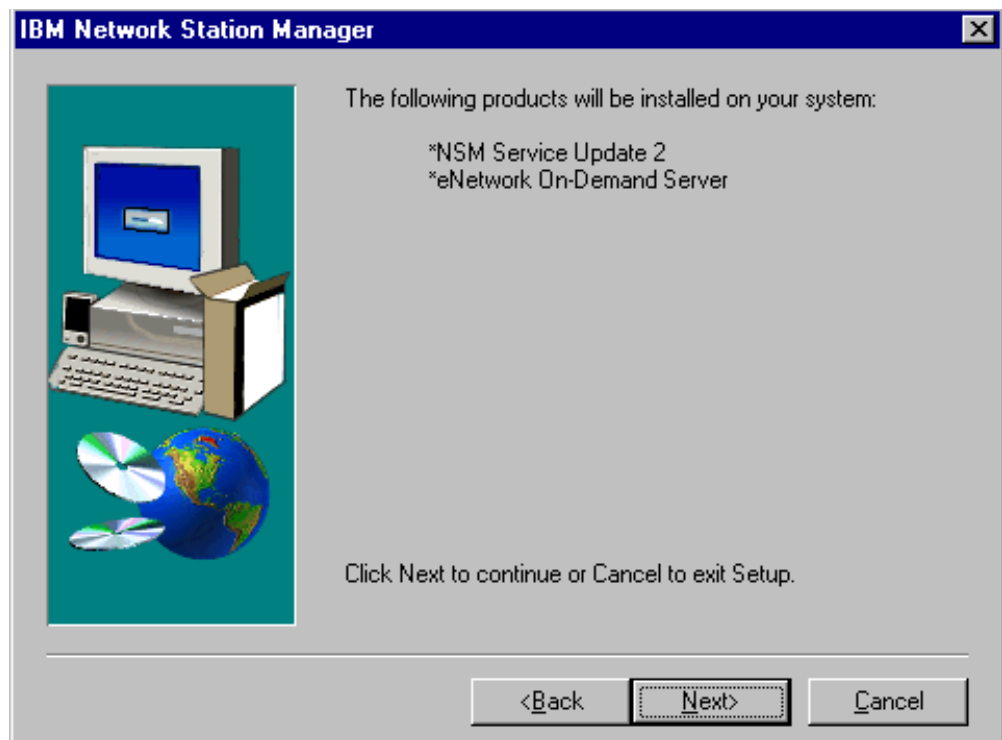


Figure 40. Service Update Message (2)

### 2.6.5 Desktop Shortcut for the IBM Network Station Manager

The install process offers to create, on the desktop, a shortcut that is used to launch the IBM Network Station Manager. The browser selected as the target by the shortcut is the browser that is the default browser at the time of installation.

If you change browsers afterwards, you need to manually modify the properties of the shortcut to point to the new browser, as illustrated in the figure below. This is done by right-clicking on the shortcut and selecting **Properties**.

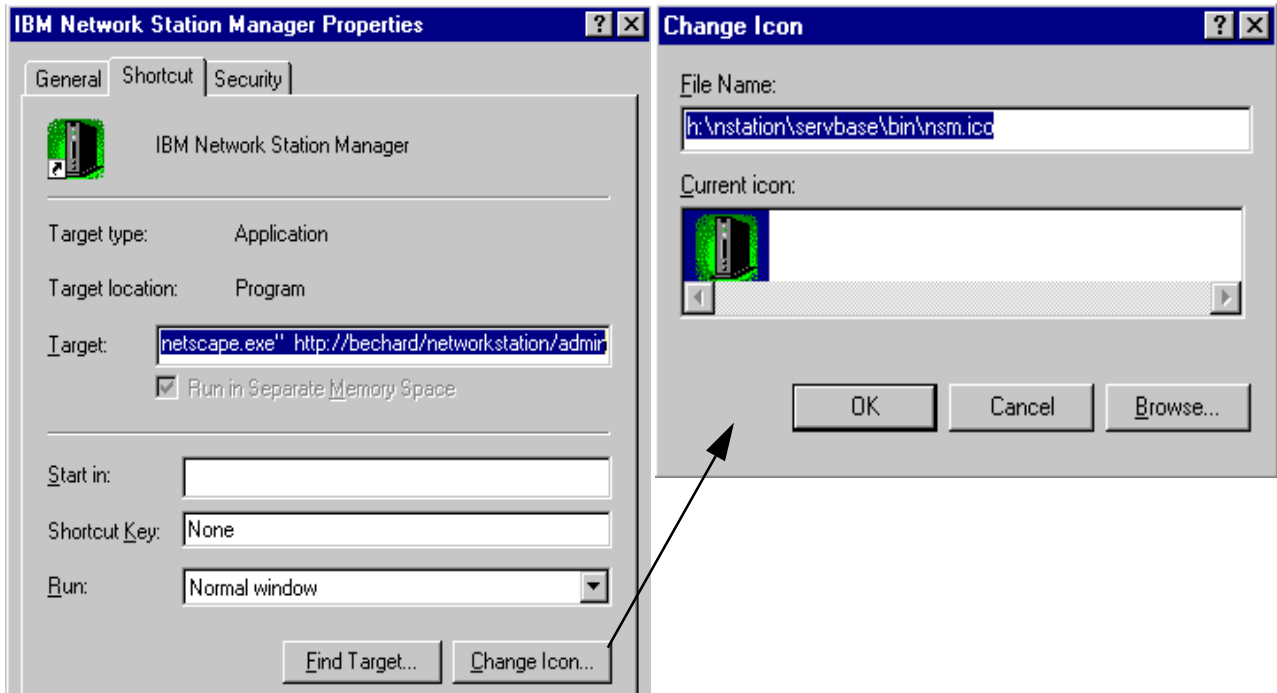


Figure 41. The IBM Network Station Manager Desktop Shortcut Properties

## 2.6.6 Lotus Domino Go Webserver Startup

If you examine the startup information for the Lotus Domino Go Webserver NT service, it should appear as automatic startup, which means that it should be automatically started after a reboot.



Figure 42. Lotus Domino Go WebserverService Startup



If you want to see the operations screen displayed on the desktop, then also select the **Allow Service to Interact with Desktop entry**, as illustrated in the figure above.

The next time you boot, the service gets started automatically (or if you want you can start it manually now using the Start button) and you should see on the desktop (assuming that you selected Allow Service to Interact with Desktop) a display as illustrated in the figure below:

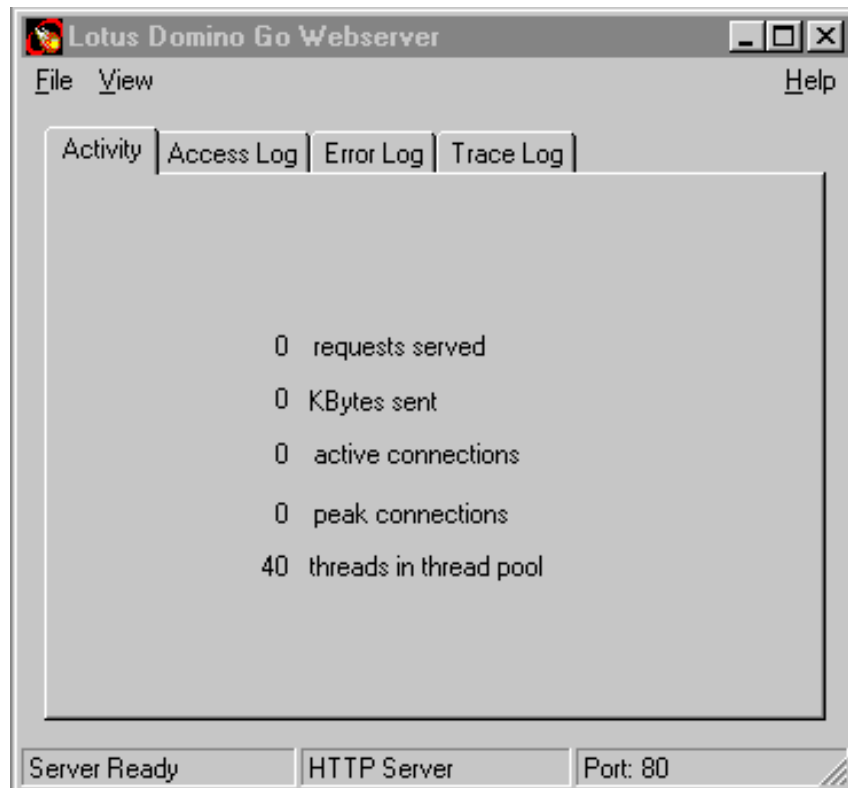


Figure 43. Lotus Domino Go Webserver Status Panel

This is a kind of status panel displaying activity statistics. Notice the bottom left-hand corner box which displays Server Ready, indicating that the Web server is indeed operational.

**Note:** If you install the Lotus Domino Go Webserver on Windows NT Server 4.0, Terminal Server Edition, the status panel shown in the above figure is not displayed on RDP clients. It is only displayed if you are logged on at the real console of the server.

Selecting the **Error Log** tab displays any error messages that were issued since startup, as shown below:

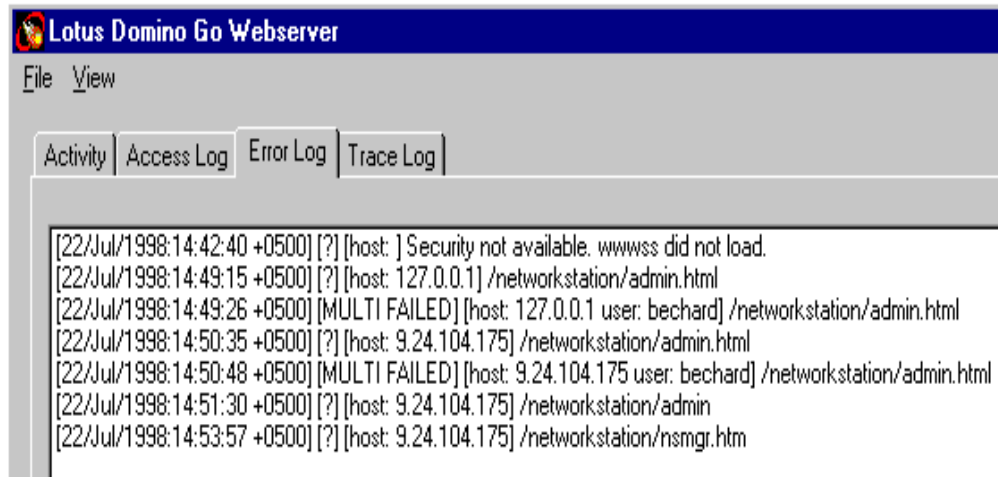


Figure 44. Lotus Domino Go Webserver Error Log

### 2.6.7 The Lotus Domino Go Webserver Configuration File

The main configuration file for the Lotus Domino Go Webserver is named `httpd.cnf` and it resides in either the `x:\winnt\` directory or in the `x:\rsant\etc\` directory.

This configuration file is updated by the IBM Network Station Manager installation process in order to add the required directory entries allowing access to the IBM Network Station Manager application from a Web server.

The only way to have these entries created automatically is to run the NSM install process. If for any reason you need to recreate these entries without a re-install of the NSM, they can be added manually using an editor.

The figure below identifies the four entries that are added by the NSM installation process and where these entries are located. The example used here is for an installation on the `D:\` drive:

Locate the line

"# NOTE: The installation defaults should be added below"  
which should be about line 1201 in the original httpd.conf file,  
and add the following two Exec statements after it:

```
Exec /networkstation/admin d:\nstation\servbase\cgi-bin\nsmcgain.exe  
Exec /networkstation/cgi/* d:\nstation\servbase\cgi-bin\*
```

Locate the line

"# \*\*\* ADD NEW PASS RULES HERE \*\*\*"  
which should be about line 1210 after the previous additions,  
and add the following Pass statement after it:

```
Pass /networkstation/* d:\nstation\servbase\html\*
```

After the last line, add the following statement:

```
Authorization /networkstation/* d:\nstation\servbase\bin\nsmgauth.dll:nsmGoAuth
```

Figure 45. Adding NSM Configuration Entries to HTTPD.CNF

Note that if you install NSM on the d: drive, during which the httpd.conf file gets updated as shown above, and then later on remove NSM and re-install on an E: drive, the statements in the httpd.conf configuration file get correctly updated during the re-install of NSM to indicate E:\ as the NSM install drive.

Once these statements have been added, you can either stop and restart the Webserver using the NT Services panel, or you can also use the Restart function on the desktop panel, as illustrated below.

The restart causes the Webserver to reread its configuration file.

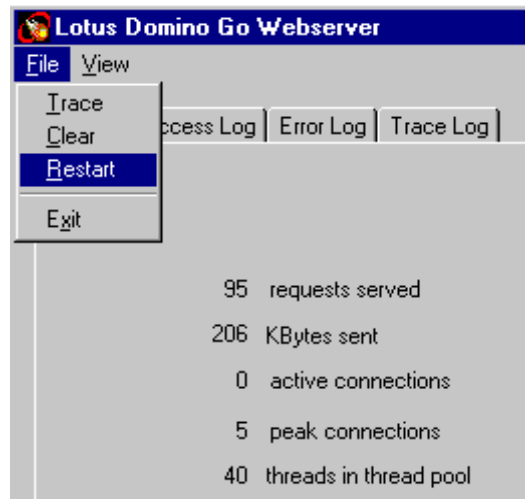


Figure 46. Restart the Lotus Domino Go Webserver after Altering httpd.conf

## 2.6.8 Microsoft IIS 4.0 Web Server

If the installed Web server is Web Server IIS 4.0 from Microsoft, you should see a virtual directory called **networkstation** added to your virtual directories and pointing to `x:\nstation\servbase\html`, as illustrated in the next figure:

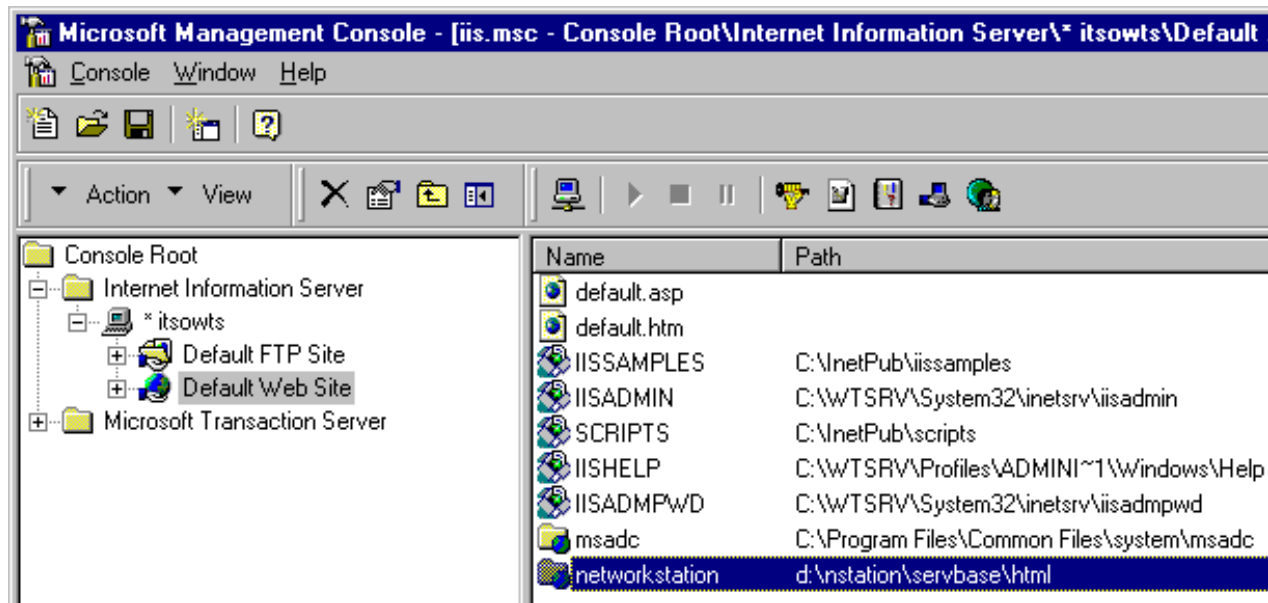


Figure 47. Updating Microsoft's IIS 4.0

If you examine the properties for this entry by right-clicking on the **networkstation** entry and selecting **Properties**, you get the following display:

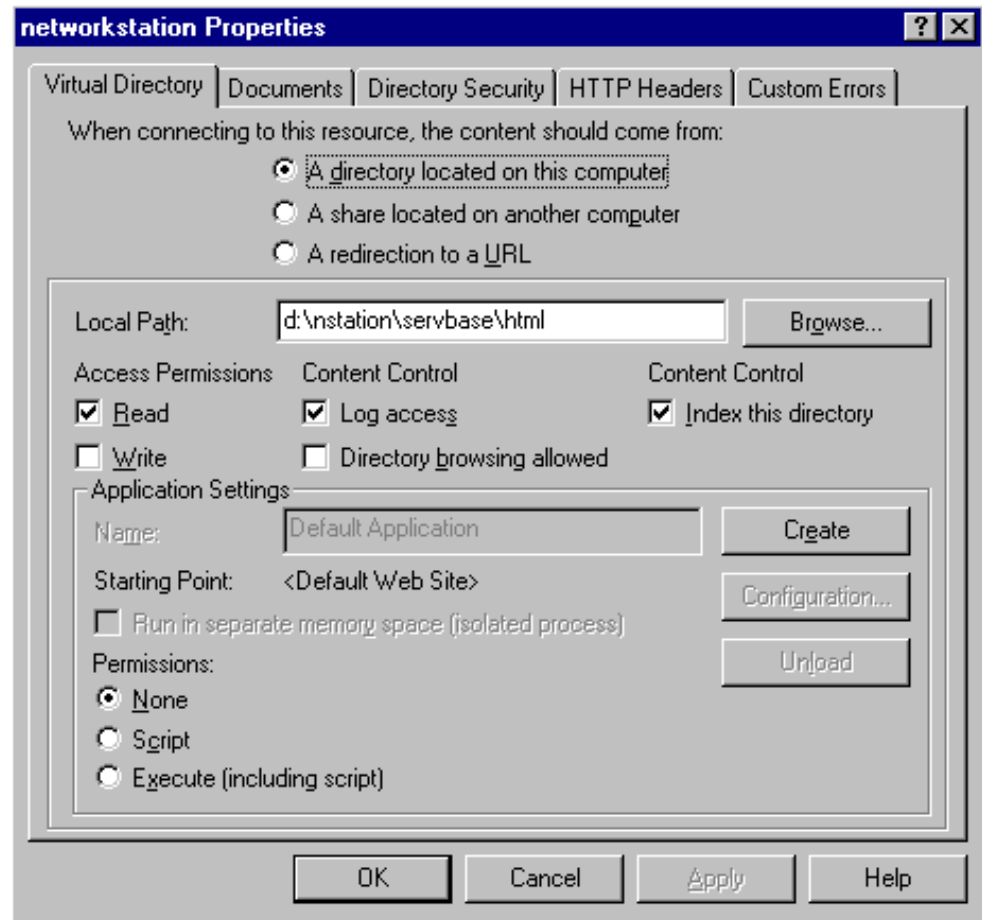


Figure 48. Properties for the networkstation Virtual Directory

If you click on the **Documents** tab, you can view what the default document is, which in this case is admin.htm, which is the main panel for the IBM Network Station Manager application.

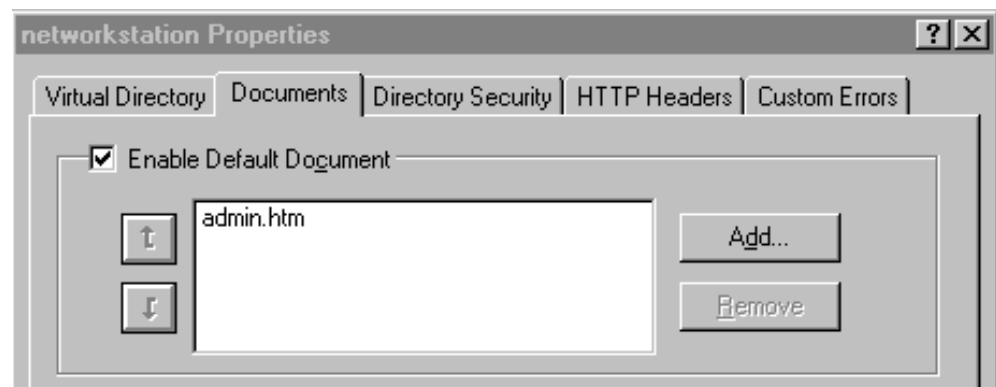


Figure 49. Default Document - IIS 4.0

**Note:** Interestingly, if you happen to have both the IIS 4.0 and the Lotus Domino Go Webserver installed (which would probably be unusual) the IBM Network Station Manager installation process updates both products with the entries required by NSM. In our test environment, we could therefore easily switch from

one Web server product to the other just by shutting down one of them and starting the other.

---

## **2.7 Documentation**

We identify here where the online documentation for the products that were installed is located.

### **2.7.1 IBM Network Station Manager**

The documentation for the IBM Network Station Manager is accessed through the online help on any of the IBM Network Station Manager panels.

There is always a Help button located at the bottom right-hand corner that can be used to bring up the panel in the next figure.

The frame labeled Contents on the left-hand side of the panel always displays the contents that can be accessed, but what appears on the right-hand side depends on the task that you were performing at the time that you clicked on the Help button, so that you are automatically positioned at the help text for the task that you were in the process of completing.

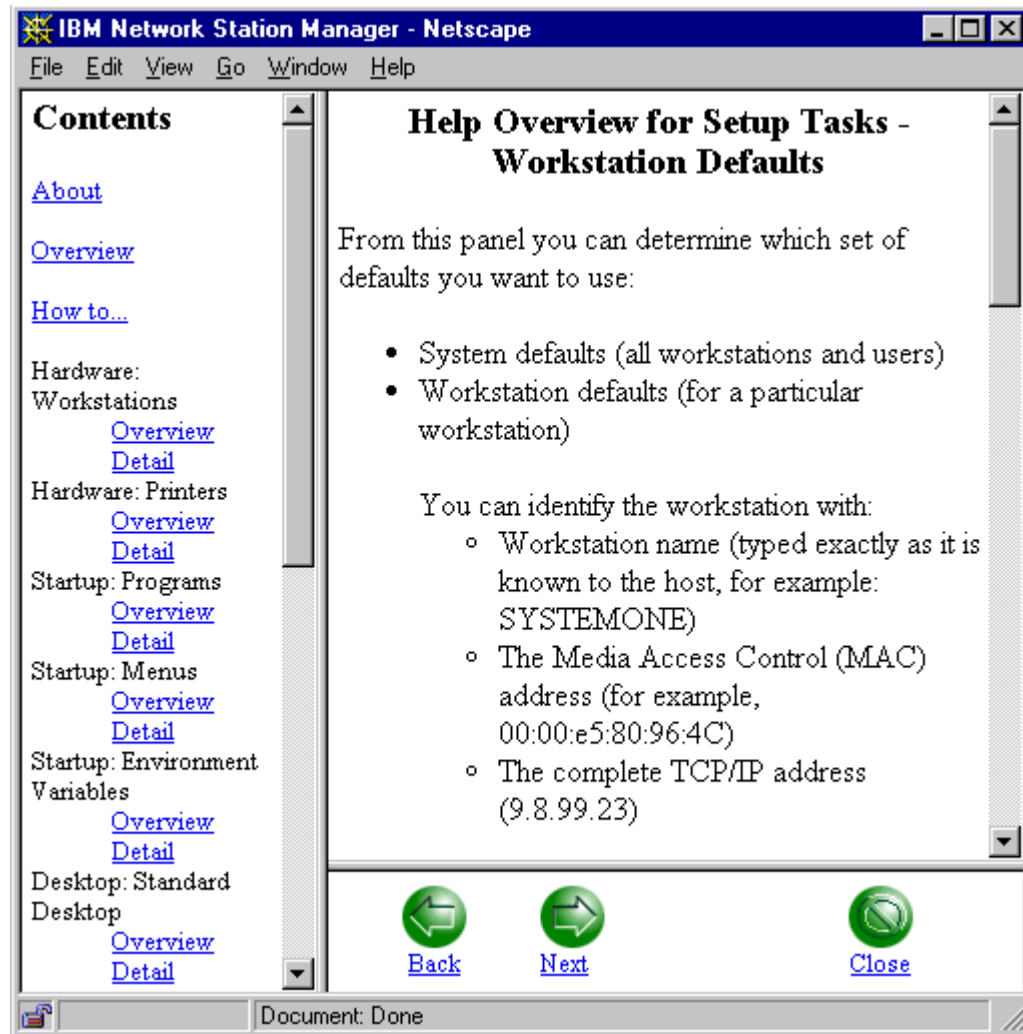


Figure 50. IBM Network Station Manager Online Help Facility

## 2.7.2 eNetwork On-Demand Servers

The documentation for the eNetwork On-Demand Servers is accessed by clicking on **Start=>Programs=>eNetwork On-Demand Server=>Documentation**.

It is HTML-based and the master file called by this shortcut is located at `x:/OnDemand/SERVER/NsmInst/HTML/OnDemand/en/mtocmst.htm`.

The primary panel displayed is as shown in the next figure.

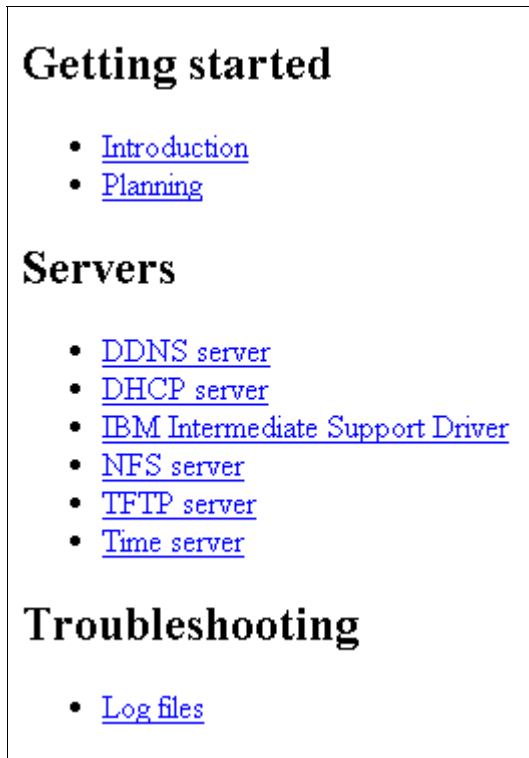


Figure 51. eNetwork On-Demand Server Online HTML Documentation

### 2.7.3 Lotus Domino Go Webserver

The documentation for this product is accessed through your browser. By default, when the product is installed, the default main page is the Lotus Domino Go Webserver page.

So, if you point your browser on the server at the loopback interface 127.0.0.1 you get the following panel:



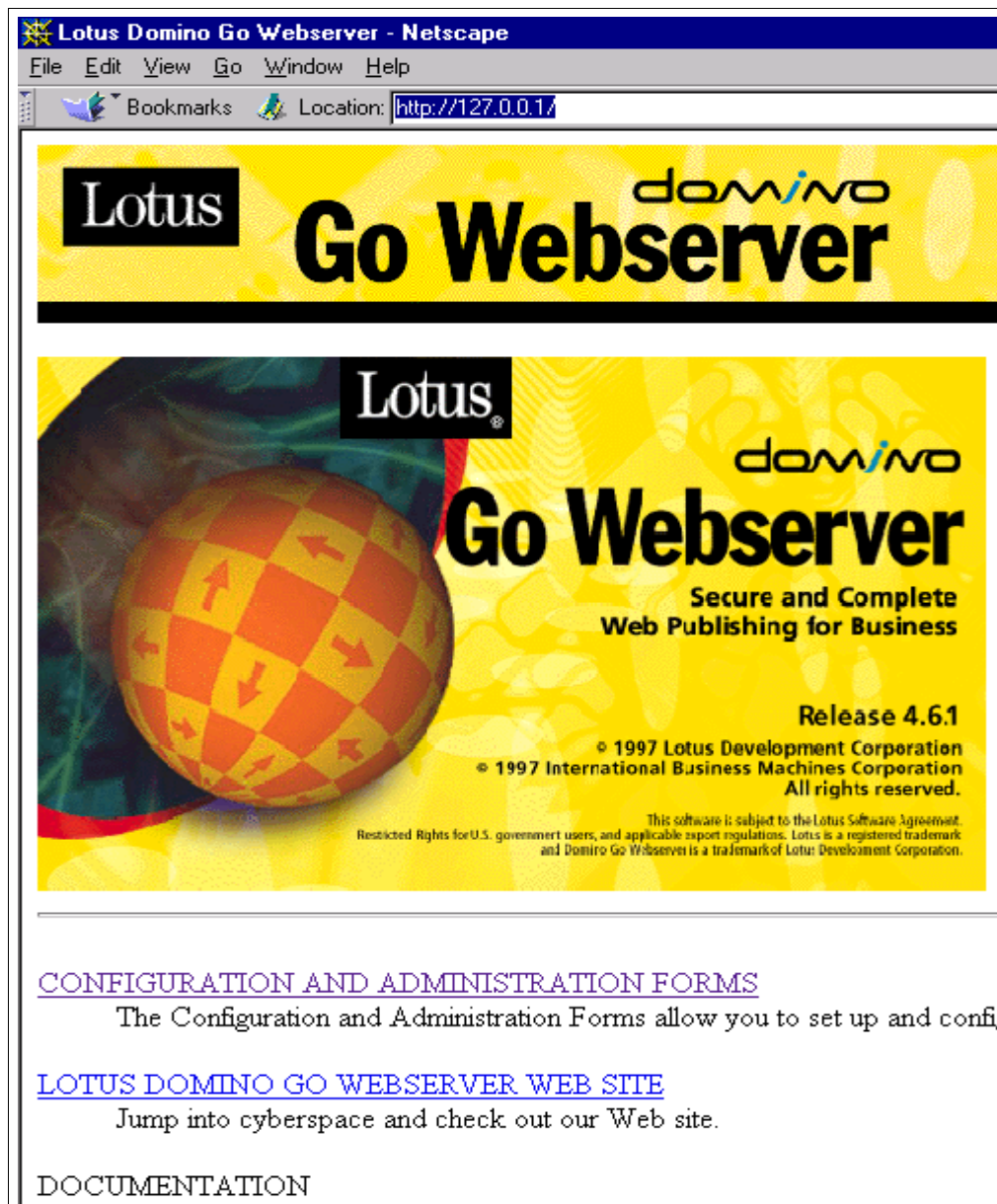


Figure 52. The Lotus Domino Go Webserver Main Page

The last line on this panel, labeled Documentation, lists the following entries:

## DOCUMENTATION

Hypertext versions of the following books that you can read with your Web browser.

- Quick Beginnings in [HTML](#) or [PDF](#)
- Webmaster's Guide in [HTML](#) or [PDF](#)
- [Web Programming Guide](#)
- [Webserver Search Engine Installation](#)
- [Webserver Search Engine Administration](#)
- [JIE Developer's Guide](#) (for Windows NT only)
- [Tuning Your Webserver for Better Performance](#)
- [Additional documentation](#) on the Lotus Domino Go Webserver Web site.

Figure 53. Lotus Domino Go Webserver Documentation

### 2.7.3.1 Additional Information on Lotus Domino Go Webserver

Additional information on the Lotus Domino Go Webserver can also be found in the following publications:

- *Network Computing Framework Component Guide, SG24-2119*  
Chapter 4, entitled "Servers", describes the basics about the product and its configuration and functions.
- *Internet Security in the Network Computing Framework, SG24-5220*  
This publication provides more details on the security aspects of the Webserver.

### 2.7.4 Microsoft's IIS 4.0

Online help is available from the Help pull-down on the Microsoft Management Console, as shown in Figure 47 on page 44.

---

## 2.8 Installed Directory Structure

The directories created by the IBM Network Station Manager installation process and the eNetwork On-Demand Server installation are slightly different from those used in previous versions of NSM.

The next figure illustrates the differences:

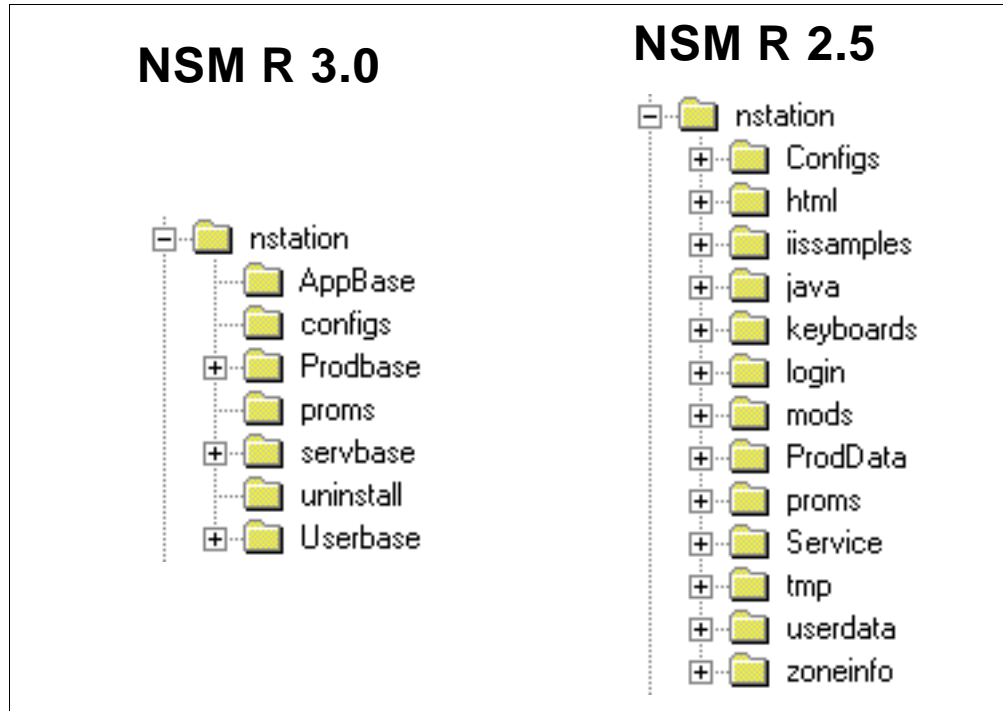


Figure 54. Directory Structures (R3 and R2.5)

In the figure above, the structure on the left is the new Release 3 structure and the one on the right is the old Release 2 structure. Notice the following:

- The `..\nstation\configs` directory in the R3 structure, as well as the `..\nstation\proms\` directory, is there for compatibility reasons with the previous release and to allow for an easier migration.

You can understand how these compatibility entries are used when you examine the retargeting process described in 3.4.2, “Client Retargeting” on page 80.

- The `prodbase` directory contains just about everything that is needed to make the IBM Network Station operational, such as hardware configuration files, fonts, proms, application modules, keyboard definitions, etc. See the next figure where this subdirectory has been expanded.
- The `userbase` directory contains all the data that is user-specific as well as the user home directories. If you use the separation of servers functions (see Chapter 4, “Separation of Servers” on page 101 for details), these directories can be located on a server other than the boot server.

The main subdirectories have been expanded in the next figure to give you an idea of their contents:

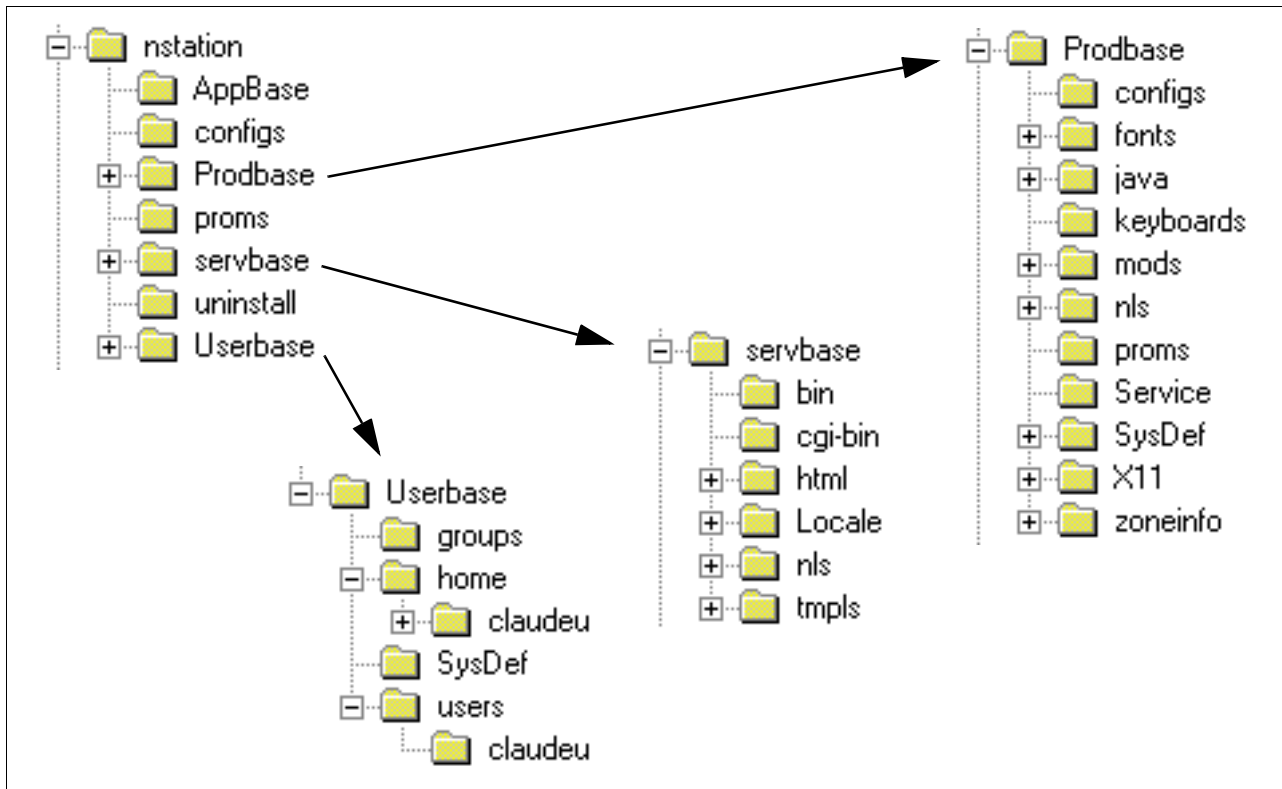


Figure 55. Main Directories Expanded

The eNetwork On-Demand Server installation process creates the directories as seen in the following figure.

This replaces the IBMTCP/IP directory that was used in the Release 2 version. This directory does not have to be installed on the same drive as the IBM Network Station Manager directories, but can be placed on any drive.

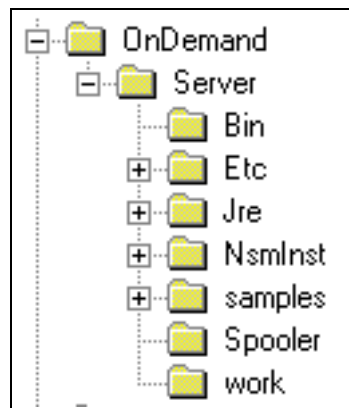


Figure 56. eNetwork On-Demand Server Directory Structure

---

## 2.9 Installing NSM on Windows NT Server 4.0, Terminal Server Edition

Installation of these components on a Windows NT Server 4.0, Terminal Server Edition system is the same as on a normal Windows NT Server 4.0 system, except that, prior to starting the installation process, the change user /install command should be issued in a command prompt window.

In reality, this command (change user /install) should probably be required only for the Netscape Navigator browser if this is the browser that all users connecting into the server are using. However, it appears at this point in time that the Lotus Domino Go Webserver installation also requires this command.

In any case, it does not hurt to issue this command when it is not needed, so just make sure it is issued before you begin the installation.

If you need to learn more about the effect of the change user /install command, see Chapter 18, "Installing Applications on WTSE" on page 303.

---

## 2.10 Uninstalling Products

Following are a few notes on the uninstallion of these products that might be useful if you need to experiment or if you run into installation problems.

### 2.10.1 Netscape Browser and Lotus Domino Go Webserver Uninstall

If you need to uninstall any of these components, the Netscape browser and the Lotus Domino Go Webserver each have an independent uninstall process, which is initiated through the Add/Remove Programs in the Control Panel.

The Lotus Domino Go Webserver uninstall process, when triggered through the Add/Remove Programs, does leave behind some entries in the Start=>Programs=>Lotus Applications, which are the pointers to the readme and the uninstall, but these are without consequence.

The Lotus Domino Go Webserver uninstall process is also made up of five different uninstall processes, each one started individually and each one requiring a click on OK after the uninstall is complete in order to continue with the next uninstall.

### 2.10.2 IBM Network Station Manager Uninstall

Removing the IBM Network Station Manager using the Add/Remove Programs also removes the other products that were installed by the IBM Network Station Manager install process, such as the eNetwork On-Demand Server and the NC Navigator. However, these products can still be removed individually using their respective entries in the Add/Remove Program list.

See also 2.6.4, "Re-Installation and Update" on page 38 for the difference between a full uninstall and an uninstall done as part of a re-installation.

### 2.10.3 IBM Intermediate Support Driver Uninstall

Removing the eNetwork On-Demand Server component does not remove the IBM Intermediate Support Driver that was installed as part of the eNetwork On-Demand Server installation process.

This driver must be removed manually by selecting the **Protocol** tab of the **Network** icon in the Control Panel.

#### 2.10.4 NSMAdmin and NSMUser User Groups

The NSM R3 uninstall process does not remove the NSMAdmin and NSMUser groups from the User Manager for Domains. If users were defined as belonging to these groups, they remain as members of these groups after an uninstall of the IBM Network Station Manager Release 3.

Note that this is not the case, however, for the NSM R2 uninstallation, which does remove these user groups. Therefore, special care must be taken when migrating from Release 2. It is best to let the R3 migration handle this process. See Chapter 3, "Migration from Release 2" on page 71 for details on migrating from Release 2.

#### 2.10.5 Remaining Files and Directories

If you uninstall all components except the base operating system, each of these uninstallation processes leaves behind some directories and files containing either log files or configuration files.

In summary, the sizes of these directories are as follows after a full uninstallation:

*Table 3. Size of Remaining Directories after Uninstall*

Component	Size of Remaining Directories
IBM Network Station Manager	13.8 MB
eNetwork On-Demand Server	83 KB
Lotus Domino Go Webserver	14.5 KB
NC Navigator	524 KB

---

### 2.11 Installing Products Individually

The integrated streamlined installation process makes it very easy to install all the required products in one simple operation.

However, should there be a need to install any of these products individually after the initial installation, this can be accomplished by executing the setup.exe for the desired product.

- For the eNetwork On-Demand Server, execute setup.exe from x:\ntnsm\en\products\enod\tcpip.
- For the NC Navigator (128-bit version), execute setup.exe from x:\ntnsm\en\products\ncnav.
- For the IBM Intermediate Device Driver, use the Network folder in the Control Panel to add a protocol and point to x:\ntnsm\en\products\enod\ndis.
- For Netscape, go to x:\ntnsm\en\products\netscape, then the subdirectory for the desired language, and run the executable found in that directory.

- For Lotus Domino Go Webserver, go to x:\ntnsm\en\products\lotusgo, then the subdirectory for the desired language, and run the executable found in that directory.

---

## 2.12 Batch Mode Installation

The readme file contains instructions on how to do a silent install from the command line using a response file in order to easily propagate an install to multiple identical servers. This is also called an automated or batch install.

Note that this automated install works for the IBM Network Station Manager, the eNetwork On-Demand Server, the NDIS Intermediate Support Driver and the NC Navigator. It is not applicable to the prerequisite products. In addition, the servers using this automated install must all have identical prerequisite software installed; otherwise, the installation process reverts to manual prompting.

### 2.12.1 Recording an Automated Install

In order to build an initial response file, install the prerequisite software on the first server, including the Web browser and the Web server, and when it is time to install the IBM Network Station Manager, launch the install from the command line using the following command where x: is the CD-ROM drive:

```
x:\ntnsm\en\products\nsm\setup.exe -r -SMS
```

This triggers the recording of the responses during the installation to a file named setup.iss located in c:\winnt.

The next figure shows the content for a sample setup.iss file.

```

[InstallShield Silent]
Version=v5.00.000
File=Response File
[DlgOrder]
Dlg0=SdWelcome-0
Count=11
Dlg1=SdLicense-0
Dlg2=AskYesNo-0
Dlg3=SdAskDestPath-0
Dlg4=SdSelectFolder-0
Dlg5=AskPath-0
Dlg6=AskPath-1
Dlg7=AskYesNo-1
Dlg8=MessageBox-0
Dlg9=AskYesNo-2
Dlg10=SdFinishReboot-0
[SdWelcome-0]
Result=1
[SdLicense-0]
Result=1
[AskYesNo-0]
Result=1
[SdAskDestPath-0]
szDir=d:\nstation
Result=1
[SdSelectFolder-0]
szFolder=IBM Network Station Manager
Result=1
[AskPath-0]
szPath=. \
Result=1
[AskPath-1]
szPath=d:\OnDemand\SERVER\
Result=1
[AskYesNo-1]
Result=1
[MessageBox-0]
Result=1
[Application]
Name=IBM Network Station Manager
Version=3.00.000
Company=IBM
[AskYesNo-2]
Result=1
[SdFinishReboot-0]
Result=1
BootOption=3

```

Figure 57. Sample setup.iss Response File

### 2.12.2 Using the Automated Install

To use this automated install, copy the setup.iss file from the C:\WINNT directory on the first server to the C:\WINNT directory of the other server(s) to be installed, on which you already have the prerequisite Web browser and Web server



installed, and issue the following command in a command prompt window, where x: is the CD-ROM drive:

```
x:\ntnsm\en\products\nsm\setup.exe -s -flc:\winnt\setup.iss
```

This launches the install, causes the setup.exe to read its responses from the setup.iss file and the install to take place automatically.

#### 2.12.2.1 Installation Language Dialog Prompt

The readme file indicates that you may get a dialog box prompting you for the installation language at the beginning of the installation.

If you do, you have three options:

1. Leave it as is, which means that you do not have a fully automated installation, but have to at least do one manual Enter to continue with the installation.
2. Disable the language prompt.

You can disable the language prompt by changing the EnableLandDlg=Y entry in the setup.ini file to read EnableLandDlg=N. However, since the setup.ini file is on the CD, you can't change it there, so you need to copy the CD directory structure to a shared drive, change the setup.ini file there and then use these copied file as the source of installation.

Consult the readme file for more details.

3. Wait for a fix, which is being worked on, that will eliminate this problem. This fix is nearly ready so that this problem will likely not exist by the time this document is published.

**Note:** During a silent install, there is no feedback or progress report on the screen indicating that the installation is taking place.

#### 2.12.3 Changing the Install Drive in the Response File

If the servers that you are cloning have a different disk configuration, and you need to install on a different drive than the one that was used on the initial server, the setup.iss file can be manually updated to reflect this change.

In the above sample file, only the two statements below need to be changed. Simply replace drive d: with whatever drive you want to use for the nstation and OnDemand\server directories.

```
szDir=d:\nstation  
szPath=d:\OnDemand\SERVER\
```

---

### 2.13 Boot Server Special Install

This special install is intended for a server that is used only as a base code server. That is, it is only used to supply the kernel, the application modules and the font files, and it is not authenticating users or serving any of the configuration files.

This is part of the separation of servers functionality, so please refer to Chapter 4, "Separation of Servers" on page 101 for detailed information on the functions provided by the separation of servers, the benefits and some examples.

Therefore, this boot server does not need to have the IBM Network Station Manager installed, nor a Web server installed, nor does it need any of the configuration files or the Network Station login server since it is not authenticating any users.

The only prerequisites in that case are the Windows NT 4.0 base operating system with Service Pack 3 and the TFTP and NFS server capabilities.

To install as a boot server, use the /bs option on the setup.exe from a command line, for example:

```
x:\ntnsm\en\products\nsm\setup.exe /bs
```

**Note:** If you need to use any other options such as -r -SMS when recording an install, make sure that the /bs is the first option specified otherwise it will not have any effect. Indeed, the /bs switch is order-dependent and must be placed before any InstallShield options.

Let us examine now what the exact effect is of using the /bs option on the setup.exe command. Use of this option causes the following to happen:

1. A Windows NT registry entry is created indicating the install type. This entry is called Install Type and is assigned a value of Boot Server.

The figure below illustrates this entry in the registry.

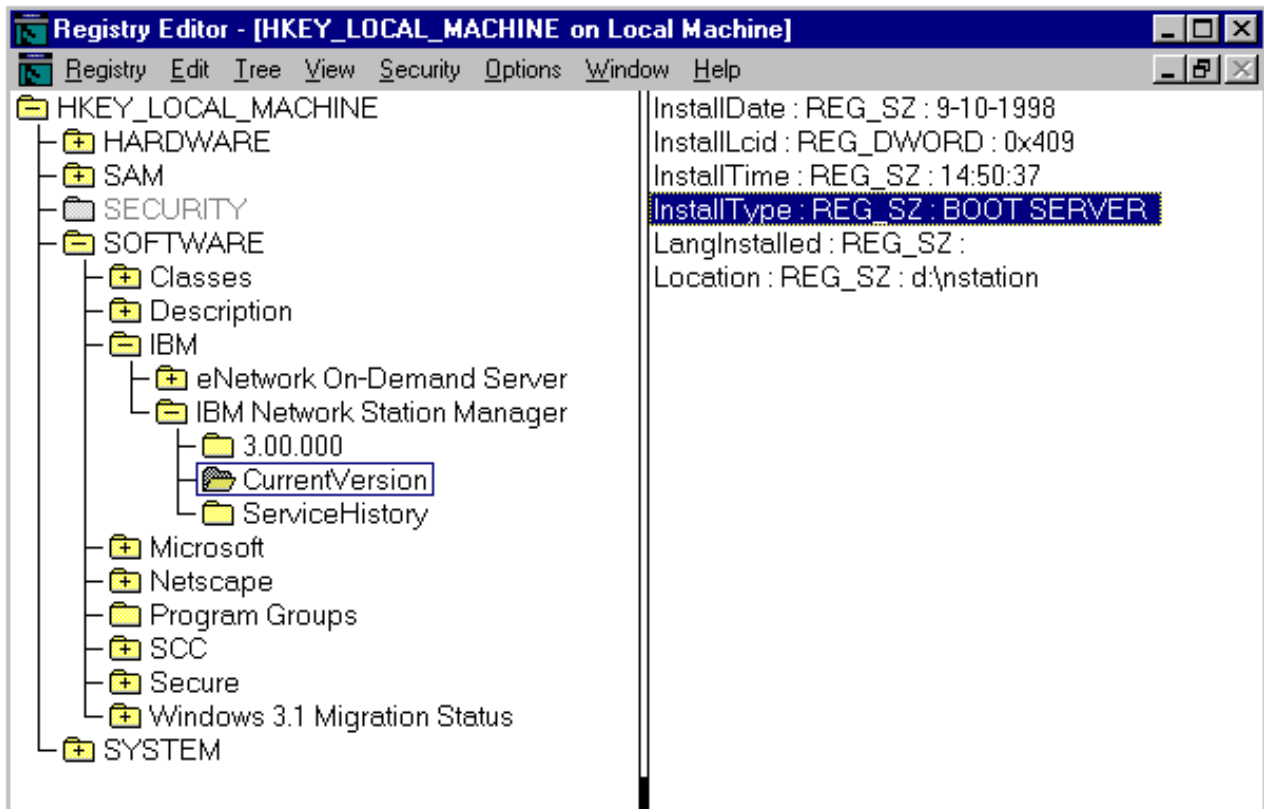


Figure 58. Install Type Registry Entry

This registry entry, once made, will direct all other subsequent re-installs to be performed as a boot server install. In other words, when you next execute

setup.exe on this server, you will not need to specify the /bs switch again. The setup.exe will query the registry to determine the type of install that was done the last time and will automatically perform the same type of installation without the user having to use the /bs switch on the setup.exe command.

At this time, there is no function provided to force a standard server install after a boot server install has been performed once. If for some reason it becomes necessary to go back to a standard server install, perform a full uninstall first and then re-install Release 3. The install type registry entry will then have the value STANDARD SERVER.

In other words, a full uninstall removes all the registry entries and the next install can then be performed from scratch; but if you use the uninstall process which is kicked off as part of an install, the install process then saves some key information, such as these registry entries and the location of the installed directories, in order to use this information after the uninstall. So, an uninstall done as part of an install process is not the same as a stand-alone full uninstall.

2. The Network Station Login Daemon (NSLD) does not get installed since it is not expected that IBM Network Stations will log on to this server, but only boot from it.
3. The nstation directory is smaller by about 30 MB. Most of this reduction is the result of the absence of most of the contents of the servbase directory; the AppBase and Userbase directories are also eliminated.

**Note:** If you use the IBM Network Station Manager from the browser on an IBM Network Station by using the entry located on the menu bar of the browser, you need to make modifications to some files in order to direct the browser to the authentication server instead of the boot server, which is the default.

In other words, the IBM Network Station Manager entry on the menu bar of the browser on the IBM Network Station is set to go to the host indicated by the BOOTHOST variable. If you installed a boot server (setup.exe /bs), the entry needs to be changed to the AUTHENTICATION\_HOST variable instead of the BOOTHOST variable.

The preference file that you need to edit is \nstation\prodbase\mods\Nav\pref in which you need to change the two occurrences of BOOTHOST to AUTHENTICATION\_HOST.

This is documented in the readme file.

---

## 2.14 Authentication Server Special Install

In the event that you do separate the boot server(s) from the authentication server(s), there is an additional install option that you can use when installing the authentication server that ensures that the login client on the IBM Network Station will use the authentication server to perform authentication instead of the boot server.

Why is this required?

First, let us explain the function that we are talking about here when discussing the login client. You should first review Chapter 4, "Separation of Servers" on

page 101 if you are unfamiliar with the differences between a boot server, a terminal configuration server and an authentication server.

Be aware that by default when the login client on the IBM Network Station displays the login panel to the user, asking for a user name and password, it is set to contact the boot server as soon as the user enters the information, *unless* the user clicks the Roam button to specify a different address.

In a case where we separate the boot server function from the authentication server function, we do not want the user to have to use the Roam button to enter the address of the authentication server every time that the user has to log in, so we need to change the default target server used by the login client. This is done by adding the `-authserv` parameter to the `actlogin` command, which is the command used to start the login client.

This command is normally in the `exec-startup-command` present in the `required.nsm` file, but it can be overridden by placing a similar statement in the `defaults.dft` file (see also the section on the authentication server on page 114).

In summary, what the authentication special server installation actually provides is a way of placing this statement (`exec-startup-command`) in `defaults.dft` in order to override the normal `actlogin` command.

To install as an authentication server, use the `/as` option on the `setup.exe` from a command line, for example:

```
x:\ntnsm\en\products\nsm\setup.exe /as
```

**Note:** Remember that if you use other options, that the `/as` must be the *first* option specified otherwise it does not have any effect. Indeed, the `/as` switch is order-dependent and must be placed before any InstallShield options.

The effect of using the `/as` option on the `setup.exe` command is as follows:

1. A Windows NT registry entry is created indicating the install type. This entry is called `Install Type` and is assigned a value of *Authentication Server*.

The same considerations that we have discussed above for the registry entry caused by the `/bs` switch apply here as well.

2. The following line is appended to `defaults.dft`, where `auth_server_address` is the IP host name of the server on which the install is taking place:

```
set exec-startup-commands = {{ mcuis } { "actlogin -authserve  
auth_server_address" }}
```

**Note:** If the administrator already had specified this command (`exec-startup-command`) in his or her `defaults.dft` file, the easiest solution is to not use the `/as` install switch and enter the `actlogin -authserv` parameter himself or herself, or to use the `/as` switch and then manually add the other modifications that he or she had entered on the `exec-startup-command`. Remember that two `set` commands can exist for the same parameter in the same configuration file, in which case the last one read is the one that overrides all the other statements.

3. Subsequent installs on this server, however, will *not* append again to the `defaults.dft` file; in other words, the append is done only the first time that the `/as` switch is used. This is because it is assumed that this statement, once placed in the `defaults.dft` file, does not need to change.

However, if you do want to cause a rewrite of this statement to the defaults.dft file as in the first time use of the /as, you can force this by using the /asf option instead of /as on the next install to force a rewrite of the statement to the defaults.dft file. This is summarized in the figure below:

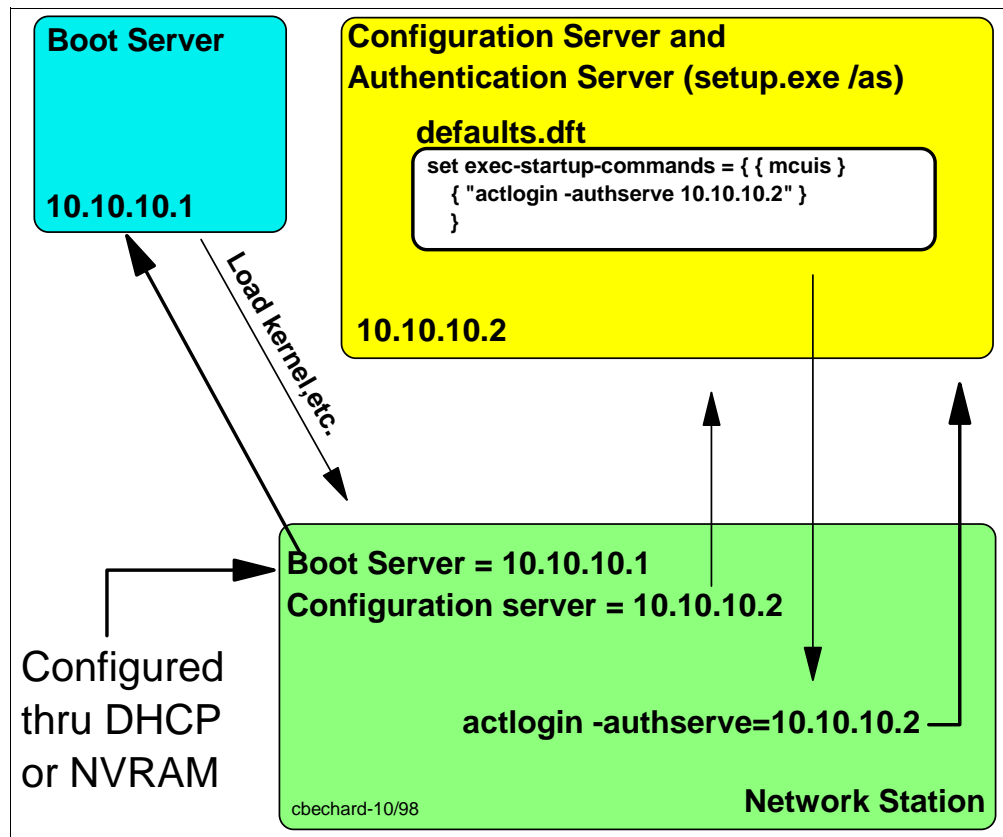


Figure 59. Authentication Server Installation

**Note:** If you are also separating the terminal configuration server from the authentication server, then you can use the /as option when installing the authentication server, but since it is the defaults.dft file on the terminal configuration server that is used, you then need to move the set exec-startup-command statement that was appended to the defaults.dft file on the authentication server to the defaults.dft file on the terminal configuration server.

This is illustrated in the next figure.

A reminder that if you do not configure a specific terminal configuration server, by default, the boot server is considered to be the configuration server and the defaults.dft configuration file is fetched (along with all the other configuration files) from the boot server.

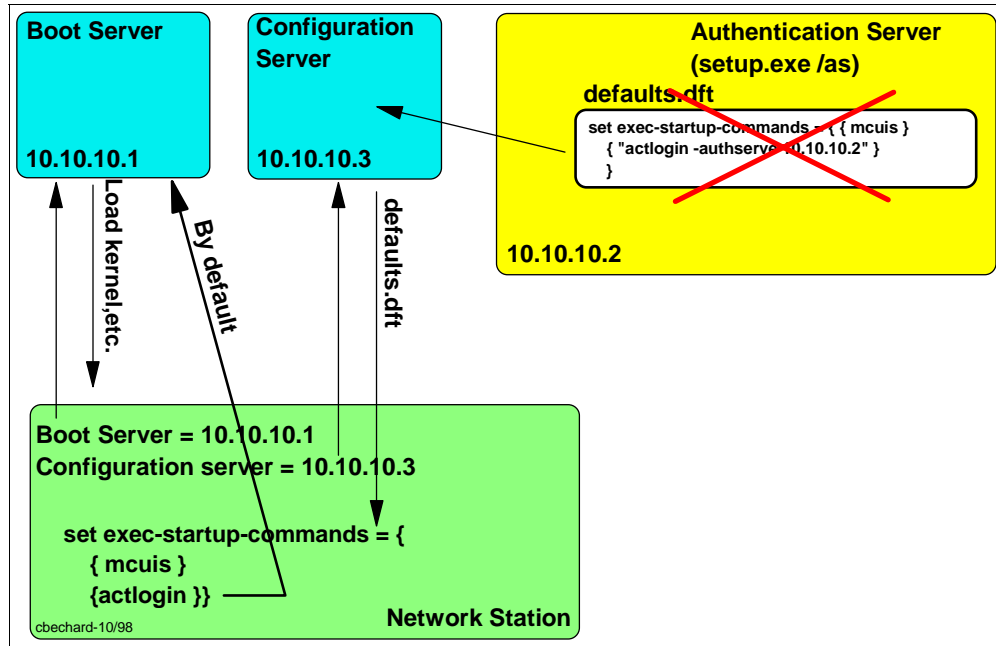


Figure 60. Authentication and Configuration Server

## 2.15 Windows NT Server 4.0, Terminal Server Edition Installation

Installing Windows NT 4.0 - Terminal Server Edition is no different from installing a base Windows NT 4.0 Server, so we do not feel that there is a need to cover this topic here.

If necessary, there are installation steps for the Windows NT 4.0 Server included in the *IBM Network Station Manager Installation and Use, SC41-0664* product publication that you can refer to.

## 2.16 MetaFrame from Citrix Systems Inc.

MetaFrame is a product from Citrix that installs on top of the Microsoft Windows NT 4.0 Terminal Server Edition in order to provide access to the WTSE system through the ICA protocol.

Please refer to Chapter 17, "Connecting to Windows Applications Servers" on page 277 for additional details on MetaFrame and where it fits.

### 2.16.1 MetaFrame Installation

We found the MetaFrame installation process to be very easy and straightforward with few responses required when using the defaults.

There is excellent documentation shipped with the product so there is little point to repeat any of that information here; therefore we only highlight a few key points.

On inserting the CD, the following panel comes up and a click on **MetaFrame Setup** is all that's required to start the install process.



Figure 61. MetaFrame Installation Autorun Panel

There are few decisions to be made during the install process so mostly we just accept the defaults.

After installation the folder illustrated in the next figure contains all the MetaFrame-related applications.

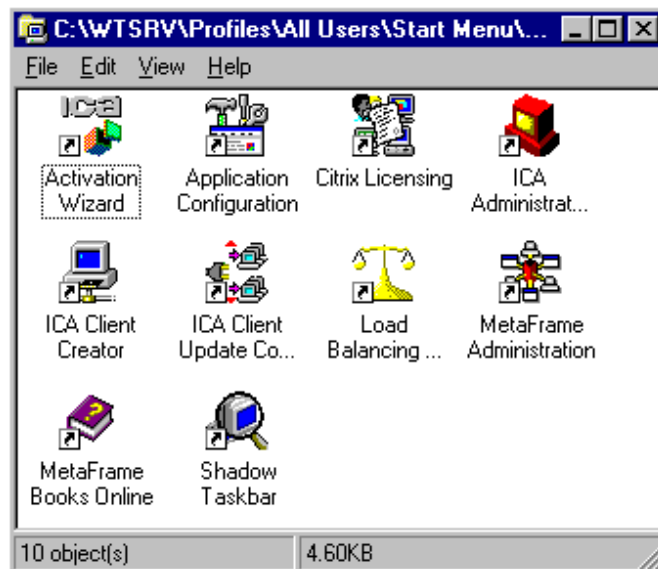
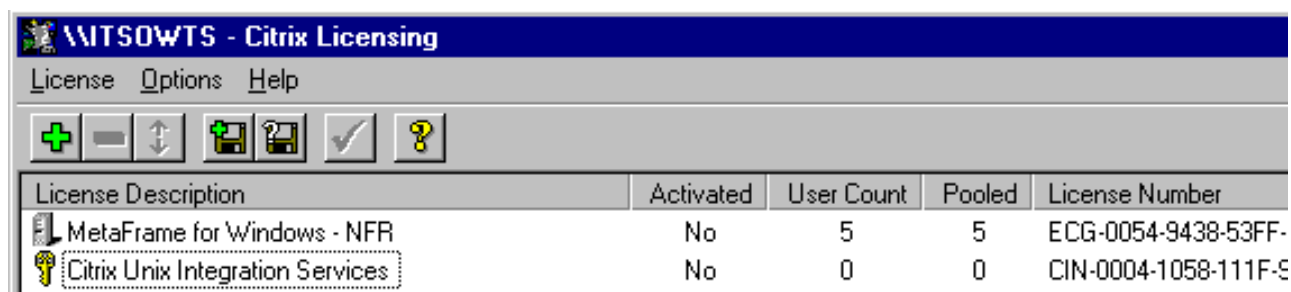


Figure 62. MetaFrame Tools and Applications Folder

## 2.16.2 Licensing

During the installation, you are asked to enter the serial number that appears on the CD. This creates a record in the Licensing application, such as that shown in the first line of the panel illustrated in the next figure.

There is a second license, shown in the figure below, called Citrix UNIX Integration Services. This is the result of the next product installation, which we discuss next.



License Description	Activated	User Count	Pooled	License Number
MetaFrame for Windows - NFR	No	5	5	ECG-0054-9438-53FF-
Citrix Unix Integration Services	No	0	0	CIN-0004-1058-111F-S

Figure 63. MetaFrame Licenses

In the case shown here, we entered the serial number but did not actually activate the license yet, in case we ran into installation problems and had to re-install. There is a grace period of 35 days during which the product is functional without the license having been activated, and there is a reminder of this period of time issued every time you boot.

To activate the license, one must contact Citrix Systems Inc., through a variety of means, including a Web browser, in order to obtain an activation code based on the license number that appears in the window shown above. That license number is made up of the serial number you entered to which eight more digits have been added.

The activation code is an additional eight digits, obtained from Citrix, that must be entered using the licensing application above, by selecting **Activate license** under the License pull-down.

### 2.16.3 Administration

At this point, ICA is ready to be used without further configuration.

See Chapter 17, "Connecting to Windows Applications Servers" on page 277 for details on how to use the IBM Network Station Manager to configure ICA connections for IBM Network Stations.

To monitor sessions and users, use the MetaFrame Administration application. We illustrate the main panel for this application in the next figure.

In this example, it shows that MetaFrame is listening for X.11 clients, ICA clients over NetBIOS, ICA clients over TCP, and RDP clients over TCP.

It also shows that there are three sessions active: one is the user administrator logged on to the system console, another is a user called Ariane connected over an X.11 session, and the third one is a user called Thomas connected using ICA over TCP.

For more details on the use of this application, please consult the product documentation.



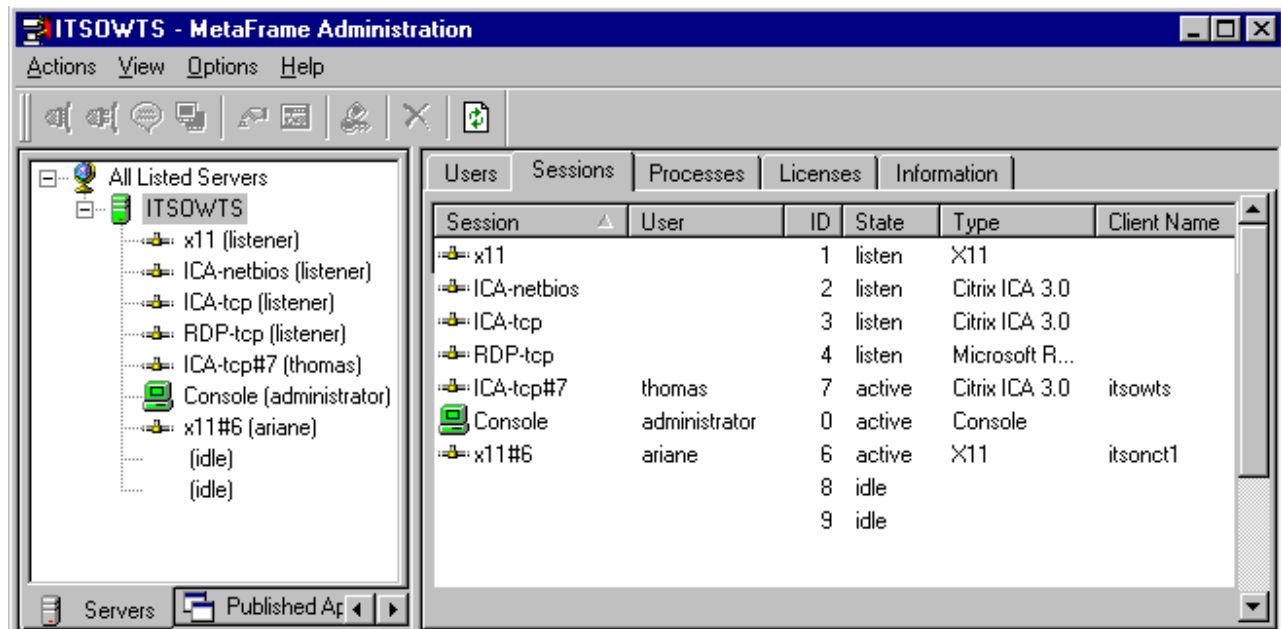


Figure 64. MetaFrame Administration

#### 2.16.4 MetaFrame Documentation

Shipped with the MetaFrame CD are the two following publications that contain all the required details for the installation of the product:

- *Citrix MetaFrame Administrator's Guide*
- *Citrix MetaFrame ICA Client User's Guide*

The MetaFrame documentation is also online, as shown below:

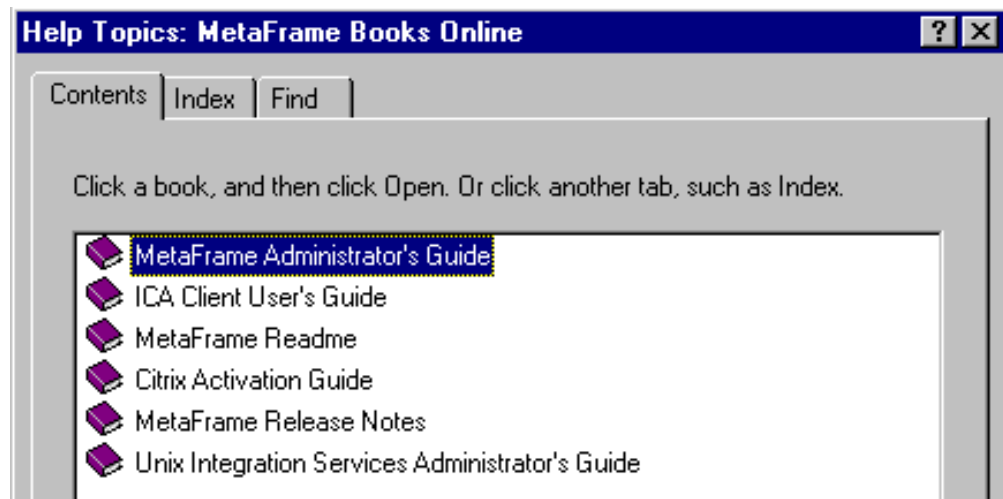


Figure 65. MetaFrame Online Documentation

## 2.17 UNIX Integration Services (UIS) for MetaFrame

UNIX Integration Services is a product that installs on MetaFrame in order to provide X.11 connection support into MetaFrame. If you are familiar with WinCenter, this can be called WinCenter for MetaFrame.

Please refer to Chapter 17, "Connecting to Windows Applications Servers" on page 277 for additional details on UNIX Integration Services for MetaFrame and where it fits.

### 2.17.1 UIS Installation

Here again, as for MetaFrame, the installation process is simple, with few interactions. It is well documented in the documentation that comes with the product, so we do not feel it is necessary to go into any details here.

The next figure illustrates the main autorun panel. Simply click on **Install UIS** to begin the install process.

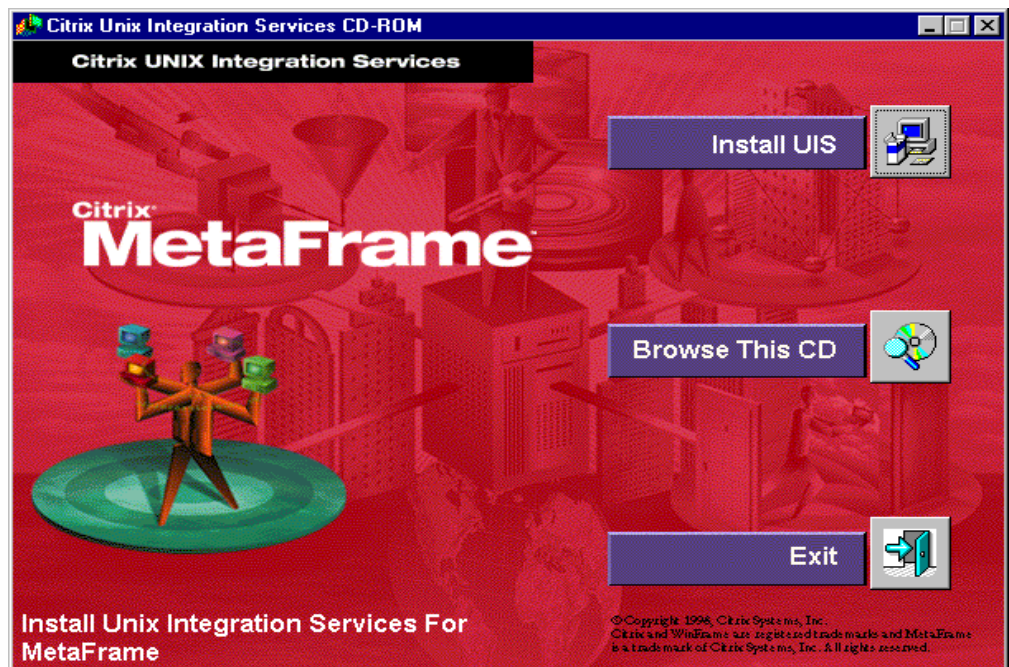


Figure 66. UIS Installation Panel

You do get asked for a license during installation, and you can enter it at that time, or after the installation. This process is similar to the one we discussed for MetaFrame. Enter the serial number provided on the CD and you get an entry added in the licensing panel, as shown in Figure 63 on page 64. If that license number is not added, the X.11 support is not available.

After adding the license, you get a panel asking whether you want to disable X.11 connections until such time that you have configured X.11 connection permissions, and it is recommended that you do disable access initially.

This is because client licenses are assigned automatically to specific client desktops as they connect in. So, in order to avoid assigning licenses to

unauthorized desktops, it is preferable to disable the X.11 access, then configure the specific desktops that are allowed to connect in, and then re-enable X.11 access.

This way, only the desktops you have configured can get a client license allocated to them.

The applications illustrated in the next figure are available in the UIS folder after installation.

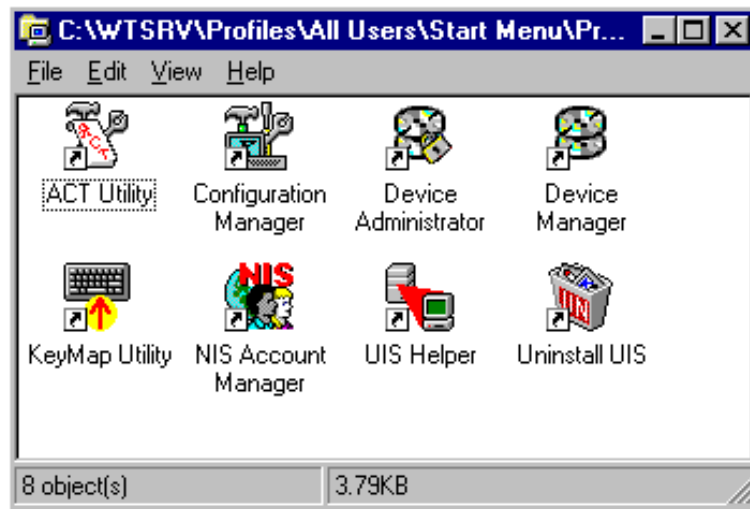


Figure 67. UIS Applications Folder

### 2.17.2 UIS Configuration

After the installation completes, you need to restart the system in order to use UIS, but if you have disabled the X.11 support during the installation, and need to configure some desktop access permissions, it is preferable to do it at this point, before rebooting, since you need to reboot anyway after changing the UIS configuration.

To configure UIS, use the UIS Configuration Manager, as illustrated in the next figure:

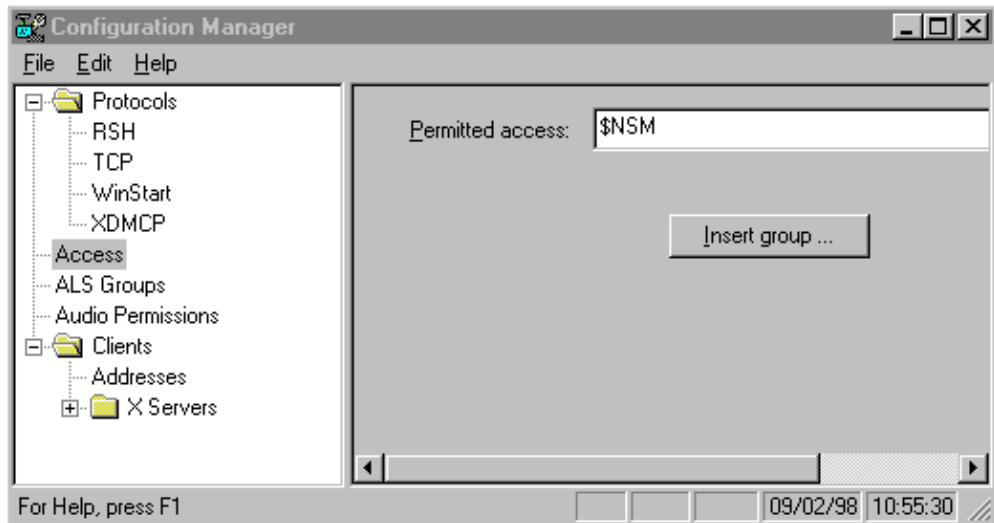


Figure 68. UIS Configuration Manager

On the left-hand side in the above panel, the four protocols that can be used to connect into MetaFrame are displayed in tree fashion, and each can be selected to be enabled or disabled.

Then the Access item, which is the selected entry in the figure above, is used to specify who is authorized to access the system. By default, the entry here shown on the right side of the panel is the group \$ALL, which allows everyone to have access.

In this example, we changed the \$ALL entry for \$NSM after we created a group called NSM.

This group was defined by selecting the next entry called ALS Groups. In the next figure, we display the group NSM after it was created. The group contains two desktops, at addresses 9.24.104.189 and 9.24.104.175; therefore, these are the only desktops allowed to connect at this time.

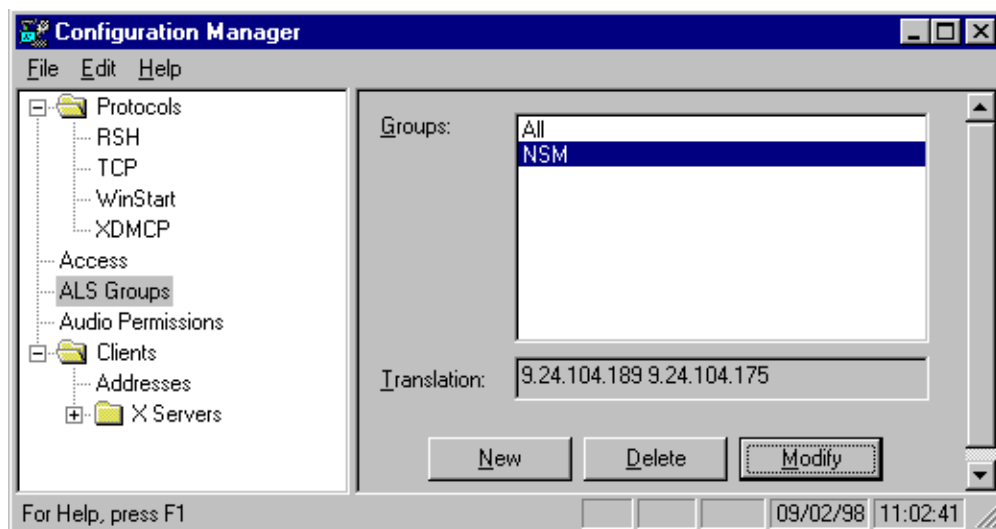


Figure 69. UIS Group Definition

You can then use the Terminal Server Connection Configuration to re-enable the X.11 connection that was disabled during UIS installation.

Select **Start=>Programs=>Administrative Tools, Terminal Server Connection Configuration** to bring up a panel similar to the one in the next figure:

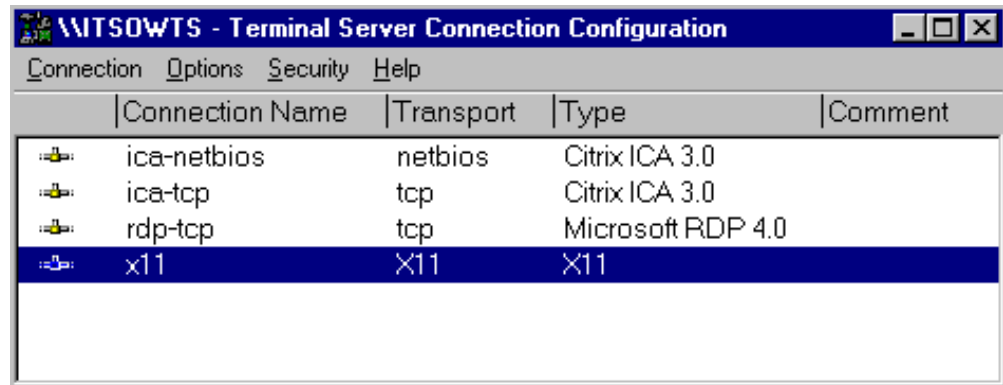


Figure 70. Enabling X.11 Connections

Select the **X.11** protocol, as shown above and select **Enable** from the **Connection** pull-down on the menu bar.

At this point, reboot your system in order to enable the configuration changes, and upon restarting the selected desktops have X.11 access to the MetaFrame Server.

See Chapter 17, “Connecting to Windows Applications Servers” on page 277 for details on how to use the IBM Network Station Manager to configure X.11 connections for IBM Network Stations.

### 2.17.3 UIS Documentation

During UIS installation, the *UNIX Integration Services Administrator's Guide* is added to the MetaFrame Book Online Help topics. The way to get to this document is by clicking **Start=>Programs=>MetaFrame tools=>MetaFrame Books Online**.

This document appears as the last one in Figure 65 on page 65.



---

## Chapter 3. Migration from Release 2

The intent of this chapter is to describe the IBM Network Station Manager Release 3 migration support that allows you to move from all versions of Release 2 (2.0, NT NSM Service Pack #1, NT NSM Service Pack #2) to Release 3.

The objective of the migration support and facilities is to perform the migration of servers with little manual intervention, especially at the IBM Network Station itself, other than the explicit action of installing Release 3.

In some cases, it can indeed be done with little or no manual intervention but in other cases, more changes may be required.

Migration can be, depending on the environment, a complex issue that should not be taken lightly and may require many steps to be performed such that users see little or no impact on their productivity.

The official source of migration instructions is in the product publication entitled *IBM Network Station Manager Installation and Use, SC41-0664*, and we recommend that this should be your primary source of information.

What we describe below is our own experience and findings when we attempt to go through some migration scenarios. In the process, we try to understand and explain as best we can how the migration process works so that you will be in a better position to do problem determination should anything go wrong in your migration process.

---

### 3.1 Migration Overview

The migration process can be divided into two main stages:

1. Migrating the server

This is the task of replacing the IBM Network Station Manager Release 2 level of code on the server with the Release 3 level of code, as well as upgrading any other prerequisite software.

This also includes migrating user preference types of data and home directories.

2. Migrating the clients

This is the task of changing the configuration data of one or more IBM Network Stations to cause them to boot from a newly installed Release 3 server.

This task is also called *retargeting* clients, meaning that a client's target boot server is changed from the old server to the new server.

This retargeting is not only a change of the IP address of the target boot server but it also includes a change in the boot protocol, from TFTP which was the standard adopted for Windows NT in R2, to NFS which is now the required protocol for R3.

Note as well that the actual target server may be the same physical server if the server was upgraded in place from R2 to R3.

## 3.2 Migration Methods

There are two migration methods that can be used:

1. The single server migration
2. The dual server migration

Each of these is equally valid and which one is used is a question of preference or company policy concerning migration procedures. However, the single server upgrade method might not always be applicable or possible.

Each of these is discussed below in more details.

### 3.2.1 The Single Server Migration

This is an in-place migration method, whereby the old release is replaced with the new release *on the same machine*, therefore making that server unavailable during the migration period.

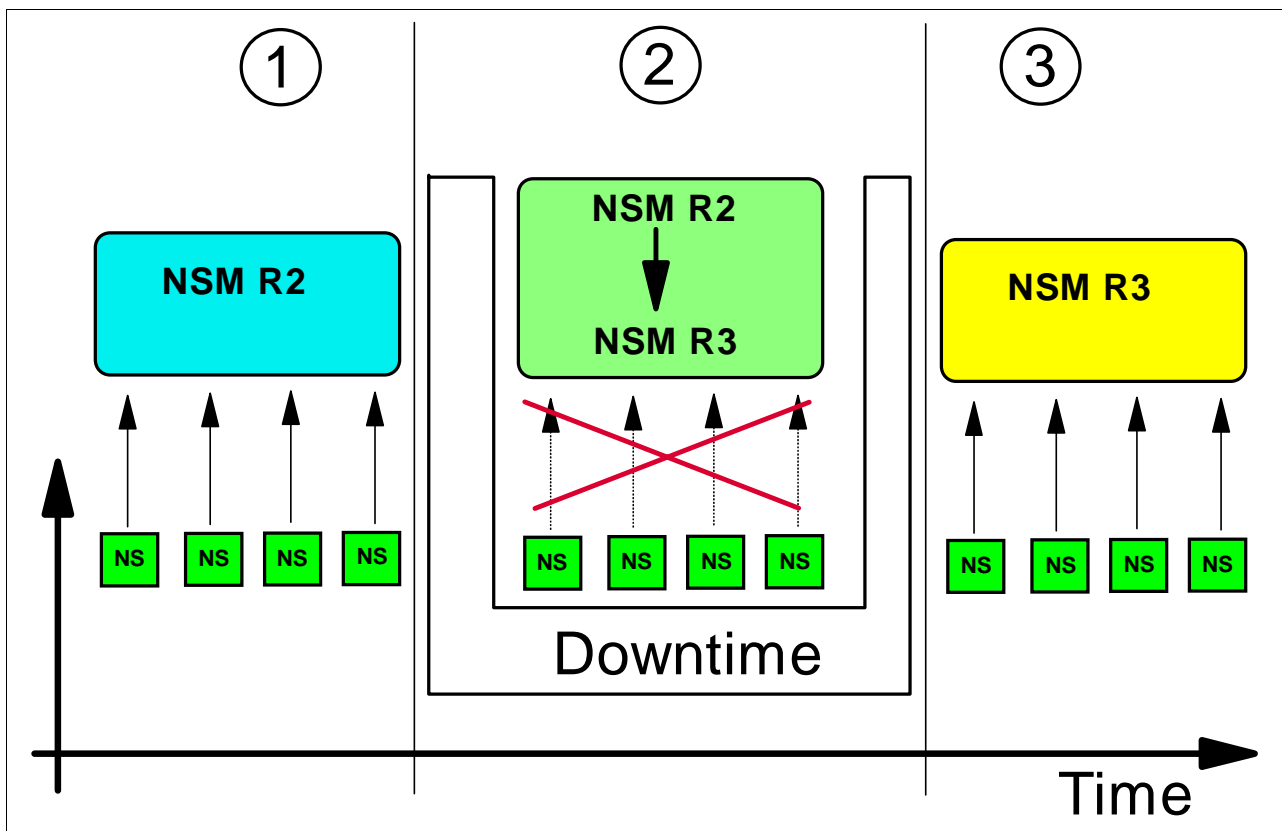


Figure 71. Single Server Migration Method

In the figure above:

1. During period 1, all the IBM Network Stations clients are operational with a server running Release 2 of the IBM Network Station Manager.
2. During period 2, which could be overnight or a weekend for example, the server is totally unavailable while the administrator is installing new releases of the IBM Network Station Manager and other prerequisite software.



3. As part of this process, a few pilot clients are tested to ensure that they can operate with the new server before the rest of the population is allowed to migrate the next day.
4. During period 3, all the IBM Network Station clients are changed so that they now operate with the upgraded server running Release 3 of the IBM Network Station Manager.

#### **3.2.1.1 Advantages**

The main advantage of this method is that it does not require additional equipment (that is, an additional server for the duration of the migration).

#### **3.2.1.2 Disadvantages**

The disadvantages are that there is inevitably some down time for the clients, although scheduling an overnight migration or a weekend migration might minimize the impact of the down time, and there is more risk involved since it might be difficult to go back to the old release should any severe problem be encountered.

This method is also not possible if the migration is from other than a Windows NT 4.0 U.S. English server to Windows NT 4.0 U.S. English. That is, if you want your new server to have a non-U.S. English Windows NT version, then the base operating system needs to be re-installed and this then becomes a complete re-install as opposed to an in-place migration. Also, if you are migrating from a WinFrame server or to a Windows NT Server 4.0, Terminal Server Edition, this also requires a re-install of the base operating system.

### **3.2.2 The Dual Server Migration**

This is the more traditional method whereby the new release is installed on a machine other than the current server; then, when everything is deemed to be ready, clients are migrated over to the new server.

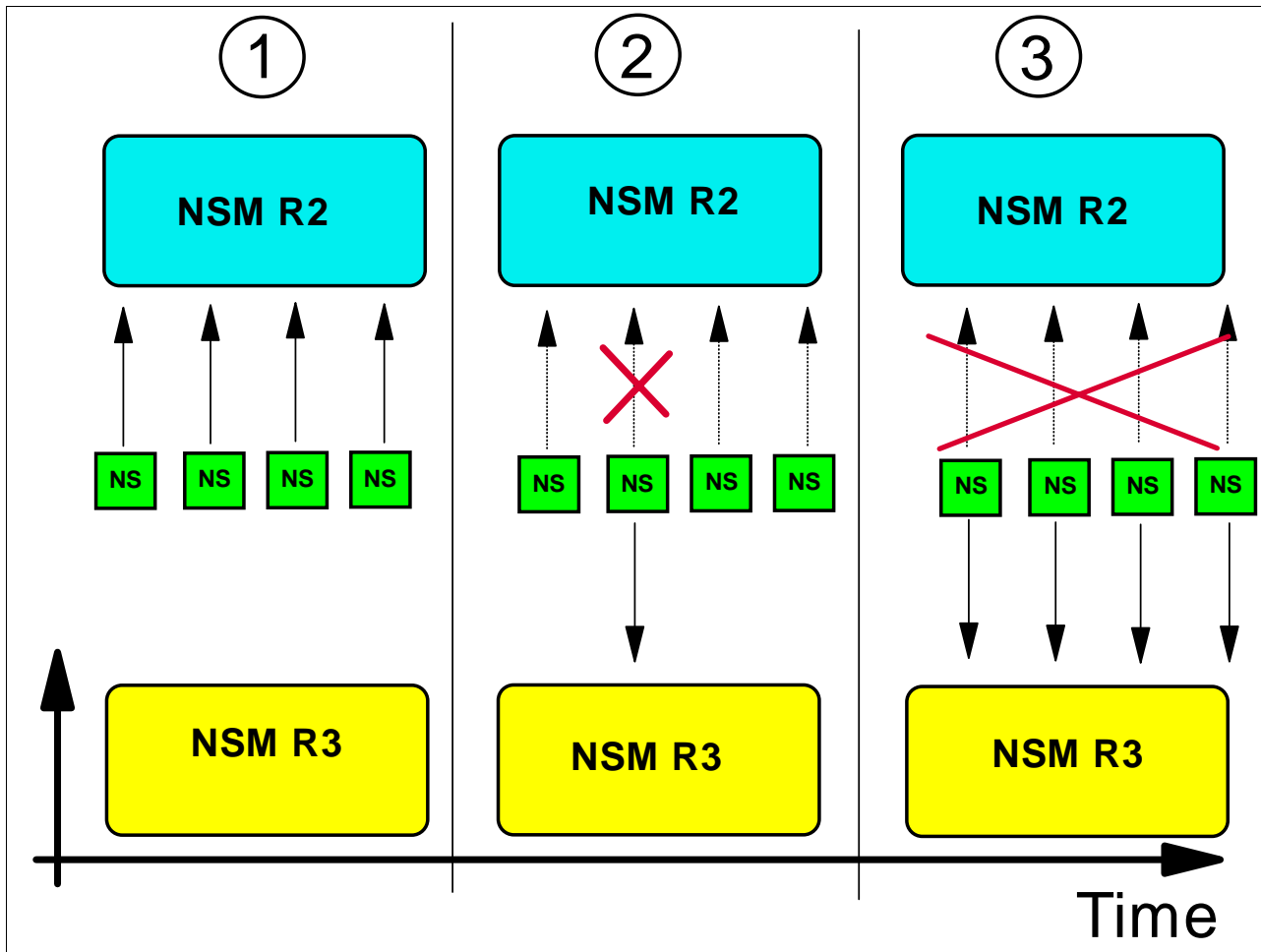


Figure 72. The Dual Server Migration Method

In the figure above:

1. During period 1, all IBM Network Station clients are operational with a Release 2 server.

During that period, a new Release 3 server is installed, and, as part of the installation process, all the user preferences files located on the Release 2 server are migrated over to the new R3 server.

2. During period 2, a few selected clients are retargeted and migrated over to the R3 server to verify the functionality of the new server and to test out the retargeting procedures.

The retargeting procedure should include a scenario where the client is retargeted back to the R2 server in case of unforeseen problems.

3. During period 3, all clients are then retargeted to the new R3 server and the R2 server is kept available, as backup, for a period of time after which it is retired or reassigned.

**Note:** It might be necessary to re-migrate the user preference files from the R2 server to the R3 server if the period of time where both R2 and R3 users are operational. This re-migration can be performed with a migration utility, to ensure that users do not lose any data. For example, if user A had saved

some new browser bookmarks between the time that the first migration was done in period 1 and the time that user A is migrated over to the R3 server in period 3, he or she would lose his or her new bookmarks unless we ensure that we get the latest copy of his or her preference files.

#### **3.2.2.1 Disadvantages**

The disadvantage of this method is that it requires additional equipment, at least for the duration of the migration period, and that the migration utility for user preferences might have to be run multiple times. This approach is also slightly more complex.

#### **3.2.2.2 Advantages**

The advantages are that this is a more traditional, safe and orderly approach, which does not induce any down time, which can be done at a more leisurely pace and which always affords clients the possibility to go back to the old release in the case of unforeseen or severe problems.

---

### **3.3 What Actually Needs to Be Migrated?**

Before we carry on with this topic, let's take a look at the elements of migration, that is, what actually needs to be migrated when going from Release 2 to Release 3 of the IBM Network Station Manager and which components and facilities are involved in this migration.

This will give you an idea of some of the details that you need to pay attention to in order to benefit from a trouble free and easy migration and give you a better understanding of what happens in case you need to do problem determination.

We then illustrate a few migration cases with practical examples.

On the server, the elements of migration are:

1. Installation of new releases of the prerequisite Web browser and Web server products, if they are not already at the proper level.
2. The upgrade of Release 2 of the IBM Network Station Manager program to Release 3.
3. The Windows NT user accounts that are part of the NSMAdmin and NSMUser groups.

In order to find out which users need to be migrated, the migration program queries the local machine's NSMAdmin and NSMUser groups. If these groups cannot be obtained locally, and the machine is attached to a domain, the migration program queries the primary domain controller. If these user groups cannot be located, the migration program does not migrate any of the user files.

4. A utility named NTNSMRR2.EXE, located in \nstation\servbase\bin (and in the ntasm\en\utility directory on the CD), that can be used to remove all the components from Release 2 prior to installing Release 3.

This utility preserves the data necessary for a migration during the Release 3 installation, because it renames the NSMAdmin and NSMUser groups to some other name prior to a Release 2 removal, and renames them back to their original names after the completion of removal of the Release 2 level of code.

This is because the Release 2 removal (uninstall) process deletes these groups from the Windows NT user accounts; the utility is therefore used to rename these groups prior to uninstall so that we can retain these user accounts.

**Attention**

You should use caution when using this utility; see Chapter 3.6.3, "Using the NTNSMRR2.EXE Utility" on page 95 for additional details.

5. The \nstation\configs directory on the R2 server contains the R2 terminal configuration files, most of which are replaced by the R3 files, but some are copied over to the \nstation\prodbase\configs directory on the R3 server because they are custom configuration files, such as defaults.dft, and "name".trm, etc.  
  
The migration process determines which of these files are needed and which are not.
6. The \nstation\userdata directory on the R2 server contains the per user data for each user. The migration process determines which subdirectories and files to migrate to the appropriate \userdata\ subdirectories on the R3 server based on the users that are present in the NSMUser and NSMAdmin groups. Data for users that are not listed in these two groups is not migrated.
7. The x:\users directory on the R2 server contains the user's home directories. These home directories, for the users being migrated, are copied to the \userbase\home\"username" on the R3 server.
8. On the R3 server, the \nstation\ directory contains copies of the new R3 kernel in uncompressed format. This is retained for compatibility purposes in order to enable R2 clients to load the R3 kernel until their boot monitor has been upgraded to be able to download the compressed kernel from the normal R3 \nstation\prodbase\ directory.
9. On the R3 server, the \nstation\configs\ directory has been retained for compatibility purposes and contains a defaults.dft file, defaults.r2 file and standard.nsm file. These files are used during the client retargeting process to make the process as automatic as possible. We examine the contents of these files later when we discuss retargeting in 3.4.2, "Client Retargeting" on page 80.
10. The \nstation\proms directory, which is defined to be accessed through TFTP, contains copies of the new boot monitor (bootm) and the new TRN flash code (trflash). These are duplicates of what already exists in the normal R3 \nstation\prodbase\proms directory, but they are there for compatibility purposes to facilitate the retargeting process when R2 clients are still using TFTP until they get updated to use NFS.
11. The nsmmigr.exe utility, located in \nstation\servbase\bin, is used to migrate the per user preference files from an R2-based server to an R3-based server.  
  
This utility is called during the installation process; it prompts for the location of the R2 files (usually x:\nstation where x: is the drive where the R2 code was installed) and copies the required files from an R2 to an R3 server based on the users present in the NSMAdmin and NSMUser groups.

This utility can also be run independently of the R3 install process, at any time, and as many times as required, in order to re-migrate the per user data in cases where users being retargeted to an R3 server have been active on the R2 server since the last time this utility was run. Caution must be used though to avoid re-migrating users that have been active on the R3 side.

**Note:** Any customized configuration parameters that were added to any of the R2 NSM managed files such as `standard.nsm`, `required.nsm`, `control.nsm`, `hosts.nsm`, `defaults.nsm`, `"name".nst`, `"username".nsu`, etc. are *not* migrated by the migration process.

These custom changes must be examined, and if still appropriate, either replaced with NSM controlled parameters or manually migrated. See 3.7, “Migrating Custom R2 Configuration Files” on page 97 for details on how to proceed for these custom changes.

On the IBM Network Station, the elements of migration are:

1. Update of the boot monitor prom to Level 3.0.1.
2. Update of the token-ring network flash.
3. Update of the boot server address, the boot protocol and the boot directory in the IBM Network Station Setup utility or update of the corresponding DHCP options on the DHCP server.

---

## 3.4 Dual Server Migration Example

As a first example, we use a dual server migration scenario since we believe that this is probably the most common scenario that will be used.

We have an operational R2 server on Windows NT 4.0, which we migrate to a Windows NT 4.0 R3 Server.

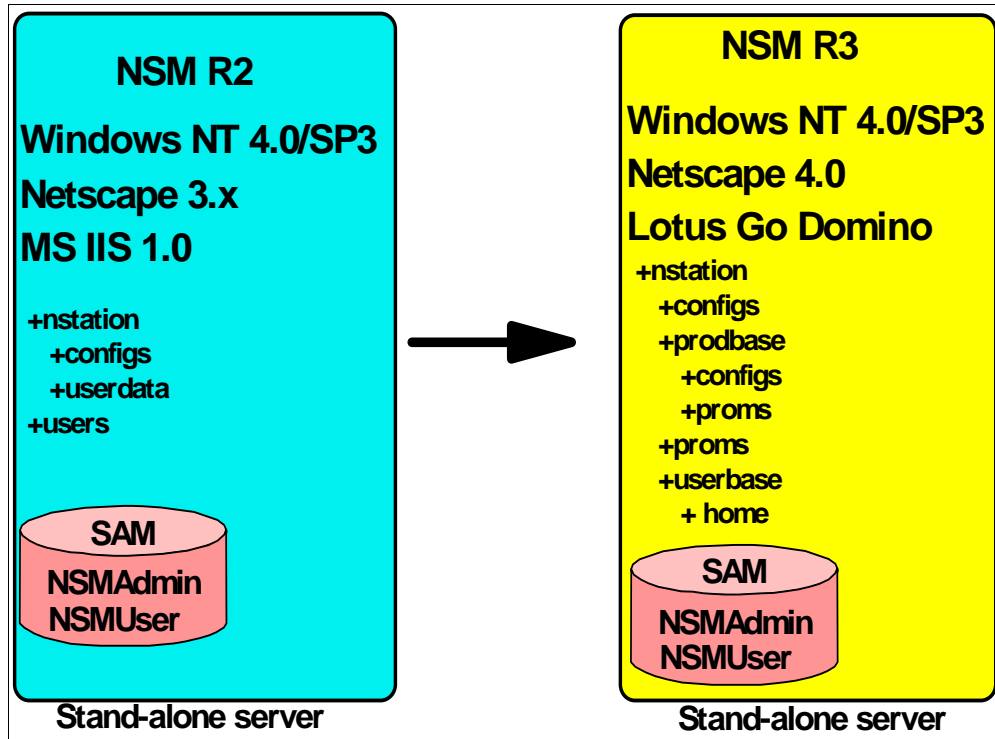


Figure 73. Dual Server Migration - Example 1

The environment is as illustrated in the figure above:

- Each server is a stand-alone server with users defined locally.
- The existing R2 server has an NT 4.0 system at the Service Pack 3 level, a Netscape Browser 3.x, Microsoft's IIS 1.0 Web Server and the IBM Network Station Manager Release 2 level of code.
- Our target environment is an R3 server with Netscape 4.0 and Lotus Domino Go Webserver and IBM Network Station Manager Release 3.

Here are the steps we use to migrate our R2 server to R3.

### 3.4.1 Server Migration

The server migration steps are as follows:

1. Install Windows NT 4.0 + Service Pack 3 (in this example, we install as a stand-alone server) and install the prerequisite products, Netscape Navigator 4.0 and Lotus Domino Go Webserver on the R3 server.
2. On the R2 server, share the drive containing the \nstation directory and on the R3 server map a network drive to that shared drive on the R2 server. This is to allow the install process on the R3 server to access the old R2 directories on the R2 server and migrate the data over.

If a network drive cannot be mapped between the old and new servers, use any other method, such as copying files to diskette, that will make these files accessible during the R3 install process. The directories to copy are (where x: is the drive where the IBM Network Station Manager R2 is installed):

- x:\users\

- x:\nstation\userdata\
  - x:\nstation\configs\
  - x:\nstation\esuite\registry
3. Use the User Manager for Domains application on the R3 server to create the NSMAdmin and NSMUser groups, and create accounts for the users that are to be migrated, making sure they belong to the NSMUser group.  
  
This is needed because the migration utility queries the local Windows NT Security database and migrates users only if they are members of the local NSMUser or NSMAdmin groups.
  4. Start the IBM Network Station Manager installation process on the R3 server. When prompted for a migration path, as shown in the figure below, enter the network drive mapped to the old server, or to whatever other media you used for these files. Typically, this is x:\nstation.

If the path is not valid, you get prompted again for a valid path.

**Note:** If you prefer to delay this migration step until after you have completely installed your new R3 server, you have the choice of leaving the migration path blank and to use the nsmmigr.exe utility later on to accomplish the same tasks, but independently of the install process.

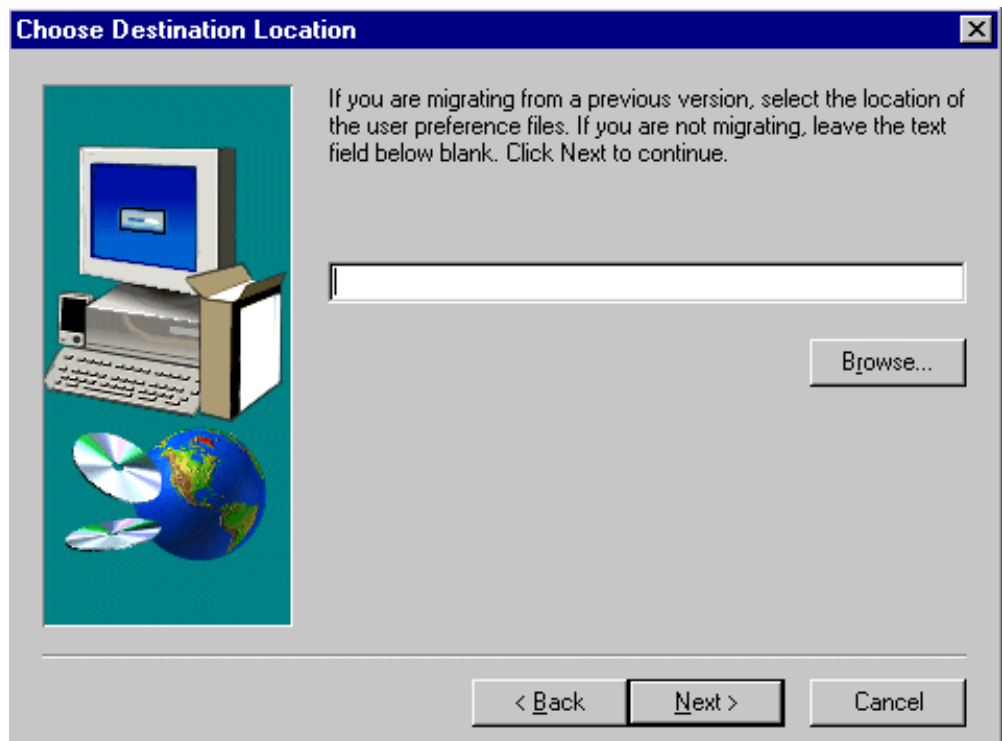


Figure 74. Migration Path Prompt during NSM Install

5. After the install completes, reboot your R3 server.

This completes the install of the R3 server and the migration of the user data from the R2 to the R3 server. This was the first part of the migration; the next step is the retargeting of the IBM Network Station clients from the R2 to the R3 server.

### 3.4.2 Client Retargeting

Client retargeting is the task of causing an IBM Network Station client to switch from booting from an R2 server to booting from R3 server.

If the task consisted only of changing the address of the target server, this would be a very simple task indeed (and hopefully will be the case for the next migration to the follow on release to R3). However, in this case, it is a little bit more complex because in addition to changing the address of the target server, we also need to change the boot monitor version on the IBM Network Station, possibly reflash the token-ring code, change the boot protocol from TFTP to NFS and change the boot and configuration file directories.

The objective is to accomplish all of this without a need for manual intervention at the client (the IBM Network Station) other than to do one or more power off and power on sequences.

So let's take a look at the steps involved and the recommended procedure.

There are two possible cases:

1. Clients that boot using NVRAM

This is probably the most common case for existing R2 clients, and it is also the simplest case.

2. Clients that boot using DHCP

For these clients, the procedure is a little bit more complicated than if using NVRAM. However, once clients start using DHCP with Release 3, any future migration should be easier.

### 3.4.3 Retargeting Clients That Boot Using NVRAM

Let's take a look at the simplest case first, that of clients that boot using NVRAM.

In this case, it is assumed that all IBM Network Station clients probably had their NVRAM parameters set according to the following values, since these were the defaults and recommended settings in R2:

- The boot protocol is TFTP.
- The boot directory is /nstation/.
- The configuration directory is /nstation/configs/.

The Set Boot Parameters panel in the Setup utility should look like the panel shown in the next figure:



SCRN06	IBM Network Station
	Set Boot Parameters
Boot File .....	
TFTP Boot Directory .....	/nstation/
NFS Boot Directory .....	
Configuration File .....	
Configuration Directory .....	/nstation/configs/
TFTP Order .....	1
NFS Order .....	Disabled

Figure 75. Release 2 Boot Parameters

The sample procedure that we describe next is based on NVRAM values being as shown in the above figure.

In this example, we identify each step that needs to be performed, but we also try to explain why each step is required or why it is done that way. This should provide sufficient details to allow you to modify these procedures if your environment is different than our sample scenario.

#### 3.4.3.1 General Procedure

The general procedure consists of three stages:

1. Prepare the server for the retargeting procedure.
2. Select a few pilot clients and have only these clients go through the retargeting process to verify that it functions properly.
3. Modify the server so that all clients are caused to go through the retargeting process.

The summary of the procedure is illustrated in the next figure:

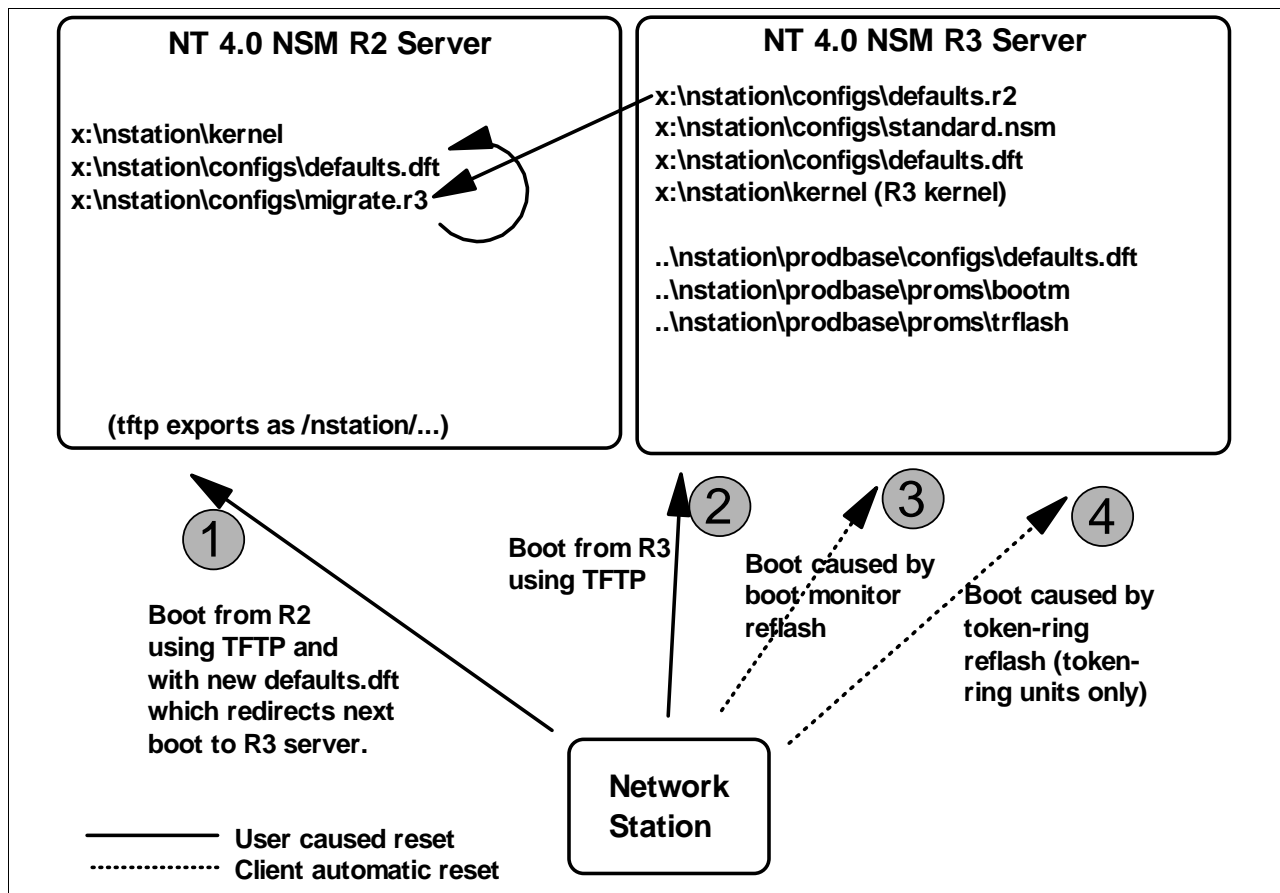


Figure 76. Summary - Retargeting NVRAM Clients - Dual Server Method

In the above figure, once we have prepared the servers and tested the retargeting procedure with one or more pilot clients (a detailed description is provided further down), the retargeting process for all clients are as follows:

1. A client does a normal boot from its old R2 server. This causes an update of its configuration data, which will cause the next boot to be directed at the R3 server.
2. The client reboots again, this time from the R3 server, and the configuration data that it downloads from that server indicates that a boot monitor update is required.
3. The boot monitor update takes place on the client, which causes an automatic reboot of the client, and the configuration data that it downloads from that boot indicates that a TRN flash update is required
4. If the client is a token-ring unit, a token-ring reflash is done, also causing an automatic reboot, which completes the retargeting procedure.

#### 3.4.3.2 Detailed Example

Here is the detailed procedure to follow to set up the proper retargeting procedures:

1. Copy the file x:\nstation\configs\defaults.r2 on the R3 server to x:\nstation\configs\migrate.r3 on the R2 server.

The contents of this file is the following, where x.x.x.x is the IP address of the R3 server:

```
set boot-tcpip-desired-server = "x.x.x.x"
```

This parameter sets the address of the boot server that should be used at the next boot.

**Note:** The name migrate.r3 is arbitrary; you can choose another if you wish, as long as it is not defaults.r2.

2. Select one (or more) client as a pilot client.
3. Change the pilot client's NVRAM settings so that the configuration file name is migrate.r3, as illustrated in the next figure:

SCRN06	IBM Network Station
Set Boot Parameters	
Boot File .....	
TFTP Boot Directory .....	/nstation/
NFS Boot Directory .....	
Configuration File .....	<b>migrate.r3</b>
Configuration Directory .....	/nstation/configs/
TFTP Order .....	1
NFS Order .....	Disabled

Figure 77. Changing the Pilot Client's NVRAM for Retargeting

**Note:** You may be asking yourself at this point why we do not simply change the boot host address instead of including a statement that will change it at the next boot. The answer is that we are building a procedure that has to be applicable to all clients and we want to avoid having to make manual changes at the client location. The manual change to NVRAM that we do here is required only for the pilot clients. When we do the actual retargeting of all the other clients, only a power off/power on sequence will be required because we will replace the defaults.dft file with the migrate.r3 file, thereby propagating this change to all clients.

4. Reboot the client.

The client boots via TFTP from the R2 server, loads the R2 kernel from /nstation/ (which translates into x:\nstation), reads the migrate.r3 file from /nstation/configs/ (which translates into x:\nstation\configs), which resets the boot server address to the R3 server.

5. Reboot the client again.

The client still boots via TFTP but this time it boots from the R3 server. It loads an uncompressed copy of the R3 kernel from /nstation/ (which translates into x:\nstation), tries to read migrate.r3 from the /nstation/configs/ (which

translates into x:\nstation\configs) directory on R3, but it does not find the file so it reads the default standard.nsm file instead, which it does find.

The standard.nsm file contains only one statement, that is, READ defaults.dft, and the defaults.dft file contains the following statements:

```
set boot-desired-source = nfs
set boot-nfs-directory = "/netstation/prodbase/"
set config-unix-directory = "/netstation/prodbase/configs/"
set file-initial-protocol-1 = nfs
set boot-prom-update-file="/nstation/proms/bootm"
set boot-token-ring-update-file="/nstation/proms/trflash"
```

Figure 78. Defaults.dft in \nstation\configs\ on the R3 Server

Notice that this file contains statements that set the boot protocol to NFS, the boot directory to the new R3 standard directory /netstation/prodbase/ and the configuration directory to /netstation/prodbase/configs/. However, it also requests an update of the boot monitor prom and the token-ring file.

6. The reading of the defaults.dft file causes the IBM Network Station to update its boot monitor prom, and therefore, to automatically reboot after the prom update, with no intervention on your part.

When the client reboots, this time it loads the R3 kernel, using NFS, from the /netstation/prodbase/ directory (which translates into x:\nstation\prodbase) and it reads configuration files from /netstation/prodbase/configs/ (which translates into x:\nstation\prodbase\configs).

7. If the unit is not a token-ring model, the retargeting process is completed.
8. If the unit is a token-ring unit, reading of the defaults.nsm file causes a reflash of the token-ring and the station reboots automatically.
9. The boot takes place this time as a normal R3 boot, using NFS to load the kernel load and to read the configuration files. The retargeting process is complete for this pilot station.
10. Once you are satisfied that the retargeting process works fine for one or more pilot clients, the last step is to retarget all remaining clients.

This is done by copying, on the R2 server, the contents of the \nstation\configs\migrate.r3 file into the \nstation\configs\defaults.dft. From that point on, this causes every client that boots from the R2 server to be automatically retargeted to the R3 server after doing two power off/power on sequences.

In other words, instead of having to manually change each of the clients's NVRAM settings to set the configuration file to migrate.r3 as we did for the pilot client, we do the equivalent by inserting the set boot-tcpip-desired-server statement into the defaults.dft file that all these clients are already set to read.

### 3.4.4 Retargeting Clients That Boot Using DHCP

For clients that boot using DHCP instead of NVRAM, the detailed procedure is as follows:

1. It is assumed that the DHCP server configuration has the following options set for all the R2 IBM Network Station clients:

- Option 66: IP address of the R2 server
  - Option 67: x:\nstation\kernel (TFTP path to the R2 kernel)
2. For each pilot client, create a client definition in the DHCP server configuration file, identifying the client through its MAC address, so that we can assign options only to this client without affecting all the other clients.

If client definitions based on MAC were already configured, then simply modify the existing definitions.

3. For the pilot clients only, set the following options:

- Option 66: IP address of the R3 server
- Option 211: tftp (String enclosed in quotes.) This is the boot protocol.

**Note:** If option 211 does not exist, you might need to create it first. See the *IBM Network Station Manager Installation and Use, SC41-0664* for instructions on how to define new DHCP options.

The boot monitor of the R2 clients actually does not recognize this option, but it is recognized by the R3 boot monitor, after the boot monitor is reflashed. This step is *critical*. Without it, the client reads the nfs value from the defaults.dft configuration file and the boot fails, causing a need to manually change the configuration on the client.

4. Reboot the pilot client.

The client receives from the DHCP server the R3 boot server address, and it ignores option 211. Its NVRAM settings were already set for TFTP anyway.

The client boots via TFTP from the R3 server, loads the uncompressed R3 kernel from x:\nstation on R3 and reads the x:\nstation\configs\defaults.dft file on R3, the contents of which are as shown in the figure below:

```
set boot-desired-source = nfs
set boot-nfs-directory = "/netstation/prodbase/"
set config-unix-directory = "/netstation/prodbase/configs/"
set file-initial-protocol-1 = nfs
set boot-prom-update-file="/nstation/proms/bootm"
set boot-token-ring-update-file="/nstation/proms/trflash"
```

Figure 79. Defaults.dft in \nstation\configs\ on the R3 Server

5. Because of the statement in the defaults.dft file that requests an update of the boot monitor prom (set boot-prom-update-file=), the prom is updated and the client is automatically triggered to reboot.
6. On reboot, the client contacts the DHCP server again to get its options.

Since the boot monitor is now at the R3 level, this time it does recognize the option 211 (which is set to TFTP) and this option overrides the settings specified in the configuration files read by the kernel.

**Note:** Even though these configuration files are read after the DHCP options have been received, the DHCP options take priority.

The client boots using TFTP from R3, reads the uncompressed kernel from x:\nstation again, but this time, it reads the configuration files using NFS from the \nstation\prodbase\configs directory. If it is a token-ring unit, a statement in

defaults.nsm causes a token-ring reflash, which automatically causes another reboot.

7. On reboot, the client contacts the DHCP server again to get its options.

The client boots using TFTP again (that option has not changed yet), but this time it is finally a normal boot in the sense that there is no reflash of the boot prom or token-ring.

8. At this point, if you have configured DHCP option 211 only at the client level, you can change option 211 to NFS for the pilot client *only* and reboot the client. This time, the client boots using NFS and loads the compressed R3 kernel from the \nstation\prodbase directory.

9. If all went well for the pilot clients, you are now ready to retarget all clients.

It is important to realize that all clients must use TFTP first in order to update their boot monitor prom. This is why option 211 must remain set to tftp for all clients until they have all had a chance to update their boot monitor prom.

This period could be fairly long, especially in large networks, where many users might be away on vacation, or on business, and it may take days or weeks before all users have actually gone through the retargeting process.

Only when all clients have been retargeted and had their boot prom updated can option 211 be changed back to NFS so that all clients then use NFS also to load the kernel.

Of course, if the DHCP configuration has broken down the clients into different subnets for example, there is always the possibility of specifying option 211 at a subnet level if all clients in that subnet have been retargeted, but the administrator must exercise caution to ensure that clients do not boot using NFS if their boot monitor prom has not yet been updated.

---

### 3.5 Single Server Migration Example

In a single server migration, the objective is to replace the old release (R2) of the IBM Network Station Manager with the new release (R3), *on the same machine*, while conserving all of the user accounts and user preferences from the previous release.

It is therefore an *in-place* update of the IBM Network Station Manager code, but it is also a migration because the directory structure of the new release is slightly different from the old, which requires some user preference data to be moved from the old directories to the new.

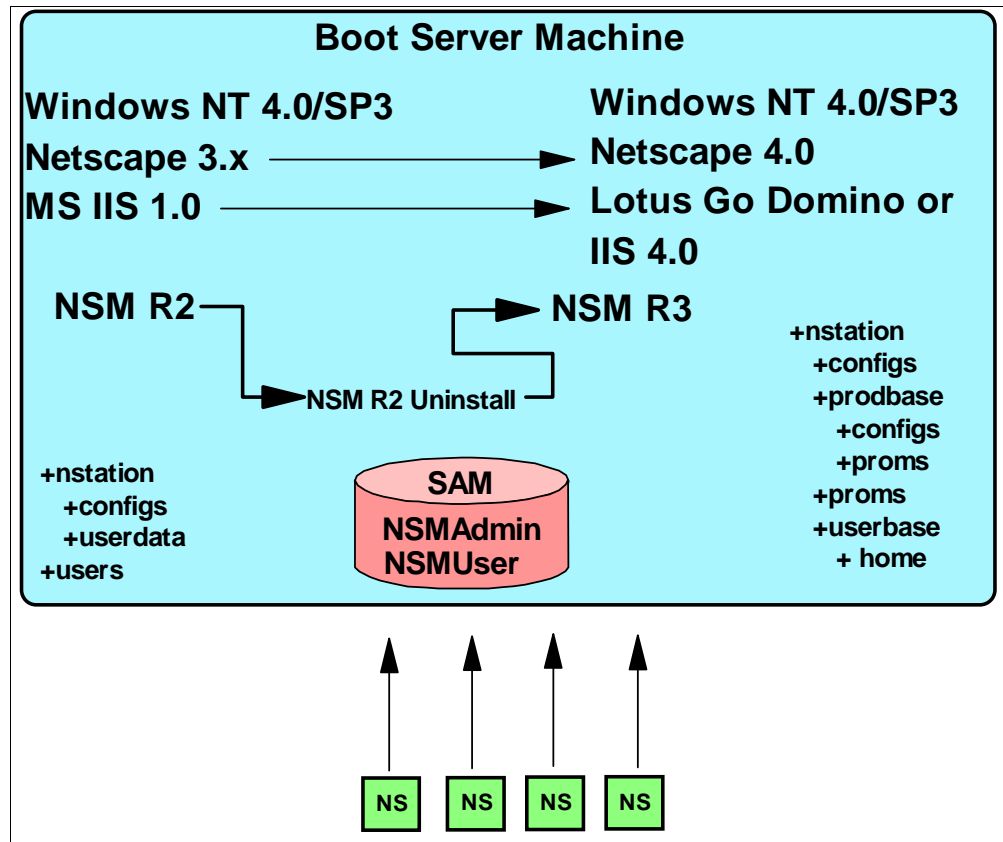


Figure 80. Single Server Migration Example

The install process accomplishes the following tasks:

- Preserves the user accounts that are part of the NSMAdmin and NSMUser groups by renaming these groups to NSMAdminTemp and NSMUserTemp. (This is required because the R2 uninstall process removes these groups.)
- Uninstalls all of the old products.
- Renames the NSMAdminTemp and NSMUserTemp groups back to their original names.
- Installs the new IBM Network Station Manager release and related code such as the eNetwork On-Demand Server.
- Based on the users present in the NSMAdmin and NSMUser groups, migrates all user preference data from the old files to the new files.

Following is an example of such a migration.

### 3.5.1 Server Migration

The server installation and migration steps are as follows:

1. Ensure that all users have logged off. This is the start of the down time period during which users will not be able to log on.
2. If the Windows NT 4.0 base system is not already at the Service Pack 3 level, install Service Pack 3.

3. Upgrade the prerequisite Web browser to either Netscape Navigator 4.0 or Internet Explorer 4.0 and the Web server to either IIS 4.0 or Lotus Domino Go Webserver.
4. Start the IBM Network Station Manager R3 installation process.
  - The install process detects the presence of the previous version and displays a panel, as illustrated in the figure below, identifying the old versions that were found:

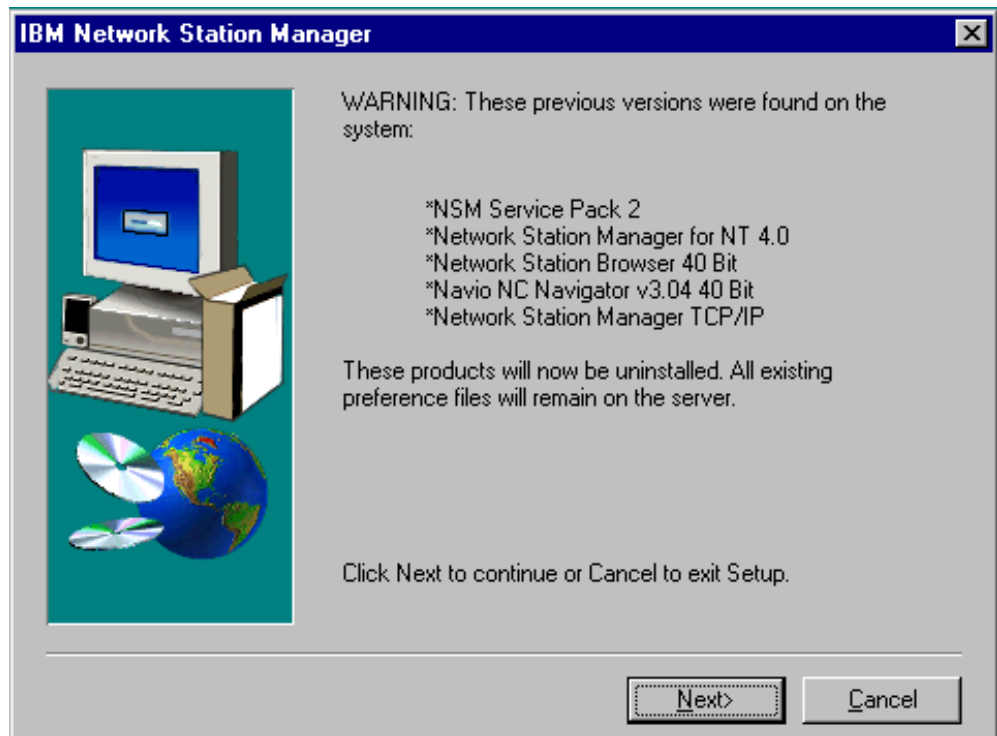


Figure 81. Detection of Old Versions

- After a click on **Next** to continue, you get the following progress panel.

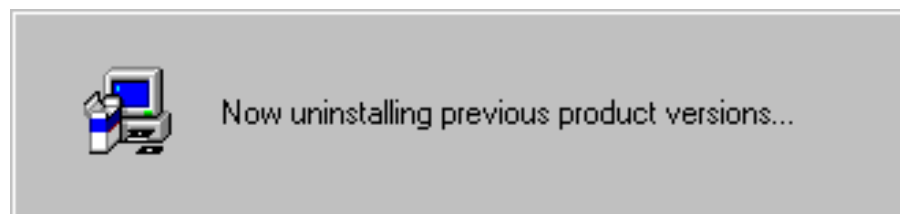


Figure 82. Progress Display - Uninstalling

- The uninstall process for every product is launched, and for every product, a confirmation prompt is displayed, such as the one displayed below:



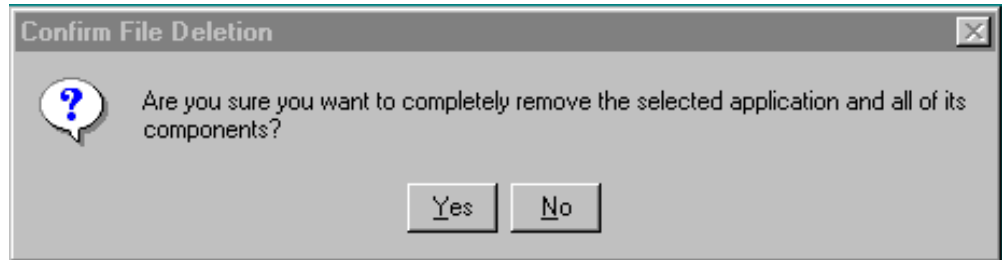


Figure 83. Removal Confirmation Panel

Then the normal unInstallShield removal progress panel is displayed after which you need to click **OK**.

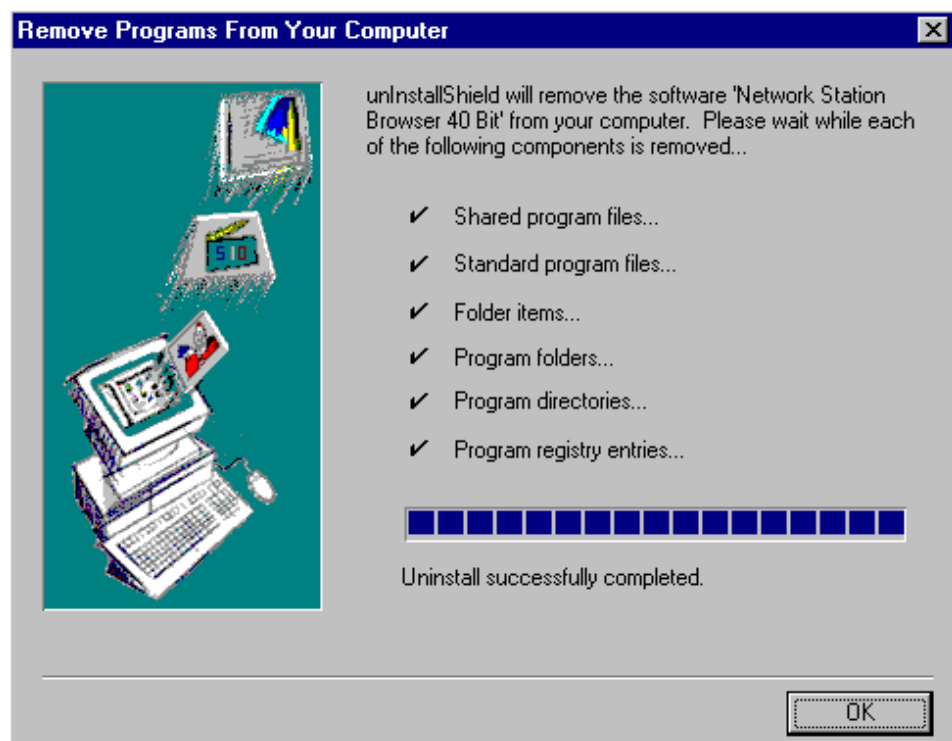


Figure 84. unInstallShield Removal Display

- This process is repeated for every product that needs to be removed. After all the NSM R2 products have been removed, the NSM R3 install process continues, and it renames the NSMAdminTemp and NSMUserTemp groups back to their original names.
5. After the uninstall of the old products completes, you are prompted to enter the path to where the old user preference files are located.

This field, called the migration path, is pre-filled (but can be changed by the user) by the install program if it has found any of the following:

1. If c:\{float}\nstation\Userbase exists, it sets the migration path to c:\{float}\nstation.

**Note:** The {float} directory indicates any directory that the user might have chosen as the install directory, for example, c:\mynetstation\nstation. Only

since the availability of R3 can such a directory be specified during the installation, so this is mainly for future migration when you will be going from R3 or R3+.

2. If c:\nstation\Userdata exists, then set the migration path to c:\nstation.
3. If c:\nstation\Userbase exists, set the migration path to c:\nstation.

In our example here, we had NSM installed on c:\ so we get the following panel:

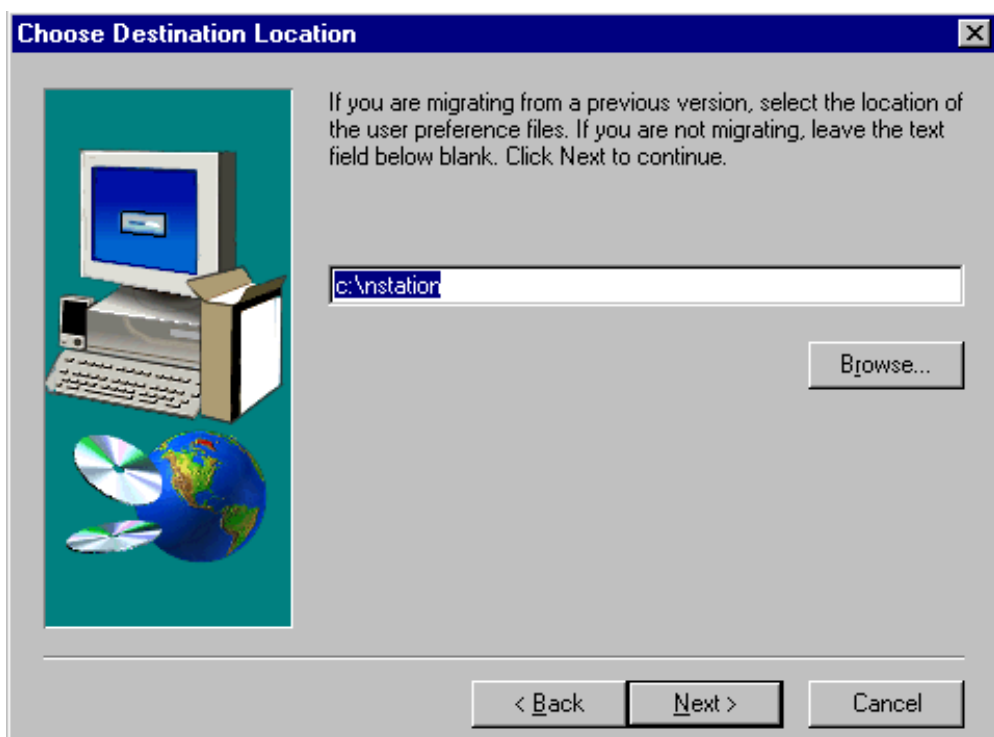


Figure 85. Location of User Preference Files to Be Migrated

**Note:** If you prefer to delay this migration step until after you have completely installed your new R3 code, you have the choice of leaving the migration path blank and to use the `nsmmigr.exe` utility later on to accomplish the same task independently of the install process.

6. The rest of the installation process is identical to a normal (non-migration) installation as described in 2.5.4, "Installation of IBM Network Station Manager" on page 28.

This completes the migration of the server from R2 to R3. The next step is the retargeting of the IBM Network Station clients. Note that in this case (single server migration), the retargeting process does not actually mean that we change the target server, since the server is the same physical machine, but we do need to update the boot monitor code on the clients to change the boot protocol to NFS and some of the directories, which is done as part of the retargeting process.

### 3.5.2 Retargeting Clients that Boot Using NVRAM

This is the simplest of the retargeting scenarios because it does not require any changes to the IBM Network Station configuration.

It is assumed that the IBM Network Station client's NVRAM was configured to boot using TFTP and that the boot directory was /nstation/.

The R3 installation process has automatically created R2 compatibility entries to allow this automatic retargeting process to take place.

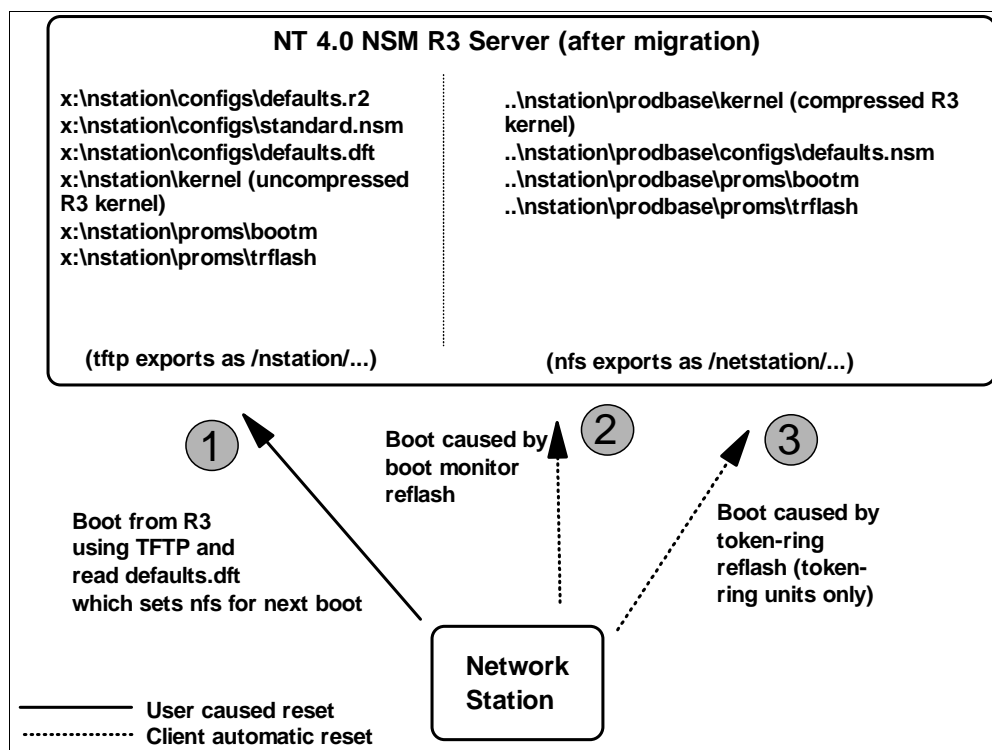


Figure 86. Single Server Migration - Retargeting NVRAM Clients

Here are the detailed steps taking place during the retargeting process:

1. Reboot the client to initiate the retargeting process. The client boots using TFTP, loads the uncompressed R3 kernel from /nstation/ (which translates into x:\nstation where x: is the drive where the NSM was installed) and it reads defaults.dft using TFTP from /nstation/configs/ (which translates into x:\nstation\configs).

This configuration file contains the following statements:

```
set boot-desired-source = nfs
set boot-nfs-directory = "/netstation/prodbase/"
set config-unix-directory = "/netstation/prodbase/configs/"
set file-initial-protocol-1 = nfs
set boot-prom-update-file="/nstation/proms/bootm"
set boot-token-ring-update-file="/nstation/proms/trflash"
```

Figure 87. Defaults.dft from \nstation\configs on R3 Server

The set boot-prom-update-file = "/nstation/proms/bootm" statement causes a reflash of the boot monitor code, where the new R3 boot monitor is loaded from x:\nstation\proms, which causes a reboot of the network station.

2. When the client reboots however, it now boots using NFS because this is the boot protocol that was set by the `set boot-desired-source = nfs` statement when the `defaults.dft` file was read the first time.

The client loads the compressed kernel this time from `/netstation/prodbase/` (which translates into `x:\netstation\prodbase\`) and then reads the configuration file, using NFS, from `/netstation/prodbase/configs/` (which translates into `x:\netstation\prodbase\configs`).

One of the configuration files read from `\netstation\prodbase\configs\` is `defaults.nsm`, which also contains the statement `set boot-token-ring-update-file="/netstation/prodbase/proms/trflash"` which causes a reflash for token-ring units.

3. If the unit is a token-ring unit, the token-ring is reflashed, which automatically causes a reboot. The client reboots, using NFS, loads the compressed R3 kernel, and then all the configuration files using NFS as well. The retargeting is complete for this unit.

If this is not a token-ring unit, the boot is completed and the retargeting of the station is complete.

If all goes well with one pilot client, then we can probably safely assume that all other clients, upon their next reboot, will also retarget properly. If some of the IBM Network Station clients had for some reason an NVRAM configuration different than all other units, then this might need to be investigated to see if the changes cause problems with retargeting.

### 3.5.3 Retargeting Clients That Boot Using DHCP

This process is identical to the dual server retargeting process that we describe in 3.4.4, "Retargeting Clients That Boot Using DHCP" on page 84, except that in step number 3, option 66 does not need to be changed to point to another server (R3) since it should already point to the correct server, given that we did not change the address of the server but just updated the code.

---

## 3.6 Migration/Installation Problems

Hopefully, your server migration from R2 to R3 should go without any problems.

However, as we have found during our experiments, some unforeseen problems can come up, especially if your Release 2 installation has been tampered with in some fashion.

We ran into a few cases where we were using an R2 server that we had used for experiments and to which we had made alterations that did not affect its operation status but that did effect its removability.

If any of the R2 uninstall processes encounter a problem and fail, the R3 installation process also fails.

You must then go into problem determination mode to find out why the uninstall is failing and to find a way to correct the situation.

If you restart the R3 installation process, after fixing the uninstall problem, the R3 install process displays only the products that remain to be removed. For example, the panel in the next figure shows that NSM TCP/IP and NSM SP2

remain to be removed as we had encountered a problem in the removal of the Service Pack 2, and tried to continue with the installation:

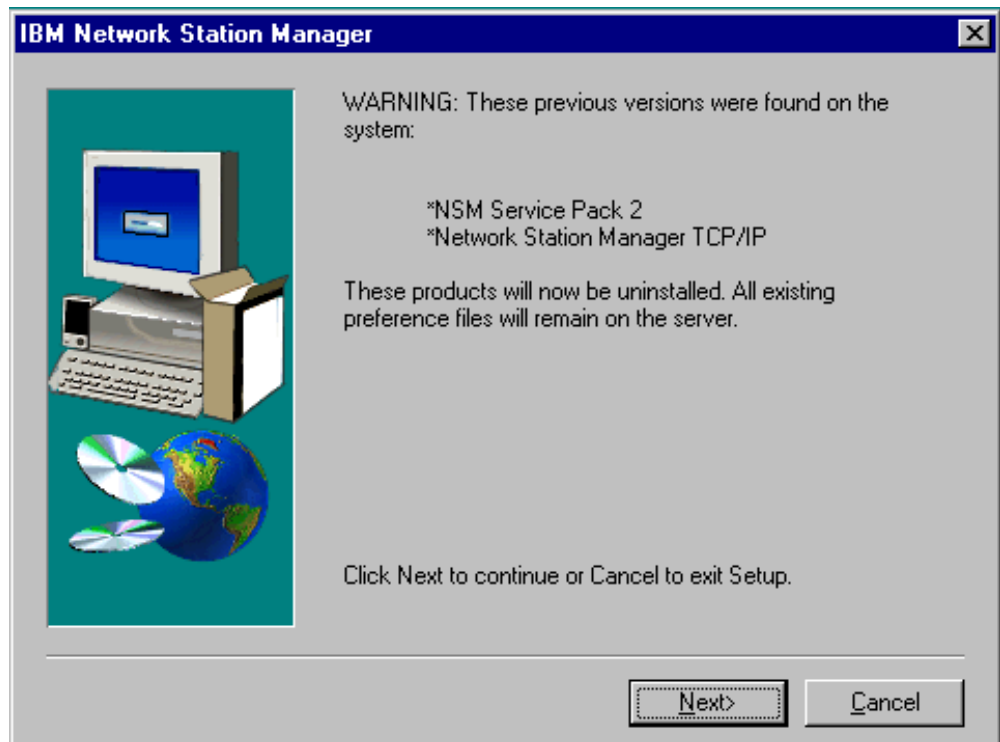


Figure 88. Detection of Old Versions, after an Interruption

In a severe case, you might have to manually remove every R2 product before attempting to restart the R3 installation process; this still allows you to continue and migrate your R2 data to R3 during the install process.

We also encountered cases where the Release 2 removal process, even though it appeared to complete, actually left components behind in the NT Registry that caused the R3 installation to fail later on.

The NSLD component seems to be particularly prone to this and we had to manually remove this service from the registry. In these cases, if at all possible, we recommend a re-install of the base operating system to make absolutely certain that you start with a clean base.

### 3.6.1 Migration Tasks

As a reminder, there are two important pieces of the installation that are considered migration tasks:

1. User accounts that are members of the NSMAdmin and NSMUser groups.

Before launching the R2 uninstall, the R3 install process renames the NSMAdmin and NSMUser groups to NSMAdminTemp and NSMUserTemp. This is because the R2 uninstall process deletes these two groups and the data needs to be saved because the R3 migration process uses the names of the users that are part of these groups in order to migrate the user preference data.

If you lose these groups, you can always recreate them manually before launching the R3 install process (see 3.6.3, "Using the NTNSMRR2.EXE Utility" on page 95).

For example, in one of our cases the groups were temporarily renamed but because the overall process was interrupted, new NSMAdmin and NSMUser groups were created while the NSMAdminTemp and NSMUserTemp were still there. So, we simply moved the members of the Temp groups to the newly created NSMAdmin and NSMUser groups.

**Note:** Remember that in R3, all users must be part of the NSMUser group. If a user is also part of the NSMAdmin group, he or she can be added to the NSMAdmin group as well, but he or she must be part of the NSMUser first otherwise that user will not be able to log on to an IBM Network Station.

## 2. Copying user preference data and home directories.

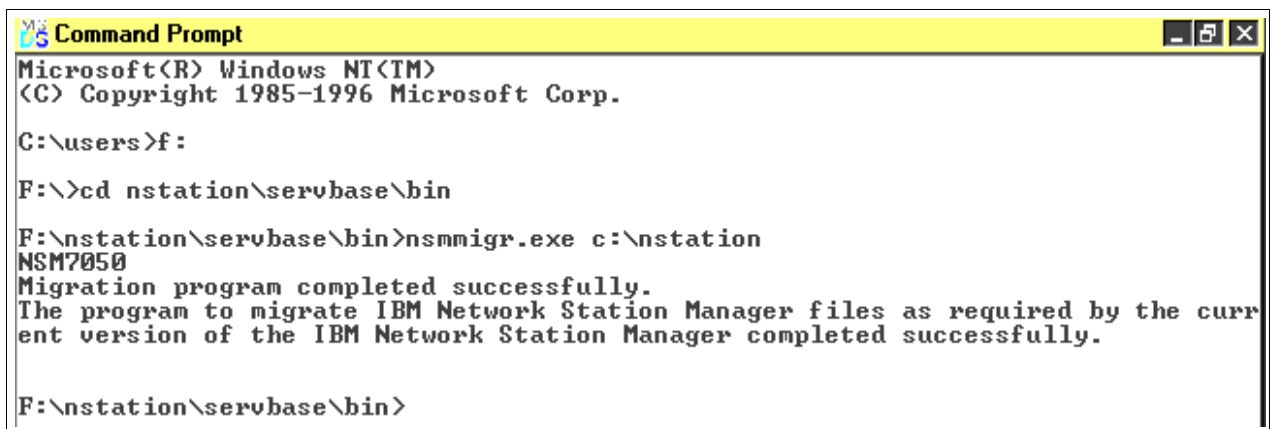
After the R3 process has created the new directory structure, it looks up the NSMAdmin and NSMUser groups, and for every user present in these groups, it copies the user data from the old directories to the new ones.

This process can also be done manually after the install process is completed by using the nsmmigr.exe utility located in \nstation\servbase\bin on an R3 system, as long as the old user preference files are still available. In fact, this process can be accomplished many times if required, since the old files are not modified in any way by this migration process.

### 3.6.2 Using the NSMMIGR.EXE Utility

In fact, due to our earlier problems with the NSMAdmin/NSMUser groups, our R3 install did not perform the migration because no users existed in these groups.

We therefore ran the utility, as illustrated below:



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\users>f:

F:\>cd nstation\servbase\bin

F:\nstation\servbase\bin>nsmmigr.exe c:\nstation
NSM7050
Migration program completed successfully.
The program to migrate IBM Network Station Manager files as required by the curr
ent version of the IBM Network Station Manager completed successfully.

F:\nstation\servbase\bin>
```

Figure 89. Running the NSMMIGR.EXE Utility

You can determine the success of this migration by examining the ..\nstation\userbase\home directory and the ..\nstation\users directory where you should have subdirectories for every user that was migrated.

For example, in the figure below, we installed under user bechard but we migrated users administrator, clauda and claudu using the utility.

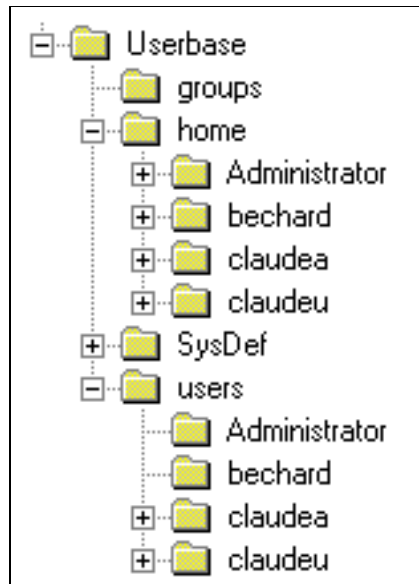


Figure 90. The \userbase\home and \users Subdirectories

### 3.6.3 Using the NTNSMRR2.EXE Utility

This utility, located in `..\nstation\servbase\bin` or on the CD-ROM in the `ntnsm\en\utility` directory, can be used to remove all the products of a Release 2 system.

Before it removes the NSM R2 product however, it renames the NSMAdmin and NSMUser groups to NSMAdminTemp and NSMUserTemp respectively in order to prevent their removal by the NSM R2 uninstall process, and renames them back to their original name after NSM R2 has been removed.

When should this utility be used?

1. If your R2 system was installed on a PDC and you are migrating it off the PDC to a stand-alone server or stand-alone attached to a domain as is recommended, then this utility can be used after the migration to remove the R2 products from the PDC without removing the NSMAdmin and NSMUser groups.

This should be the primary use of this utility.

2. It can also be used to remove an R2 system, *before* installing R3, and still be able to migrate afterwards because the NSMAdmin and NSMUser groups are still there and all the users have not been deleted.

**Attention:** However, we caution against using this utility in this fashion because our experience has been that if anything goes wrong during the uninstall, which often does, and the utility does not proceed to completion, rerunning it creates problems as it attempts to rename the user groups a second time.

One way to proceed cautiously, in single server migration, is to manually and individually remove all R2 products, except the IBM Network Station Manager itself, and then run the R3 install with migration.

In an R2 removal from a PDC, we would also use the utility only to remove NSM itself, after having removed all other products individually so that the utility has a better chance of completing normally.

3. This utility can be used to remove an R2 system after the migration is complete.

The tasks that the utility performs are illustrated in the following figure which shows a log of the activities generated by the utility. In this case, we ran it against a system that had NSM R2 installed and Service Pack 2. It did not have Lotus eSuite nor the IBM Network Station browser installed.

In this particular case, the utility ran fine, removed all of the products and properly saved our NSMAdmin and NSMUser users by renaming these groups before and after the removal of NSM R2.



```
Obtaining the install location of Network Station Manager on the hard disk.

Checking for the existence of eSuite WorkPlace for IBM Network Station on the system.
eSuite WorkPlace for IBM Network Station has not been detected on the system.

Checking for the existence of NSM Service Pack 1 on the system.
NSM Service Pack 1 has not been detected on the system.

Checking for the existence of NSM Service Pack 2 on the system.
NSM Service Pack 2 has been detected on the system.
Uninstalling NSM Service Pack 2 from the system...
Completed uninstall of NSM Service Pack 2.

Checking for the existence of Network Station Browser 40 Bit on the system.
Network Station Browser 40 Bit has not been detected on the system.

Checking for the existence of Navio NC Navigator v3.04 40 Bit on the system.
Navio NC Navigator v3.04 40 Bit has been detected on the system.
Uninstalling Navio NC Navigator v3.04 40 Bit from the system...
Completed uninstall of Navio NC Navigator v3.04 40 Bit.

Successfully renamed NSMAdmin group.
Successfully renamed NSMUser group.

Checking for the existence of Network Station Manager on the system.
Network Station Manager has been detected on the system.
Uninstalling Network Station Manager from the system...
Completed uninstall of Network Station Manager.

Successfully restored NSMAdmin group.
Successfully restored NSMUser group.

Checking for the existence of Network Station Manager TCP/IP on the system.
Network Station Manager TCP/IP has been detected on the system.
Uninstalling Network Station Manager TCP/IP from the system...
Completed uninstall of Network Station Manager TCP/IP.

Checking for the existence of IBM DHCP Driver on the system.
IBM DHCP Driver has been detected on the system.
Uninstalling IBM DHCP Driver from the system...
Completed uninstall of IBM DHCP Driver.
Reboot your system now to complete the uninstall
of Network Station Manager and associated products.
```

Figure 91. Output of the NTNSMRR2.EXE Utility

### 3.7 Migrating Custom R2 Configuration Files

If you have configuration files from Release 2 that were manually edited, these manual changes need to be manually migrated, assuming that they need to be retained in Release 3 configuration files.

**Note:** The information below has been reproduced for your convenience from documents available at [www.ibm.com/nc/pubs](http://www.ibm.com/nc/pubs) under Advanced User Information.

So, the first task is to examine these manual changes and to consider why they were changed in the first place:

1. Many parameters may have been manually added to configuration files in R2 because these parameters were not supported by the IBM Network Station Manager in Release 2.

Therefore, these changes may no longer be required if these parameters are now supported by the IBM Network Station Manager in Release 3. In that case, the recommendation is to replace these manual changes by configuring the equivalent parameter through the IBM Network Station Manager application.

Note that a parameter that was manually added in an R2 file can be retained and added to one of the back door files available in Release 3; however, this approach is not recommended because you are only postponing the problem to the next migration. It is much more preferable to let this parameter be configured by the IBM Network Station Manager so that it ends up in one of the files handled by the NSM and therefore automatically migrated in the next release without any manual intervention on your part.

2. Some parameters that were manually added to configuration files in Release 2 may now conflict with settings that IBM changed or added for Release 3. It is therefore recommended you examine the Release 3 shipped configuration files to see if any of your manual changes override a shipped setting.
3. If your Release 2 files were manually edited in order to provide for a single full-screen session to a host or to a WinCenter server, it most likely disabled the Network Station login program, which is not the recommended way to handle this requirement in Release 3.

Please refer to Chapter 12, "Full-Screen Solutions" on page 215 for the proper way to do this in Release 3, which is to allow the network station login program to run, so that it can properly set environment variables, etc. but to suppress the IBM Network Station login dialog.

Follow the steps below as the recommended procedure:

1. Save a copy of all your Release 2.5 files that were manually modified.
2. Remove all statements that were manually added to the original Release 2.5 files. A copy of these original R2.5 files can be obtained from the following Web site:

<ftp://ftp.software.ibm.com/as400/pubs/netstat/config/>

3. Install Release 3.
4. Move the changes that were manually added to the Release 2.5 files (that is, only those that should be retained) to the Release 3 files, according to the following table:

<b>In Release 2.5, if you changed:</b>	<b>For Release 3, move the added or changed statements to:</b>
nstation\configs\standard.nsm, required.nsm, control.nsm, hosts.nsm or defaults.nsm	..\nstation\prodbase\configs\defaults.dft
nstation\configs\"name\" or \"name\".nst	..\nstation\prodbase\configs\"name\".trm
nstation\configs\"username\".nsu	..\nstation\prodbase\configs\"username\".usr
nstation\mods\Login\MRI2924\Login	..\nstation\prodbase\configs\nsl.dft
nstation\ProdData\SysDef\NCDwm\pref nstation\userdata\SysDef\NCDwm\pref, or nstation\userdata\"username\"NCDwm\pref	..\nstation\userbase\SysDef\pref.dft
nstation\ProdData\SysDef\NS3270\pref nstation\userdata\SysDef\NS3270\pref, or nstation\userdata\"username\"NS3270\pref	..\nstation\userbase\SysDef\pref.dft
nstation\ProdData\SysDef\NS5250\pref nstation\userdata\SysDef\NS5250\pref, or nstation\userdata\"username\"NS5250\pref	..\nstation\userbase\SysDef\pref.dft
nstation\ProdData\mods\NAV\pref, nstation\ProdData\SysDef\NAV\pref, nstation\userdata\SysDef\NAV\pref, or nstation\userdata\"username\"NAV\pref	..\nstation\userbase\SysDef\NAV\pref.dft
nstation\ProdData\SysDef\startup.nsm, nstation\userdata\SysDef\startup.nsm, or nstation\userdata\"username\"starup.nsm	..\nstation\userbase\SysDef\startup.dft

Table 4. Migrating Manual Changes from Release 2.5 to Release 3

### 3.8 Migrating the Boot Monitor Prom

If you have a station that is/was not involved in the retargeting process, and you need to start using this station with R3, but it is still at the R2 level of the boot monitor prom, what should the procedure be?

Assume for example that the station is at boot prom level 2.9.7. You have two choices here:

1. You can set the configuration data as it was normally on an R2 station, with the boot protocol as TFTP, boot directory as /nstation/ and configuration directory as /nstation/configs/.
2. You can change the boot protocol to NFS, boot directory to /netstation/prodbase/ and configuration directory to /netstation/prodbase/configs/.

In either case, the station boots from the server, the boot prom is updated from the previous level to 3.0.1, and the station is rebooted. After the reboot, the new setup utility (at Release 3 level) now shows the boot protocol as NFS (NFS order is 1, TFTP order is disabled), and the boot directory as /netstation/prodbase/.

The setup utility configuration data shows the first configuration directory as /netstation/prodbase/configs/, as it should for R3, and the second configuration directory as /nstation/configs/. The order is NFS first, TFTP second.

There is a slight difference in the boot process though. As in case 2, the configuration files will be read before the kernel determines that it needs to

update the prom; whereas in case 1, this was done immediately after loading the kernel.

### 3.9 Changing to DHCP Remotely

If all your IBM Network Stations were booting using NVRAM, and you wish to change them all to booting using DHCP, you can use the IBM Network Station Manager to set a parameter that causes the IBM Network Station to use DHCP the next time it boots.

This parameter is in the **Setup Tasks=>Hardware=>Workstation=>Boot Parameters** section, as illustrated in the figure below:

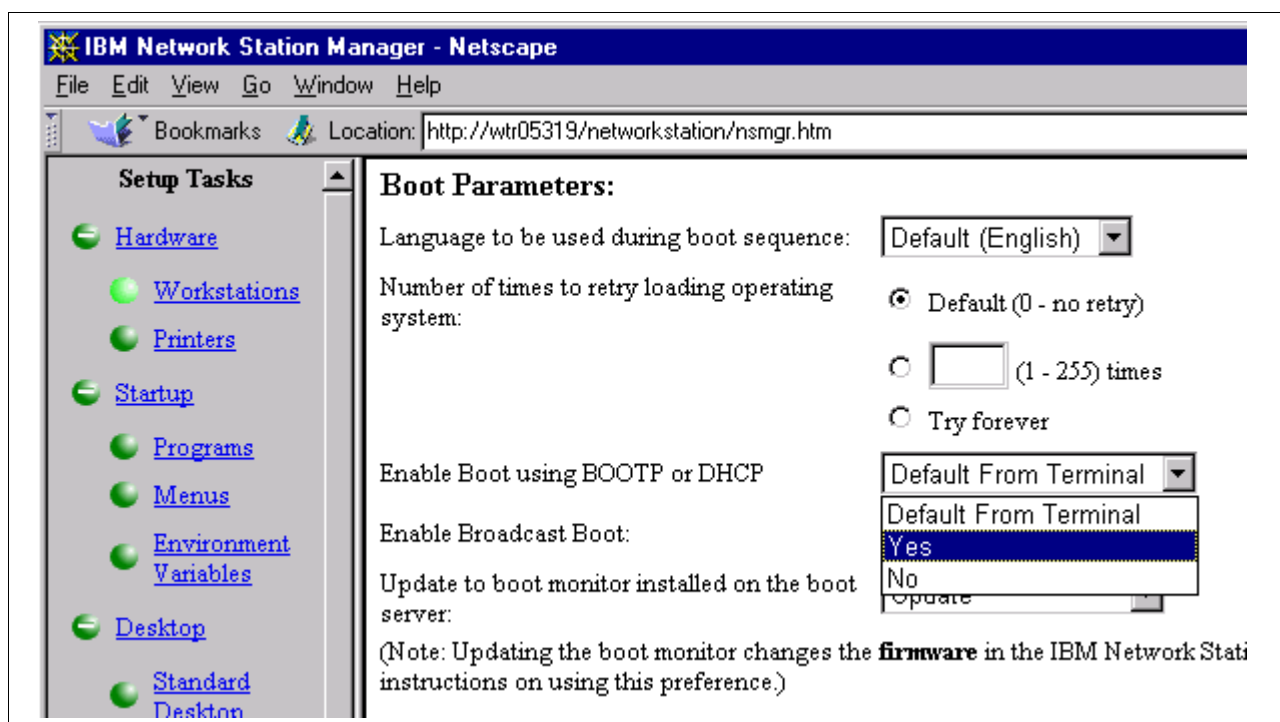


Figure 92. Boot Parameters - Enabling Boot Using DHCP

Set the Enable Boot using BOOTP or DHCP to Yes and the station is set after one more reboot to use DHCP as the boot method.

---

## Chapter 4. Separation of Servers

This chapter deals with what is commonly referred to as the *separation of servers*, or the ability for an IBM Network Station to get its required operational files from multiple servers during the overall boot process.

In summary, we discuss the following topics:

- What is separation of servers?
- What are the potential benefits?
- What are the different types of servers?
- An example and how to configure it.
- How is it implemented? The technical details behind it.

---

### 4.1 What Is Separation of Servers?

Separation of servers is the ability for an administrator to use more than one machine (and these machines may have different operating systems) in order to provide the services required by an IBM Network Station to operate properly.

The services required by an IBM Network Station include, for example:

- Getting an IP address, which is provided by a DHCP server
- Getting an operating system (kernel), which is provided by a boot server (sometimes also referred to as a *base code server*)
- Getting application modules, which is provided by a boot server
- Getting station configuration information, which is provided by a terminal configuration server
- Getting a user authenticated, which is provided by an authentication server

In the previous release of the IBM Network Station Manager, there were only two types of servers involved in this process: a DHCP server to supply network address information and a boot server to supply everything else.

With Release 3, the services that were provided by the boot server in Release 2 can now be supplied by three different servers that are called the boot or base code server, the terminal configuration server and the authentication server. Basically, the boot server provides the kernel, application modules and font files. The terminal configuration provides the system-wide hardware configuration files and the authentication server provides authentication services, user and group configuration files as well as home directories for saving user preferences.

Of course, all services can still be provided by a single server on a single machine, if desired, but the ability to dedicate separate servers to different tasks provides the administrator with a lot more flexibility in the administration of his or her network of IBM Network Stations.

For example, in the next figure, we have a corporation with a headquarter location several divisions, each division having several branch offices.

As a policy, this corporation controls the addresses in the network at the corporate level; therefore, one DHCP server has been set up at the corporate level and all stations obtain their network data from one DHCP server.

Since all stations have the same basic system-wide defaults, it has also been decided to put a configuration server at the corporate level.

However, the divisions retain control on their individual users, and therefore, users go to a division level authentication server for their authentication and user preferences.

Finally, since each division is remote from the divisional headquarters, it has been deemed preferable to have a boot server in each branch office on the local LAN.

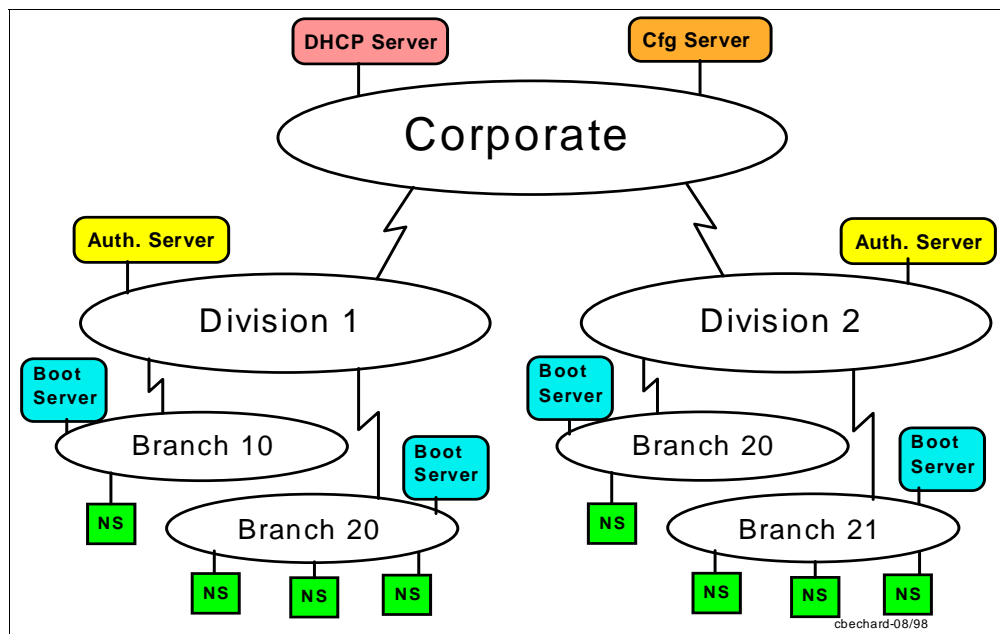


Figure 93. A Sample Separation of Servers Scenario

How a network is actually designed strictly depends on the real environment and the policies that are applicable to a particular corporation, so the above scenario is only an example to illustrate the concept of the separation of servers and what could be achieved, and may not necessarily be representative of a real solution.

## 4.2 Objectives of Using Separate Servers

So why would anyone decide to use separate servers?

There are many reasons for distributing the server roles and functions across multiple machines. Generally, it provides a lot more flexibility in the overall structure and organization of the network, and different organizations will have different reasons for adopting some of these functions, dependent on their own specific environments.

However, in all cases, there are probably three primary reasons that we can highlight for using separate servers, which are:

- Load balancing
- Centralized administration
- Ability to roam

Each of those is explained in more details below.

#### 4.2.1 Load Balancing

Some of the files that need to be initially downloaded to an IBM Network Station during the boot process, such as the kernel and the application modules, can be quite large.

In large network environments, the ability to distribute copies of these large files to many physical servers gives the flexibility to have groups of IBM Network Stations boot from different servers in order to balance the load between multiple machines.

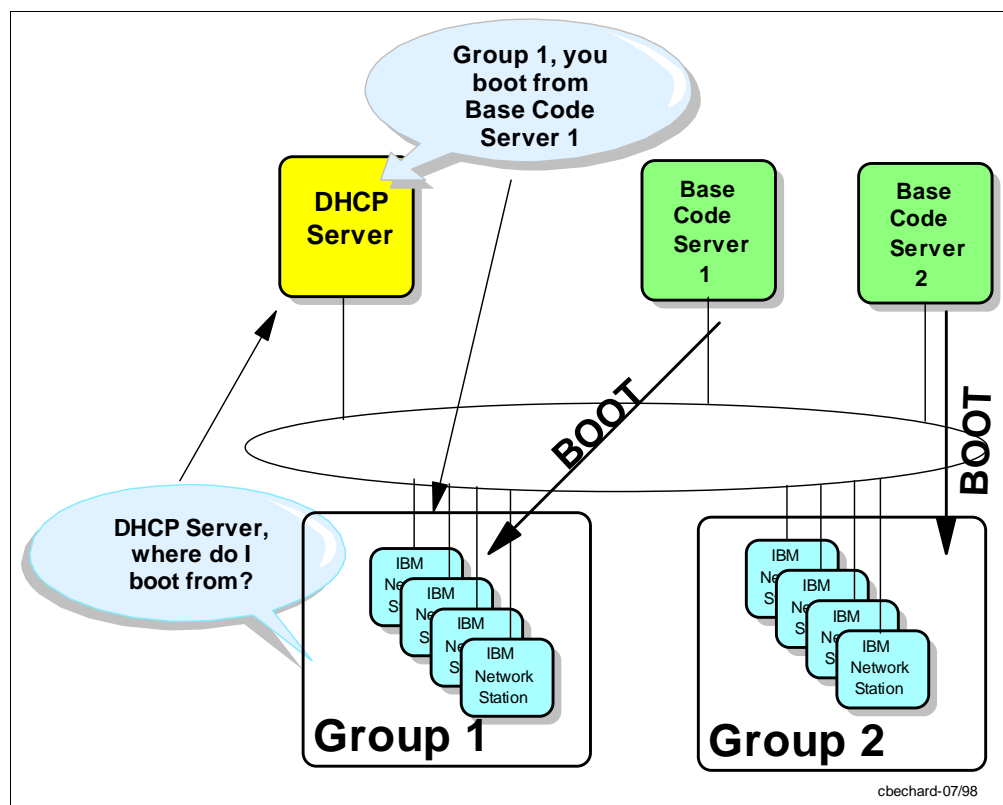


Figure 94. Load Balancing

The IBM Network Station obtains the address of the boot server that it should use from either a DHCP server or directly from the local configuration data (NVRAM configured through the Setup Utility).

In the figure above, the DHCP server is configured in such a way that when an IBM Network Station that belongs to an entity called Group 1, for example, asks a DHCP server for an IP address, the DHCP server can be configured to direct the station to boot from a specific base code server, in this case base code server 1.

Similarly, stations belonging to Group 2 can be directed to boot from base code server 2, thereby allowing the balance of the load between multiple base code servers.

#### **4.2.2 Centralized Administration**

Most organizations have branch offices scattered throughout the country that have a local area network implemented in the branch office, which is linked into a central corporate location via a wide area network type of connection.

As illustrated above in Figure 93 on page 102, it may sometimes be appropriate to consolidate the administration of the IBM Network Stations by centralizing the DHCP service and terminal configuration at a central level.

This can be accomplished while also distributing the authentication process at a divisional level, and still leave the actual boot services (downloading of the kernel and application modules) at a local level to benefit from the higher LAN speeds available from the local branch LAN.

In that case, separating the base code server from the terminal configuration server and from the authentication server provides the required mechanism to accomplish these objectives.

So, flexibility in the overall administration of the environment is a key benefit of this technique.

#### **4.2.3 Roaming**

Roaming is the ability for an IBM Network Station to get its user configuration data and preferences from a server other than the server from which it obtained its base code or other than a local authentication server, and typically in fact from a machine situated at a remote location.

This gives the flexibility for a user to roam, using different physical IBM Network Stations in different physical locations (which are booted from local servers) and yet be able to retrieve his or her own user-specific configuration and preferences from a remote server, most likely located at his or her home base location.



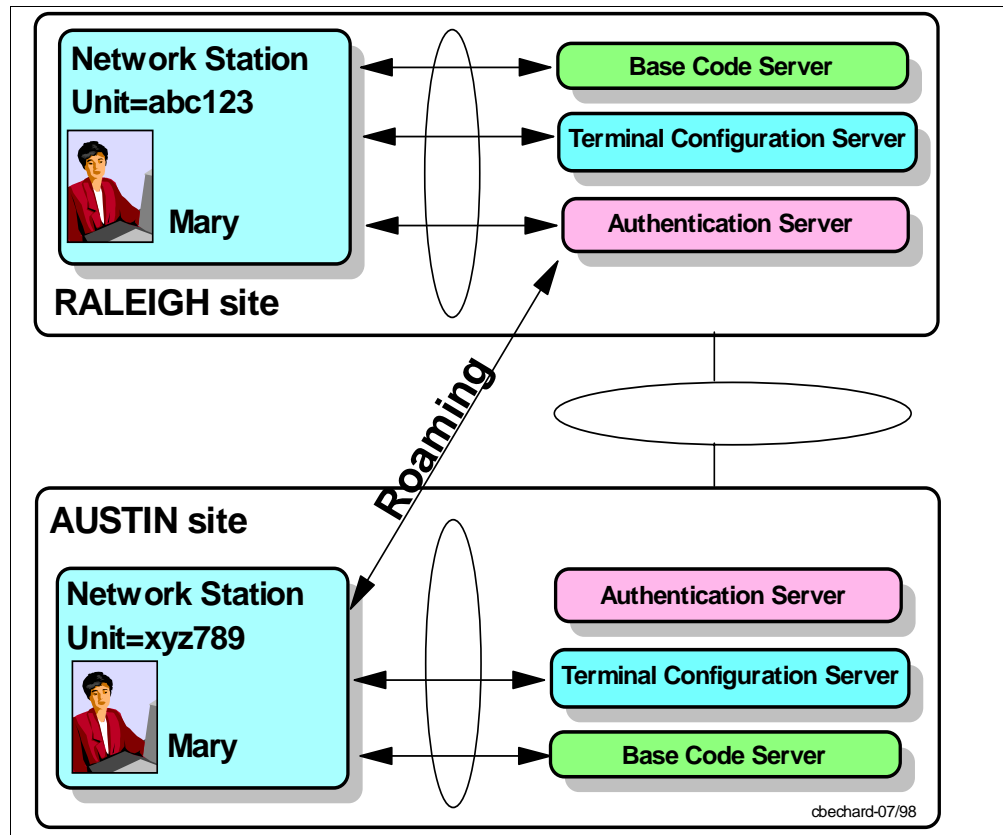


Figure 95. Roaming

In other words, as illustrated in the figure above, Mary, a user normally based in Raleigh, is currently visiting in Austin for a business meeting. When normally using her IBM Network Station in Raleigh, Mary's station is booted from a base code server physically located on her local network, and the station's configuration data is also retrieved from a local terminal configuration server. When she logs on, she is authenticated by her local authentication server.

When Mary leaves Raleigh and travels to Austin for a meeting and sits down at a local IBM Network Station located in the conference room in Austin, that IBM Network Station is booted from a base code server located on the local Austin network, and it retrieves its local terminal configuration data (for this particular physical unit) from a server also located on the local network. However, when Mary is presented with the login screen, she may select the Roaming button in order to ask that her authentication be done from her normal authentication server located in Raleigh as the source of her user configuration files.

This way, Mary benefits from being able to use a familiar desktop with all of her normal user preferences. The administrator, on the other hand, avoids having to define a user ID for Mary on the local Austin authentication server.

In the last example we have just mentioned a lot of different server names, so let us now take a look at the definition of each of these servers.

---

## 4.3 Types of Servers - Definitions

Before we go further into this topic, it is probably best to start with a definition of each type of server that is used in a IBM Network Station Manager environment so that we all use the same terminology and understand what each type of server provides in terms of files or information to be downloaded to the IBM Network Station.

### 4.3.1 DHCP Server

The DHCP server provides the initial networking configuration data that is required by the IBM Network Station in order to start its boot process.

This configuration data consists of:

- Its IP address  
This is the IP address that the IBM Network Station should use when inserting into the network.
- Subnet mask
- Gateway IP address
- Mount point for the base code server  
This consists of the IP address of the base code server, the protocol to use when contacting that server (NFS, TFP or RFS/400), and the directory where the required files are located.
- Name and directory of the kernel file
- DNS domain name and DNS server
- Mount point for the terminal configuration server  
This consists of the IP address of the terminal configuration server, the protocol to use when contacting that server (NFS, TFP or RFS/400), and the directory where the required files are located.

If you want to separate the base code server from the terminal configuration server, a BOOTP server cannot be used because it does not support the sending of all the above specifications to an IBM Network Station.

Using a DHCP server is always the preferred method for an IBM Network Station to get its network configuration data. However, if a DHCP server is not available or not possible, the Setup utility of the IBM Network Station can be used to enter the required network and boot configuration data into its NVRAM. We provide an example of using NVRAM in this chapter.

The advantages of using a DHCP server (as opposed to booting from NVRAM) are:

- There is no need for the administrator to physically enter configuration data at each station. The IBM Network Station is pre-configured, out of the box, to request its configuration data from the network so that no local administrative tasks are required.

This may not be very important when only a few stations are involved, but it is a very significant advantage when dealing with a large number of stations.

- After the initial implementation, in the event that changes are required in any of the initial network configuration data (for example, the IP address of a base code server), it is a very easy task to implement this change in a central fashion by a simple configuration change at the DHCP server. Otherwise, a qualified individual must be sent to the physical location of each station in order to implement the change in the local configuration.
- When it becomes necessary to perform changes for network performance and load balancing considerations, this can easily be implemented through changes in the centralized DHCP server configuration, whereas this is simply not practical in an NVRAM boot scenario.
- There are also all the traditional advantages of DHCP, such as the reuse of IP addresses, that apply as well to a network of IBM Network Stations. Please refer to Chapter 10, "Dynamic Host Configuration Protocol (DHCP)" on page 175 for additional details on DHCP.

### 4.3.2 Boot Server

The boot server provides the base operating system of the IBM Network Station (the kernel), all application modules for the native applications such as the 3270 and 5250 emulators, the NC Navigator browser, etc., the fonts file, and the Java classes.

In fact, the base code server provides most of what resides in the PRODBASE directories such as the mods, proms, fonts, java and nls directories on the server.

#### 4.3.2.1 Boot Server Special Install

Note that if a boot server is used only to supply the kernel, the application modules and the font files, then there is no requirement to have any of the prerequisite products installed on that server, such as the IBM Network Station Manager program installed because there are no configuration files to be managed in this environment.

The only prerequisites on that server then are the Windows NT 4.0 base operating system with Service Pack 3 and the NFS server. The IBM Network Station Manager install process does have a function allowing the installation of all the components necessary to a base code server without the need for the userbase directories for example.

This install is done using the setup.exe /bs (which stands for boot server) command from the command prompt. Please refer to 2.13, "Boot Server Special Install" on page 57 for more details.

### 4.3.3 Terminal Configuration Server

The terminal configuration server provides the terminal-based hardware preferences. These are all the configuration files that set the characteristics of the terminal (the IBM Network Station) itself, regardless of which user is actually using it. In other words, this is all the configuration data *before* the user identifies itself by logging in.

These are typically the files residing in /netstation/prodbase/configs, such as standard.nsm, required.nsm, control.nsm, hosts.nsm, defaults.nsm, defaults.dft, etc., most of which are managed by the IBM Network Station Manager.

Note that defaults.dft and "name".trm, which are user-editable files, also reside here, so the configuration server is not only for \*.nsm files.

#### 4.3.4 Authentication Server

The authentication server provides basically all the configuration data that is specific to a particular user.

In some documents, you might possibly see references to a home server, or to a user configuration server, or login server. Although it might be possible to further separate server functions by assigning a specific user configuration server to provide NSM managed application preferences, startup files and user configuration preferences, and a home server to provide non-NSM managed user configuration files and a place for the users' home directory, all of these functions are provided at the moment by one server which we call, in this document, the authentication server. This server performs three basic tasks:

1. Authenticates users

This consists in verifying that the user ID and password supplied by the user are indeed valid and authorized to use the system. This is done by the network station login server executing on the authentication server and interfacing with the NFS subsystem and the Windows NT Security subsystem, and then communicating with the network station login client executing on the IBM Network Station.

2. Provides the user-specific configuration files that contain:

- The user-specific hardware preferences

These are hardware preferences that are in addition to what the system defaults preferences are, such as left-handed mouse operation.

- The user-specific application preferences

Here also there are application-related preferences, specific to a user, that may be needed in order to override the system defaults provided.

- Startup files

These startup files contain the configuration information necessary to set some environment variables, building the items on the menu bar for example, and autostart applications.

Many of these specifications are user-specific and therefore, can only be determined after the user identifies himself or herself through the login process.

3. Provides the user with a home directory

The user has two directories on the authentication server:

- One is /userbase/users/"username", which contains NSM managed user preference files such as "username".nsu, envvars.nsm, statrup.nsm, as well as non-NSM managed files such as "username".usr. It also contains user application preference files such as /Nav/pref.
- The other is /userbase/home/"username", which is really the default directory to store anything that belongs to this user. For example, browser preferences such as bookmarks, emulator playback/record, files from eSuite, etc.

#### 4.3.4.1 Authentication Server Special Install

There is a special install option on the setup.exe (/as) for an authentication server installation. See 2.14, "Authentication Server Special Install" on page 59 for more details as well as the Authentication Server section on page 114.

---

### 4.4 Other Server Types

There are other server types that may play a role in a network of IBM Network Stations but that are not necessarily directly related to the IBM Network Station Manager. These are general types of servers used in any network.

#### 4.4.1 Application Server

An application server provides application services, which can take many forms. In the case of the IBM Network Station, there are two basic cases:

1. The application resides and executes on the station itself, but goes to a target application host.

This is the case of native applications such as the 3270/5250 emulator and the NC Navigator browser.

The application code itself is downloaded from the base code server to the station either at boot time or when the application is started by the user. From that point on, it requests services from a remote S/390 host for 3270 for example, or an AS/400 for 5250, or any Web server for the browser. In these cases, these remote hosts are the application servers.

Java applications are a bit special in the sense that they represent a case where the application could execute entirely on the station itself.

2. The application is an X-windows application that resides and executes on a remote server or application host and sends the display output back to the monitor attached to the IBM Network Station.

This is the case of using AIX applications or Windows applications from a multi-user server such as WinFrame (WinCenter) or Windows NT Server 4.0, Terminal Server Edition.

#### 4.4.2 File Server

Since an IBM Network Station, by definition, does not have any real local disk storage capability, one or more file servers can be defined so that they can be used by any application executing on the IBM Network Station that requires storage capability.

These servers can be any of the servers defined above or separate dedicated servers. In order to access these servers, the administrator simply adds entries into the local file-service-table identifying the IP address of the file server, the protocol to be used and the alias to be used to access the files.

See 4.6.1, "Access to Server Directories" on page 118 for additional details on how the file service table functions.

#### 4.4.3 Print Server

A print server provides a target where applications on the IBM Network Station can send their output to be printed.

At the time that a user requests the application to print, he or she gets a printer selector panel that lists the available printers. Some of these printers can be local printers attached to the IBM Network Station, or they can be remote printers attached to print servers.

This list of available printers is configured by the administrator using the IBM Network Station Manager.

Remote print servers can also be used to transform data from one type of data stream to another (such as from PostScript to PCL for example) in the case where the locally attached printer does not support the type of data stream produced by the application.

Examples of using local and remote printers can be found in *IBM Network Station Printing Guide, SG24-5212*.

#### **4.4.4 Summary**

In summary, the IBM Network Station can use one or more of the many types of servers we have just defined.

In the simplest case, it could in fact use just one server on one machine which would provide the services of all the server types we have identified. For example, a Windows Terminal Server Edition server can function as a DHCP server, a base code server, a terminal configuration server, an authentication server, an application server for Windows applications, a file server and a print server.

In more complex cases, each of these servers could indeed be a separate server residing on a different physical machine.

Finally, between these two extremes are all the combinations and permutations that one can envisage where these servers can be combined into one or more physical machine.

In the figure below, we summarize the server types we have discussed and the general services they provide.

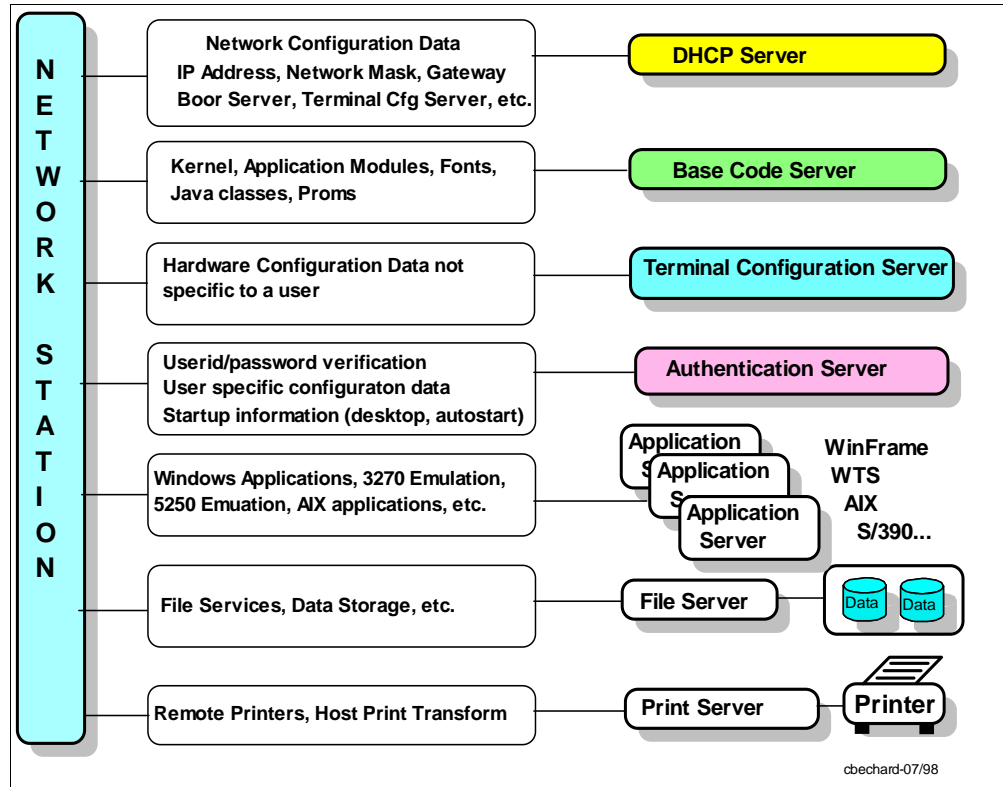


Figure 96. Server Types - Summary

We now can take a closer look at those servers involved in the booting process of an IBM Network Station, the DHCP, base code, terminal configuration and authentication servers, in order to gain a more precise and detailed understanding of the services provided by each and the benefits gained from using, or not using, separate servers.

## 4.5 An Example of Separation of Servers

Here is a simple example to illustrate the basics of how to configure to use separate servers. In this case, we use three servers:

- A boot server, located at IP address 9.24.104.175 with an IP host name of wtr05319.itso.ral.ibm.com

**Note:** Note that if this has been installed as strictly a base code server, it does not need to have the IBM Network Station Manager installed.

- A configuration server, located at IP address 9.24.104.39 with an IP host name of wtr05140.itso.ral.ibm.com
- An authentication server, located at IP address 9.24.104.47 with an IP host name of wtr05118.itso.ral.ibm.com

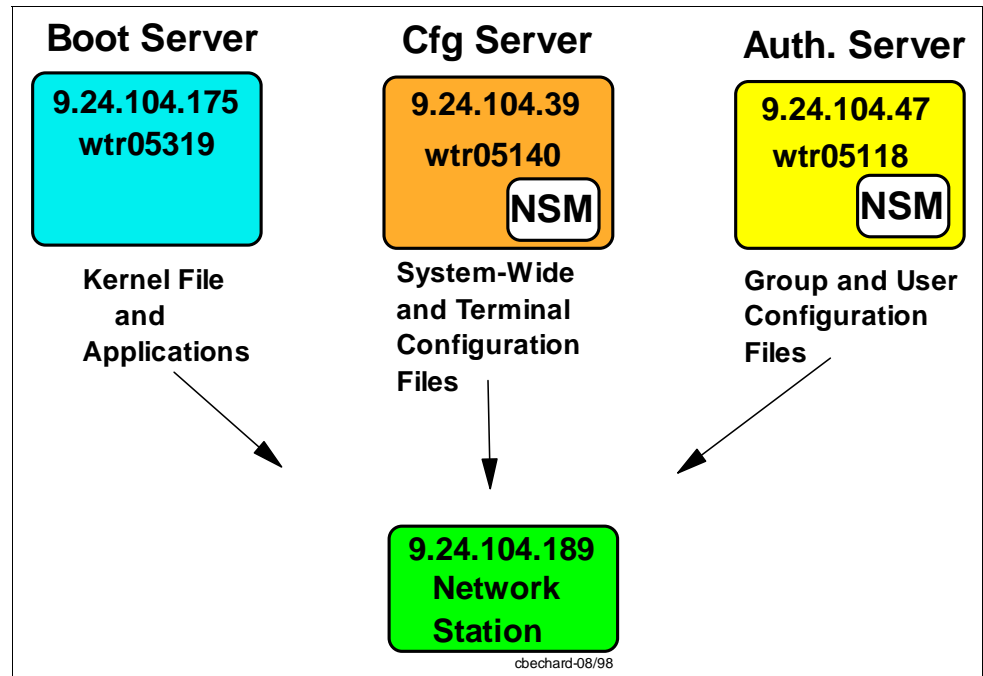


Figure 97. Separation of Server Example

## 4.5.1 Configuration

So how do we configure the IBM Network Station to direct it to use these separate servers?

As always, there are two methods that can be used: DHCP or NVRAM. We examine both here by showing the entries that are made if you use NVRAM, and the corresponding DHCP options that you need to configure on the DHCP server if you boot using DHCP.

Whether you use NVRAM or DHCP, the configuration data needed by the IBM Network Station to use these servers consists of the following elements:

- The IP address of the boot server, the protocol to use (NFS or TFTP), and the directory where the files (in this case the kernel) are located
- The IP address of the configuration server, the protocol to use, and the directory where the configuration files are located
- The IP address of the authentication server

### 4.5.1.1 Configuring Using NVRAM

If we use the NVRAM Setup Utility panels to configure these elements, we make entries into the following panels:

- The network parameters
- The boot parameters
- The configuration parameters

This we illustrate in the next figure.



Note that we simplified some of the information on these panels by removing some entries in order to save space and show only the relevant information but you should recognize immediately the layout of the Setup Utility panels.

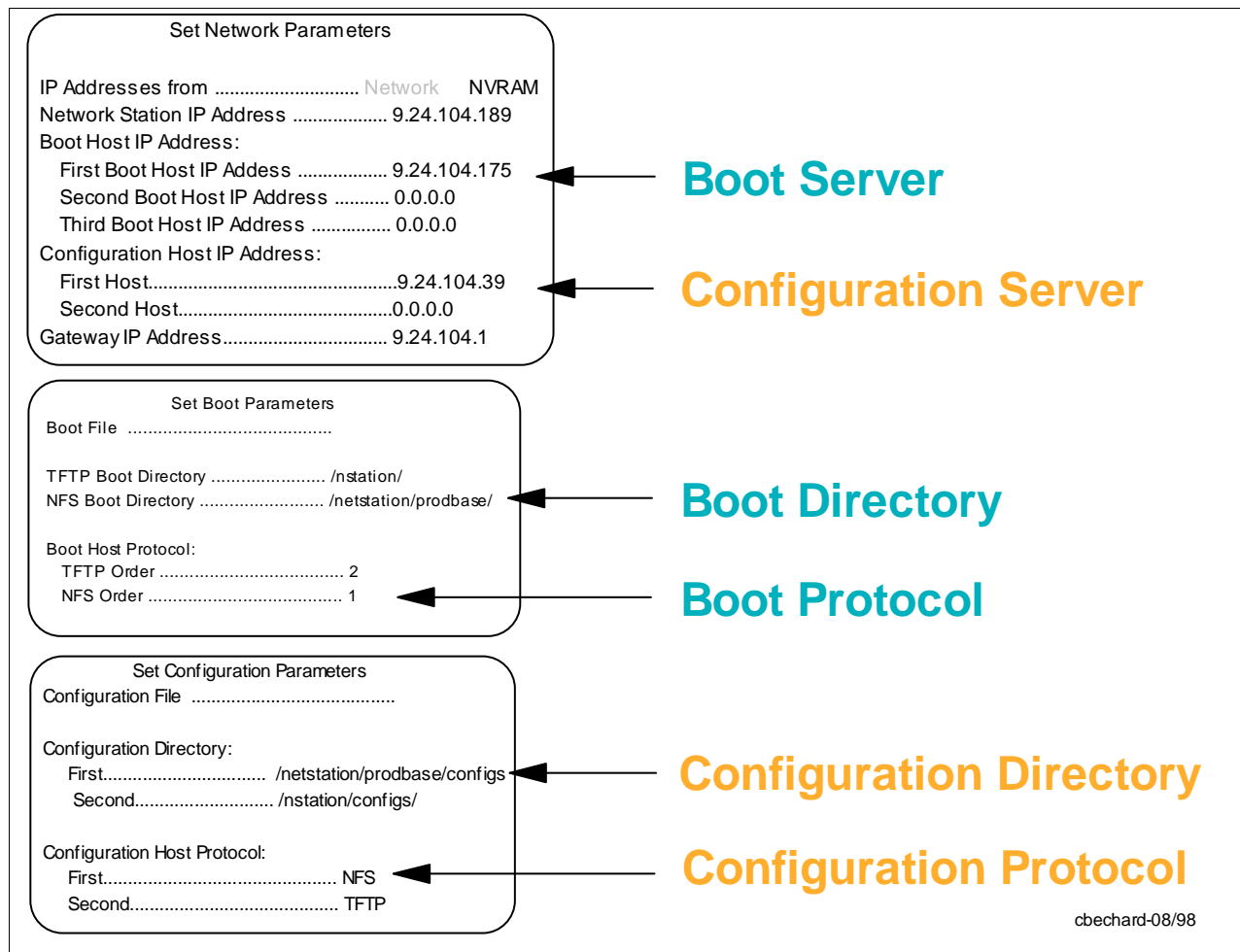


Figure 98. The Setup Utility Panels

Notice the following in the above figure:

#### 1. Boot server

In the case of the boot server, it is possible to specify up to three servers, so that if the first one is not available, the second one is tried next, and then the third one.

The other parameters for the boot server are the boot protocol that should be tried first and the boot directory to use for that protocol. Both of these parameters are specified in the Boot Parameters panel.

#### 2. Configuration server

In the case of the configuration server, up to two hosts can be specified.

Note that if the entry is left blank (meaning 0.0.0.0), then the configuration server is, by default, the boot server.

The other parameters for the configuration server(s) are the protocol that should be used and directory where the configuration files are located. Both of these parameters are specified in the Configuration Parameters panel.

### 3. Authentication server

Finally, there is the authentication server which is not configured through the Setup Utility or through DHCP.

There are three ways to identify the authentication server:

1. If nothing special is specified, the authentication server is, by default, the same as the boot server.
2. The user can use the Roam function on the login panel to identify a specific authentication server other than the boot server. This function is illustrated in the next figure:

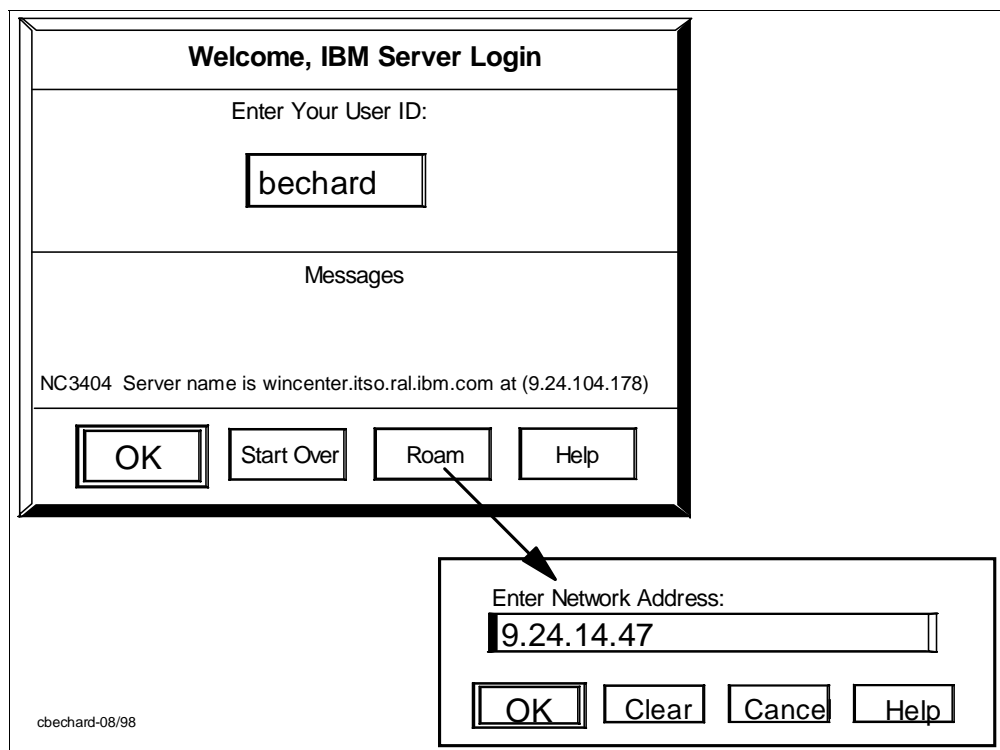


Figure 99. Using the Roam Button on the Login Panel

Entering an address on the Roam panel directs the login client on the IBM Network Station to contact the login server on the designated server instead of the default boot server, in this case, the server located at 9.24.104.47.

3. Or the administrator can pre-configure a specific authentication server to be used, by default, at login time.

To pre-configure a specific authentication server, the administrator can use the special /as option on the setup command at the time of installation (see 2.14, "Authentication Server Special Install" on page 59 for more details) or manually enter the following configuration statement in defaults.dft.

```
set exec-startup-command = {  
  { "mcuis" }  
  { "actlogin -authserve 9.24.104.47" }  
}
```

*Figure 100. Specifying an Authentication Server*

The actlogin statement is normally set to the boot server address. In this case, we have changed this to point to another server (9.24.104.47) that we want to use as the default authentication server when the user does not use the Roam button.

## 4.5.2 DHCP Options

What about using DHCP then?

If one uses DHCP, the same configuration data that we have just entered using the NVRAM Setup Utility in the example above can be used except that in this case, we are not entering the data manually but letting the DHCP functions do it for us.

If the IBM Network Station is booted using DHCP, when the DHCP server sends a positive response to the station, in addition to sending the IP address that the station can use, it also sends many other options (data) dependent on how it is configured.

All of the data that we have seen in the above Setup Utility panels can be sent by the DHCP server to the IBM Network Station, thereby creating the equivalent of manually configuring the IBM Network Station using the setup panels. This is of course much more flexible because a change in any of these configuration parameters can be done centrally as opposed to having to go and manually alter each IBM Network Station in the network.

The next figure illustrates the DHCP options that correspond to the NVRAM data. DHCP options are identified with numbers, so the number appearing to the right of the description (such as 66 for the Base Code/Boot Server) refers to DHCP option number 66.

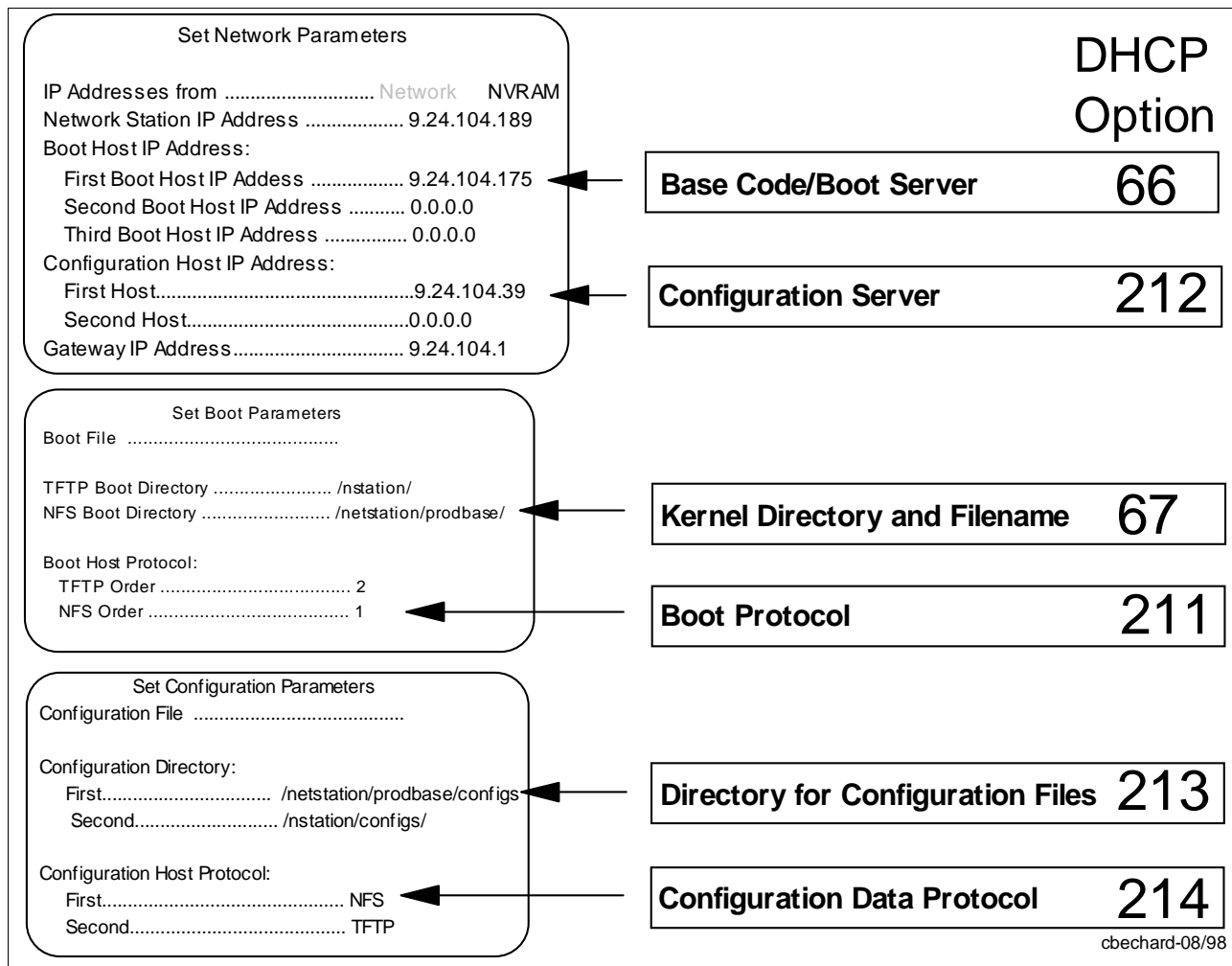


Figure 101. DHCP Options for Separate Servers

What about the authentication server though?

There is no DHCP option for the authentication server. The authentication server is chosen, as with the NVRAM setup, by either using the Roam button on the login panel, or by the administrator configuring a default configuration server other than the default boot server.

#### 4.5.2.1 Equivalent Configuration Parameters

The DHCP options we described in the previous figure are a way of specifying configuration preferences through DHCP.

In the next figure, we not only identify the DHCP option number and name, and point with an arrow to the corresponding NVRAM setting, but we also indicate the name of the configuration parameter that corresponds to these values.

This can provide you with a better understanding of some of the parameters that were used in the migration and retargeting scenarios we described in the previous chapter.

The equivalent configuration parameters are as follows:

- Option 212 (Configuration Server) is the equivalent of setting the parameters file-initial-server1 and file-initial-server2.
- Option 213 (Directory on Configuration Server) is the equivalent of setting the parameter config-unix-directory.
- Option 214 (Configuration Protocol) is the equivalent of setting the parameters file-initial-protocol1 and file-initial-protocol2.

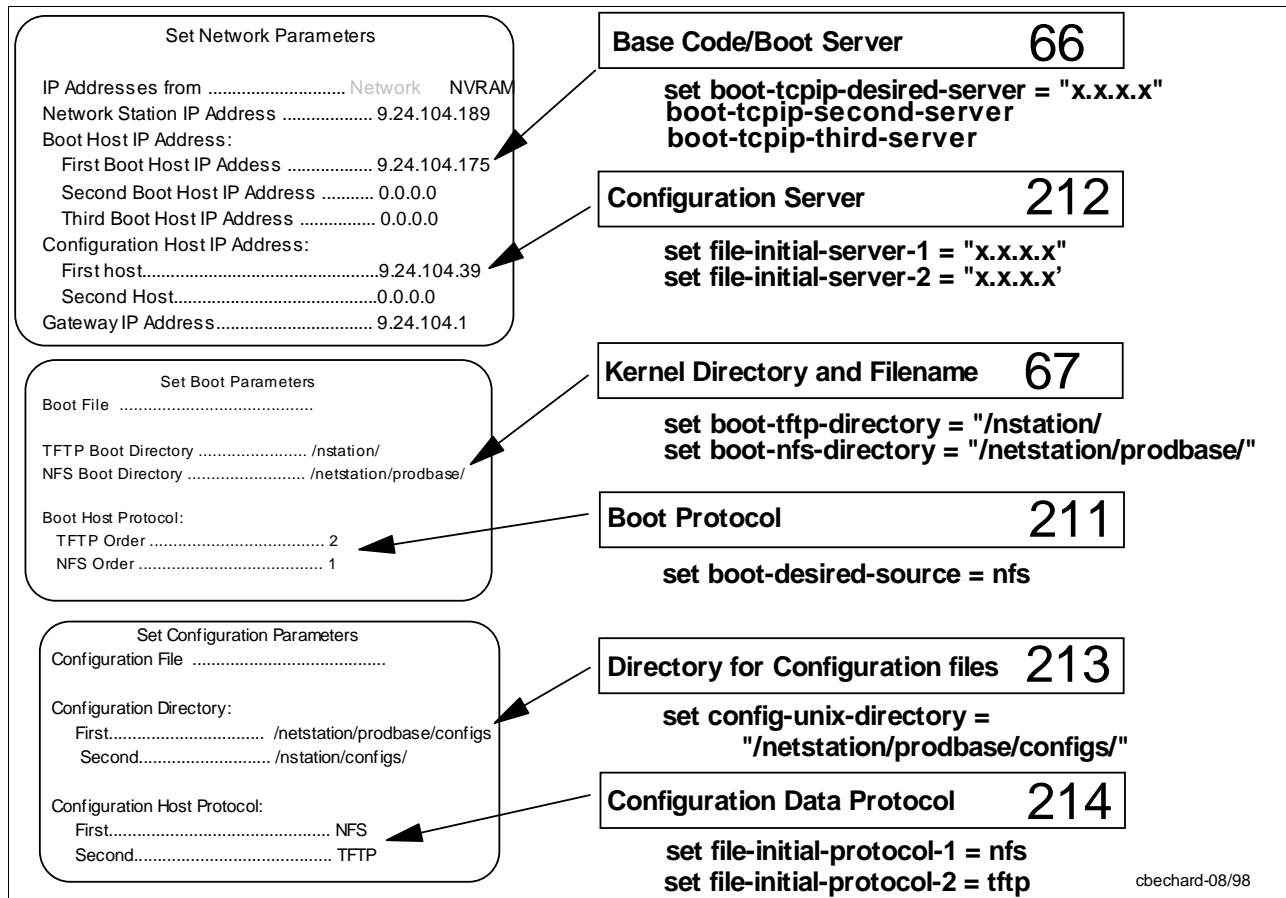


Figure 102. DHCP Options and Equivalent Configuration Parameters

Note however that the IBM Network Station Manager does not use these parameters in its configuration files, such as required.nsm, because the settings in these files would overwrite any values set in NVRAM or set through the DHCP options.

Therefore, we recommend that these parameters also should not be used in back door files such as defaults.dft in order to retain the flexibility of changing them through DHCP options.

## 4.6 Implementing Separation of Servers

One must be aware of the different configuration files involved in the booting process before one can understand the differences in the services provided by these different servers. We therefore encourage the reader to read the chapter on

configuration files (see Chapter 13, "Configuration Files Structure" on page 221) before proceeding with this chapter.

So, how is it exactly that the IBM Network Station is able to access different servers during the boot process?

What we have seen in the previous sections of this chapter is how to set the configuration parameters in order to point the IBM Network Station to different servers during the boot process. We now take a more in-depth look at what changes are caused by these configuration parameters and the mechanism by which the station reads the different files that it needs to be operational.

This has all to do with how the station accesses directories on the server(s), so let us take a look at that mechanism first.

#### 4.6.1 Access to Server Directories

If there are many servers available, how does the IBM Network Station know which files to access, where these files are located and what protocol to use with a particular server?

The answer is a table in the IBM Network Station configuration data called the *file service table*, which provides this information.

The Network Station creates a list of mount points that it uses to access server directories. Each mount point has a local side and a remote side:

- The *local mount point* is the server's directory path known by applications that run on the IBM Network Station.
- The *remote mount point* contains the address of the server, the directory path that is exported by the server, and the file protocol.

When applications open a file, they use the local mount point. The kernel looks up the remote mount point that corresponds to the local mount point and then accesses the file on the server by using the exported directory path and the protocol from the remote mount point.

Here is a simplified example to illustrate the process of the file service table:

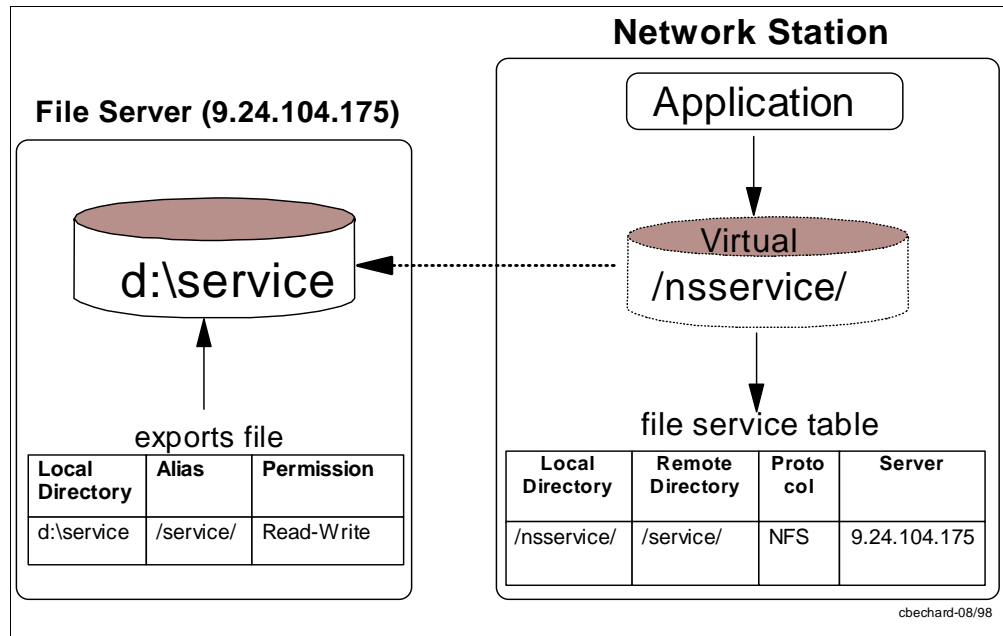


Figure 103. Accessing Directories on Servers

In the figure above, an application on the IBM Network Station needs to write a file in a directory named d:\service on a file server located at 9.24.104.175 using the nfs protocol. The following steps take place:

1. The local application uses an alias name to reference the directory where it needs to write a file. In this example, the application knows that it should reference this directory by the name /nsservice/ because that's the way it was designed and the name /nsservice/ represents a virtual directory on a local drive, which does not exist of course, since the IBM Network Station does not have any local disk storage.
2. The operating system on the IBM Network Station looks up the file service table using the name /nsservice/ and finds that it points to a server at 9.24.104.175, and that it must use the nfs protocol, and that it must access an alias called /service/.
3. The IBM Network Station issues an nfs mount request to the 9.24.104.175 server for the /service/ directory.
4. On receipt of this nfs mount request, the file server looks up its alias table (the exports file in the case of nfs where all exported directories are listed) looking for an alias called /service/ to determine whether this directory is exported and what the permissions are for that directory.

The entry /service/ points to a real directory called service located on d:\ and it has read-write permission, which allows the IBM Network Station to write a file on that directory.

#### 4.6.2 A Sample File Service Table

Now that we know how a file service table works, let take a look at a real table.

Using the same example we used before (see Figure 97 on page 112), here is a look at the contents of the File Service Table after a station has booted and after the user has done a login.

Table 5. File Service Table Contents after Boot and Login

Local Directory	Server	Protocol	Remote Directory
/netstation/prodbase/	wtr05140	nfs	/netstation/prodbase/
/netstation/prodbase/configs	wtr05319	nfs	/netstation/prodbase/configs/
/netstation/prodbase/configs/	wtr05140	nfs	/netstation/prodbase/configs/
/nstation/configs/	wtr05140	tftp	/nstation/configs/
<b>After a login from user bechard, the following entries are added.</b>			
/netstation/prodbase/SysDef	wtr05118	nfs	/netstation/prodbase/SysDef
/netstation/userbase/	wtr05118	nfs	/netstation/userbase/
/netstation/homebase/users/bechard	wtr05118	nfs	/netstation/userbase/home/bechard/

In the above table, notice the following:

- A reminder that wtr05140 is our boot server at 9.24.104.39, wtr05319 our configuration server at 9.24.104.175 and wtr05118 our authentication server at 9.24.104.47.

- The first line in the table represents the boot directory on the boot server.

- The second line in the table corresponds to the first configuration server, which we have configured as the wtr05319 server.

This entry corresponds to the first configuration host as configured in the Network Parameters Setup panel (see Figure 98 on page 113).

- The third entry in the table represents the second configuration server, which we have not configured but left as 0.0.0.0 (see Figure 98 on page 113).

Because we have not configured the second configuration server, it defaults to the base code server. Therefore, the third line in the table is identical to the second one except for the server address.

- The fourth entry in the table is caused by the fact that even though we have not configured a second configuration server address, we did configure, in the Configuration Parameters panel, a second configuration directory as \nstation\configs\ and a protocol of TFTP.

The logic is that the boot server is first tried with the normal configuration directory as specified for the first configuration host and then with the second configuration directory, if configured.

Had we not configured a second configuration directory, this entry would not be added to the table.

- After the user has done a login, the last three entries are added and you should notice that they all point to the authentication server.

**Note:** If a remote directory is specified in a configuration parameter that does not correspond to a known local directory, an entry is added to the table with the local directory name the same as the remote directory. This is a backwards



compatibility feature for applications that might have been using local directory names other than the standardized ones.

The next figure illustrates how the File Service Table looks when you display it on the IBM Network Station Setup display.

The file service table may be viewed on the Network Station by pressing Alt+Shift+Home to bring up the console, then selecting **Setup=>Change Setup Parameters =>File Service**.

Since we need to scroll to see all the entries, we have taken some liberty here with cut and paste to display the relevant entries all on the same panel. It shows the headings and the four important columns for the first three rows, that is the Local UNIX Mount point, which we refer to as the local directory, the server address, the protocol and the remote directory or server mount point as it is referred to here.

File Service Table			
Local UNIX Mount Point	Server	Protocol	Server Mount Point
/netstation/prodbase/	WTR05140.itso.ral.ibm.com	nfs	/netstation/prodbase/
/netstation/prodbase/configs/	wtr05319	nfs	/netstation/prodbase/configs/
/netstation/prodbase/configs/	WTR05140.itso.ral.ibm.com	nfs	/netstation/prodbase/configs/
<div> <div>New</div> <div>Delete</div> </div>			

Figure 104. Display of the File Service Table on the IBM Network Station

The next table also shows what the NFS exports file on these servers contains:

Table 6. Exports File on the Boot Server

Directory	Alias	Permission
c:\nstation\prodbase\service	/netstation/prodbase/service/	ReadWrite
c:\nstation\userbase	/netstation/userbase/	ReadWrite
c:\nstation	/netstation/	ReadOnly

#### 4.6.2.1 Adding Entries to the File Service Table

If you need to add an additional mount point to the local file system because some application requires that mount point, you can use the file-service-table parameter.

This parameter works differently from other parameters in the sense that the parameter contents are appended to the end of the File Service Table list, below the automatically mounted directories.

If the file-service-table parameter is specified more than once, the contents of the last parameter are added to the list.

For example, you could add the following entry to the defaults.dft file:

```
set file-service-table = { { "/demo/" nil 9.24.14.65 nfs
"/usr/local/sybase/" unknown 3 30 1024 1024 } }
```

where:

- /demo/

This is the name of the local-unix-mount point (UNIX style mount point). The application that needs to write to this file system would identify it locally by the name /demo/.

- nil

The name of the local-vms-mount-point (should always be nil).

- 9.24.14.65

The host name or IP address of the remote server where the files to be accessed are located.

- NFS

The protocol used for access (choice is either TFTP or NFS).

- /usr/local/sybase/

The name of mount point on the file server. This is the name of the alias as specified in the exports file on the server where the file resides.

- unknown

The file-name-type (always unknown for NFS).

- 3 = retransmission-timeout (seconds)
- 30 = transaction-timeout (seconds)
- 1024 = read-size
- 1024 = write-size

The above example mounts a remote UNIX file system to allow the Network Station application to access files in a /usr/local/sybase directory on a remote host located at 9.24.14.65.

---

## Chapter 5. Using the IBM Network Station

The intent of this chapter is to focus on the facilities available to the user from the IBM Network Station's desktop, mainly the menu bar and the IBM Network Station console.

Once the Network Station has completed its boot process, and a user has successfully logged in, the user has two main interaction tools at his or her disposal:

- His or her primary tool is the menu bar, which contains buttons to start applications and which can be customized on a per user basis.
- An additional tool is the console, from which additional facilities are available.

These console functions, however, are not really application functions but rather problem determination functions and services, except maybe for the Terminals applications. Many of the services available from the console are disabled, by default, but can be enabled by the administrator.

---

### 5.1 The Menu Bar

The menu bar, assuming that the administrator has decided to make one available to the user, is the user's main interface, allowing him or her to start applications. The menu bar can be customized by the administrator to contain menu entries that are applicable to all users, or entries that are applicable only to specific users or groups of users.

Note that the menu bar gets built and displayed on the desktop only after the user has done a login; based on the user name entered on the login screen, the proper startup files are selected to build the menu bar based on the user's characteristics.

Some of the following buttons are typically found on the menu bar:

- Log Out

The menu bar contains, as a minimum, a Log Out button. When the Log Out button is used, the Network Station rereads its configuration files to reset the state of the station as it normally is after a boot, and then presents the login screen for the user to enter a user name and password. This function might be used, for example, to log on with a new user name in order to get a different menu bar, containing applications specific to a user.

- Show/Hide

It can also contain a Show/Hide button which allows the menu bar to be hidden away. When it is hidden, moving the cursor to the edge of the display where the menu bar normally appears causes the menu bar to reappear. This is used when applications require the entire screen as a display area, and the user does not want the interference of the menu bar.

- Top/Bottom

There can also be a Top/Bottom button allowing to have the menu bar to appear either at the top of the display, or at the bottom.

- Lock Screen

A click on this requires the user to enter a password in order to lock the screen while he or she is away from his or her station. The user must enter the password twice to ensure there is no mistake. To unlock, the same password must be typed.

Note that the password is not retained after the user unlocks. He or she can elect to use a new password each time he or she uses the Lock function, so he or she must be careful to remember the password used. However, in the event that the user forgets his or her password, he or she can always power off and power on again to reset the station to its initial state.

- 3270 or 5250

When the user clicks on the default 3270 or 5250 button, a small dialog box appears asking for a host address. Type in an IP address or an IP host name such as wtscpok.itso.ibm.com, and after a few seconds, you should see the logo from the host system appear, assuming that this host is configured for 3270 or 5250 access.

Note that this can be customized by the administrator so that the user does not have to enter any data. Many of the characteristics of the session such as graphics and screen size, IP port, etc. are defaults that are configurable through the IBM Network Station Manager by using the 3270 setup task.

See 19.5.2, "Help on Commands" on page 379 for details on the parameters available on the ns3270 command.

- NC Navigator Browser

Causes the NC Navigator browser to start.

- Other menu bar buttons

Many other buttons, in addition to the standard ones, can be added to the menu bar.

See Chapter 7, "Using the IBM Network Station Manager Application" on page 147 for instructions on how to add menu bar items.

---

## 5.2 The IBM Network Station Console

The IBM Network Station console contains many functions, some of which have been, by default, disabled in order to prevent access by normal users. However, the administrator has the capability to enable or disable any of these functions, depending on what type of functions he or she wants to give his or her users.

The console can be toggled on and off through the use of a key sequence. The default key sequence is Alt+Shift+Home; however, this is a configurable parameter. For example, to use the Pause key instead, you would use the statement set pref-console-key-sequence = "Pause" in one of the configuration files.

Many of the pull-down menus on the console, or individual commands on some of the pull-downs, can be disabled through configuration parameters. It is up to the administrator to determine whether there is a need to make any of the console functions available to the user.

Below is an illustration of the console.

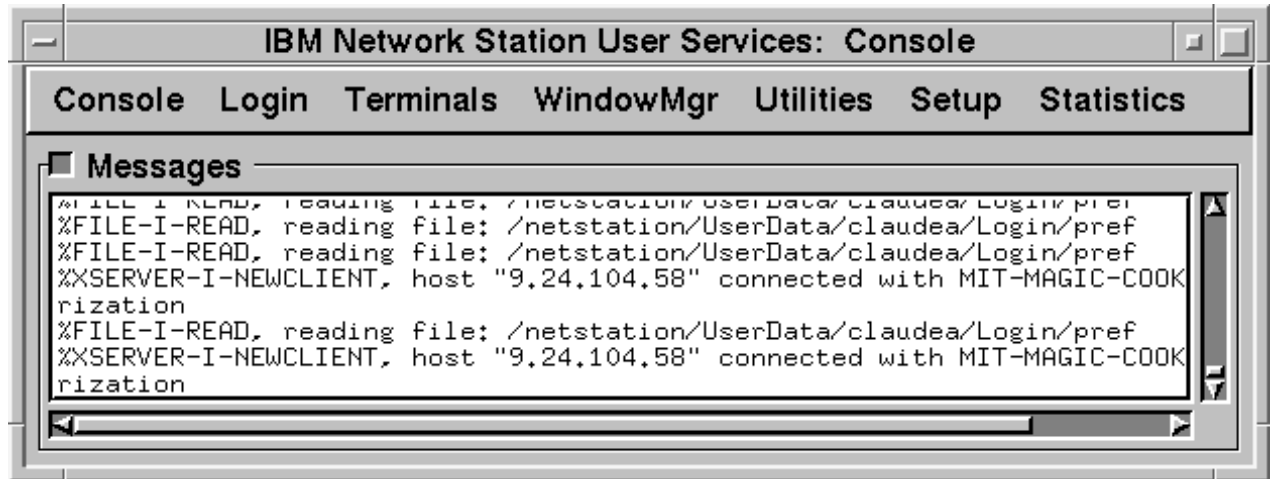


Figure 105. IBM Network Station Console

Here is a brief description of the functions available through the console, starting at the pull-down menu on the far right of the console.

## 5.2.1 Statistics

The Statistics pull-down is used to display information such as the version level of the boot monitor program, memory utilization, and other such statistics. This pull-down is normally open for all users since the information can only be displayed (and not changed). It has the four entries discussed in the following sections.

### 5.2.1.1 Show Version

This is a useful panel that identifies the version level of the software and the boot monitor program running on the Network Station. It also displays the built-in and current token-ring addresses, the TCP/IP address, memory, and a few other useful pieces of information, as illustrated below.

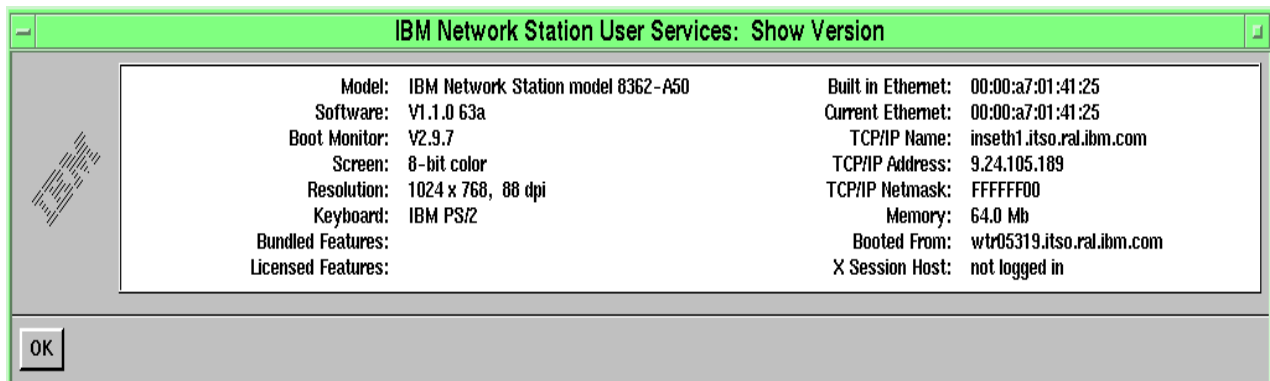


Figure 106. IBM Network Station Console - Show Version

### 5.2.1.2 Show Memory

The Memory panel displays the amount of free memory remaining. As you load applications, this panel gets updated with the new information so that the user

can monitor how much memory is left. Remember that this is a real memory system; there is no paging taking place.

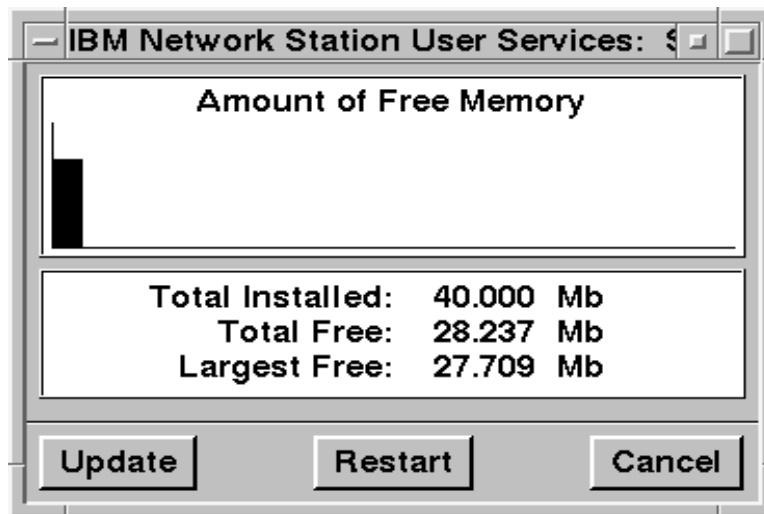


Figure 107. IBM Network Station Console - Memory

#### 5.2.1.3 Show X-Connections

Each application started on the Network Station uses some resources and gets listed in this panel along with the resources used. Click the **Update** button to refresh the information.

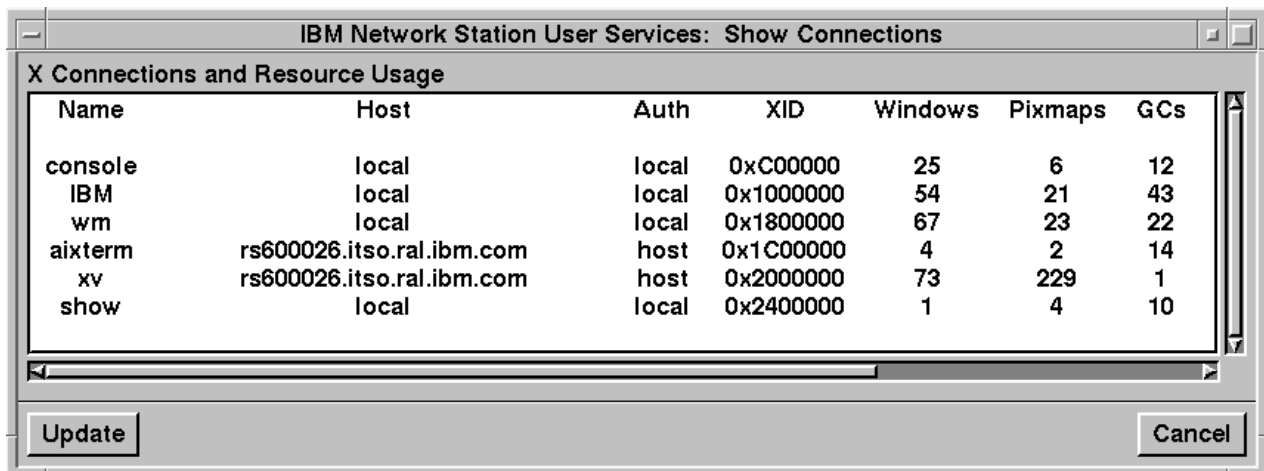


Figure 108. IBM Network Station Console - X Connections

#### 5.2.1.4 Show Statistics

There are 18 categories from which you can get statistics, as listed below. For example, under IP, you can get the number of packets received, forwarded, discarded, delivered, etc.

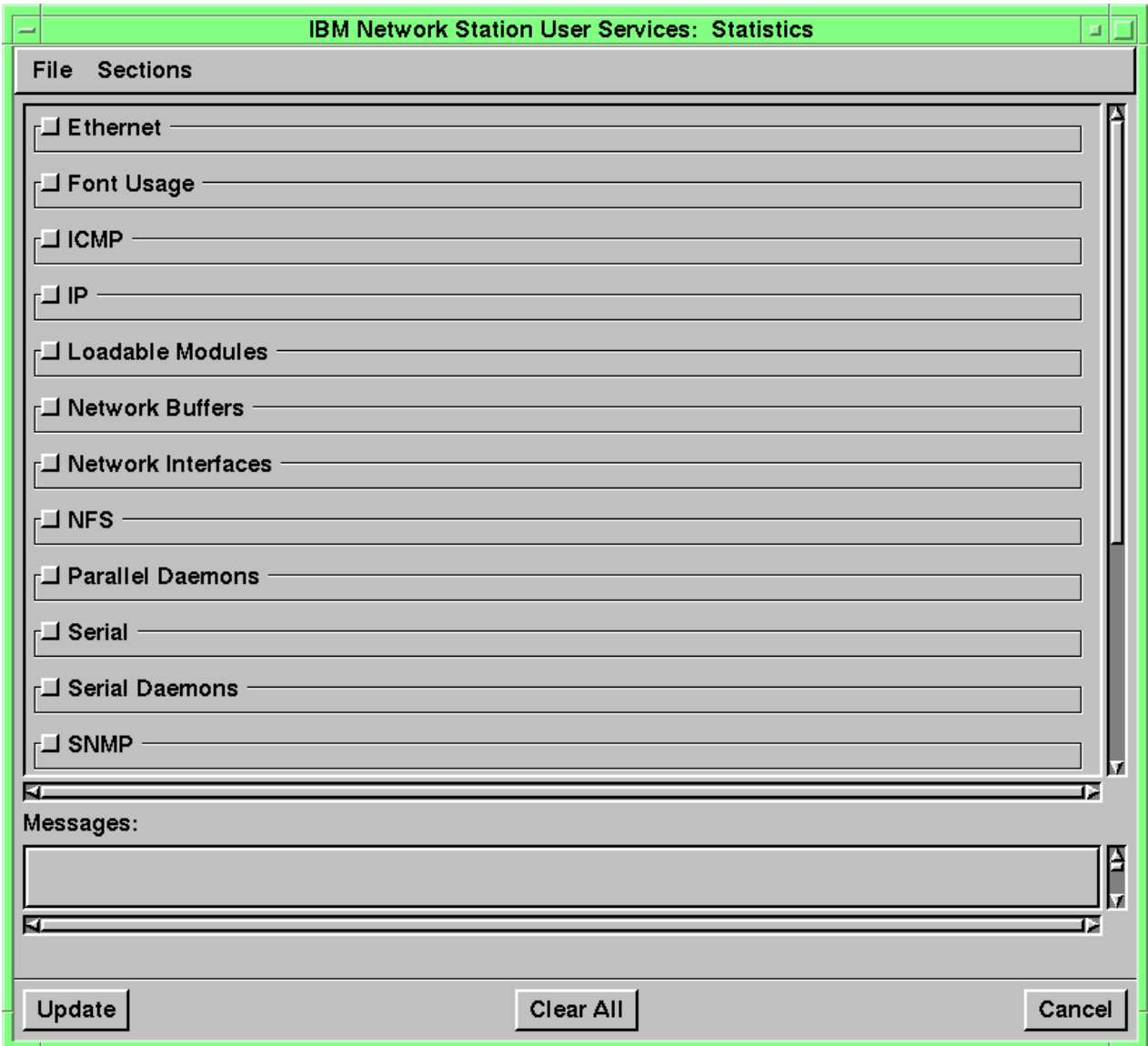


Figure 109. IBM Network Station - Statistics

### 5.2.2 Setup

This pull-down gives access to all the configuration parameters. These parameters can be viewed, or changed, but the changes are not permanent. They will take effect only until the next reboot, because the next boot will cause the replacement of all these values with the values specified in the configuration files which are read at boot time.

For problem determination purposes, this can be used to verify the settings of certain parameters, or to try a different setting without having to reboot (for those parameters whose effect is immediate).

There are three items on this pull-down:

### 5.2.2.1 Quick Setup

This deals mainly with boot parameters. These are essentially most of the same parameters that are available from the Network Station Setup Utility.

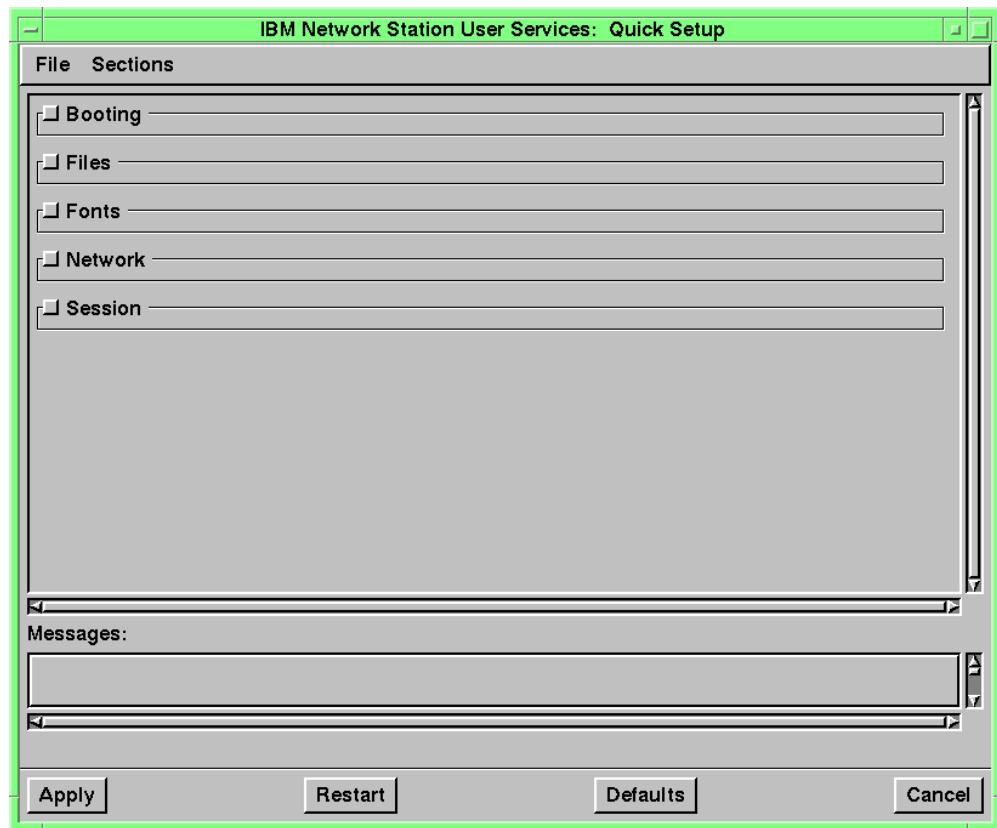


Figure 110. IBM Network Station Console - Quick Setup

### 5.2.2.2 Change Setup Parameters

The Setup parameters deal with all the main configuration parameters, as shown below:



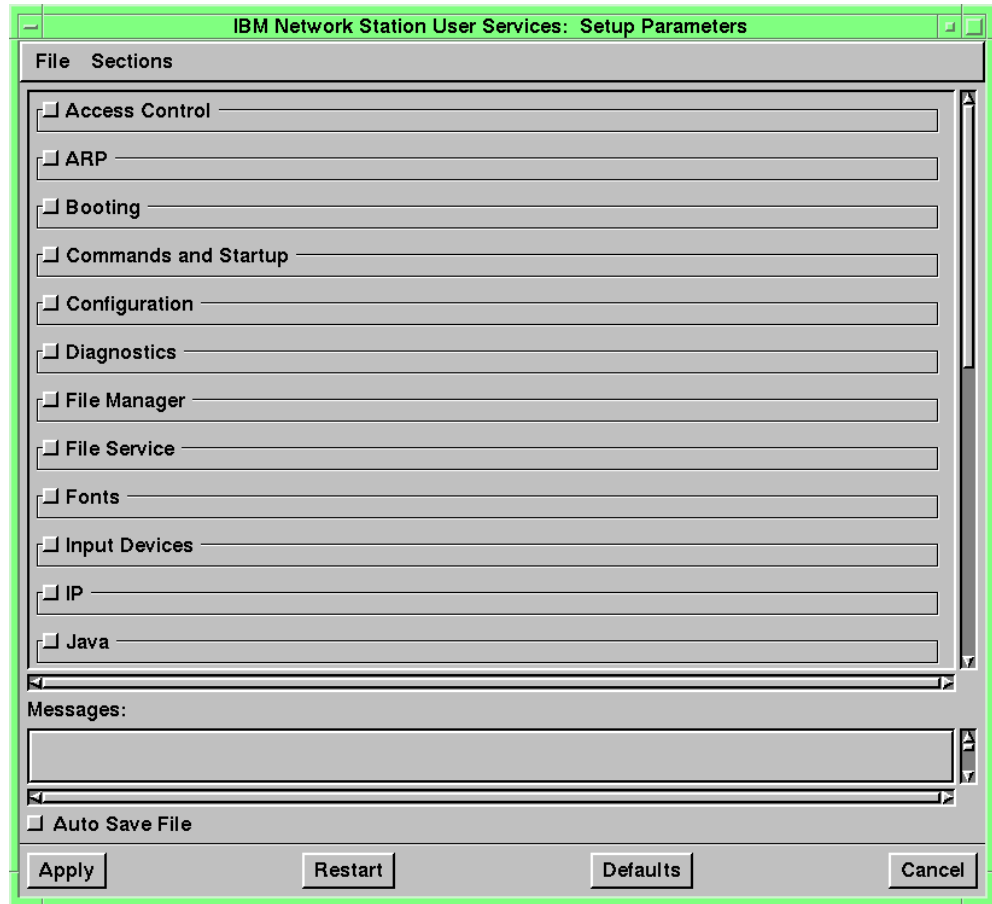


Figure 111. IBM Network Station Console - Setup Parameters

Notice the four buttons at the bottom of the panel:

- **Apply** - When you make changes in any of the categories, these changes are not really effective, or written to NVRAM, until you click on Apply.
- **Restart** - If you have made changes, but have not clicked on Apply yet, you can undo these changes by using the Restart button.
- **Defaults** - A click on this button causes the IBM Network Station to read its configuration files from the server. If you have modified a parameter for example, to test a condition, and you now want to reset the parameter values as they are after a boot, but without rebooting the station, you can use the Defaults button to do the equivalent.
- **Cancel** - Just closes the panel.

Not all categories or groups are shown on the panel above, but you can use the **Sections** pull-down to see all categories.

If you click the **File** pull-down, you are presented with the following choices:

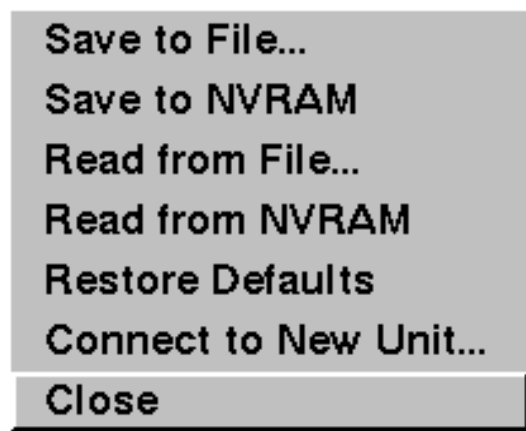


Figure 112. IBM Network Station Console - Setup - File Pull-Down

- **Save to File** - Use caution when using this option. The IBM Network Station has no knowledge of the hierarchical structure of the configuration files on the server that were downloaded and read at boot time. You can use this button to save the configuration parameters to a file on the server, provided you have proper access, but all the parameters will be in one single file. This is not a recommended method.
- **Save to NVRAM** has the same effect as the Apply button.
- **Read from File** - Assuming you had used the Save to File, you could read the parameters from the same file to which you saved them (or from another file).
- **Read from NVRAM** - Reads the settings that are stored in NVRAM. This only affects parameters that are stored in NVRAM.
- **Restore Defaults** - Same effect as the Defaults button at the bottom of the panel. All configuration files are re-read from the server, effectively resetting all the parameters without the need of a reboot.
- **Connect to New Unit** - Allows you to specify the IP address of another IBM Network Station in order to work with the parameters on that other station. If you enter the read-only password, you can only view the parameters on the other station. Using the read-write password allows you to also set parameters.

This can be a very effective problem determination tool allowing an administrator at a central site to view/modify parameters remotely on any station that is having a problem.

#### 5.2.2.3 Change User Preferences

The User Preferences panel deals with parameters that are considered to be more of a user choice as opposed to a system choice; the parameters groups are shown on the panel below:

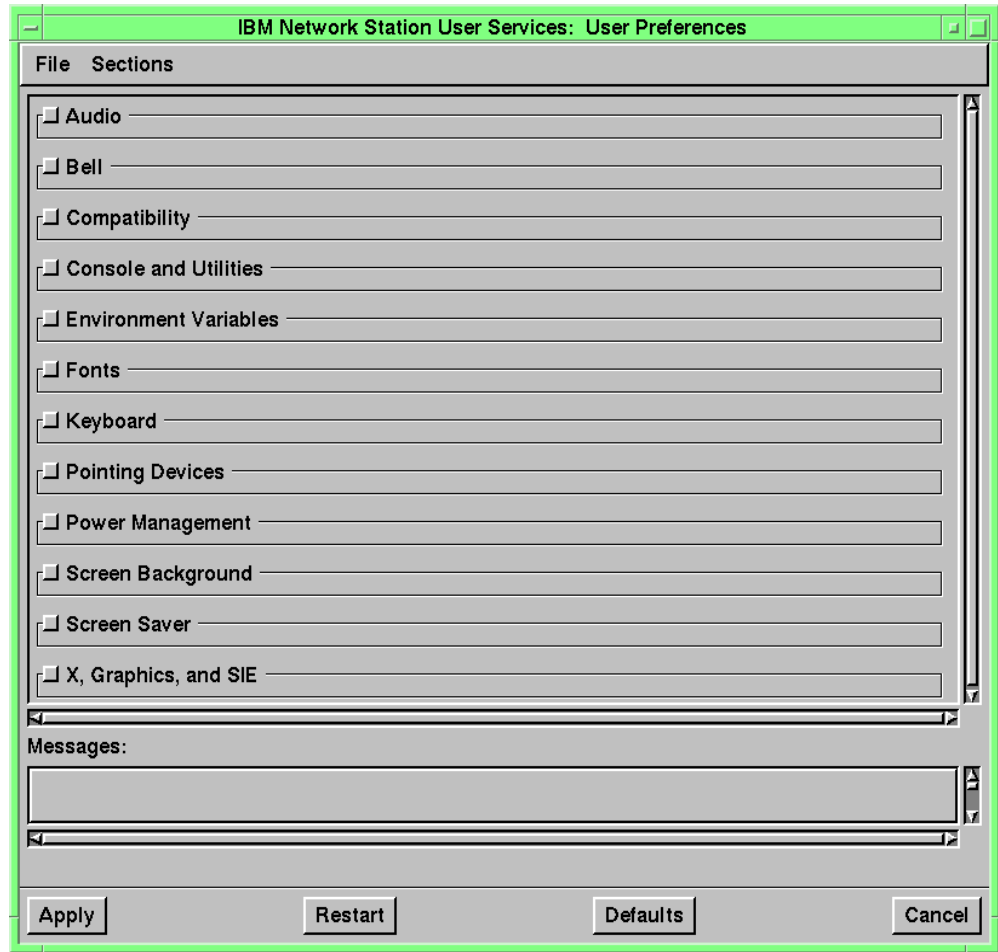


Figure 113. IBM Network Station Console - User Preferences

### 5.2.3 Utilities

There are five items under this pull-down, most of which are self-explanatory:

- Refresh Screen
- Blank Screen
- Lock Screen
- Rescan Font Path
- Test Network - This is a PING application. Just enter the host IP address or host name in the Host field and press Enter. This is to test that you have IP connectivity to another host. The panel is shown below:

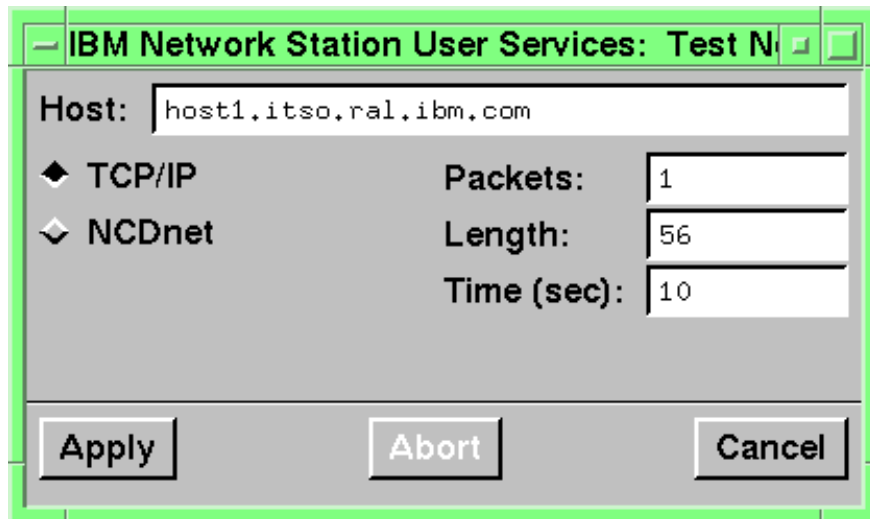


Figure 114. IBM Network Station Console -Test Network

### 5.2.4 Window Manager

This allows the user to start and stop the local window manager. There is a need to stop the local window manager when initiating an X session with an AIX system where the user wishes to use the Common Desktop Environment (CDE). This is because CDE uses its own window manager, which conflicts with the local window manager.

If you try to establish an X-session before shutting down the local window manager, the station reminds you that you need to do this before starting the session.

### 5.2.5 Terminals

The items on this pull-down are used to start a telnet session or to start a few of the services such as the diagnostic service (this is equivalent to the console messages), the configuration daemon or the file services daemon.

Note that if this is not enabled on the console, the browser can be used to start a telnet session by entering a URL of telnet://host name or address. This produces the equivalent of using the Terminals pull-down on the console, selecting Terminal and entering a hostname or address in the Service field.

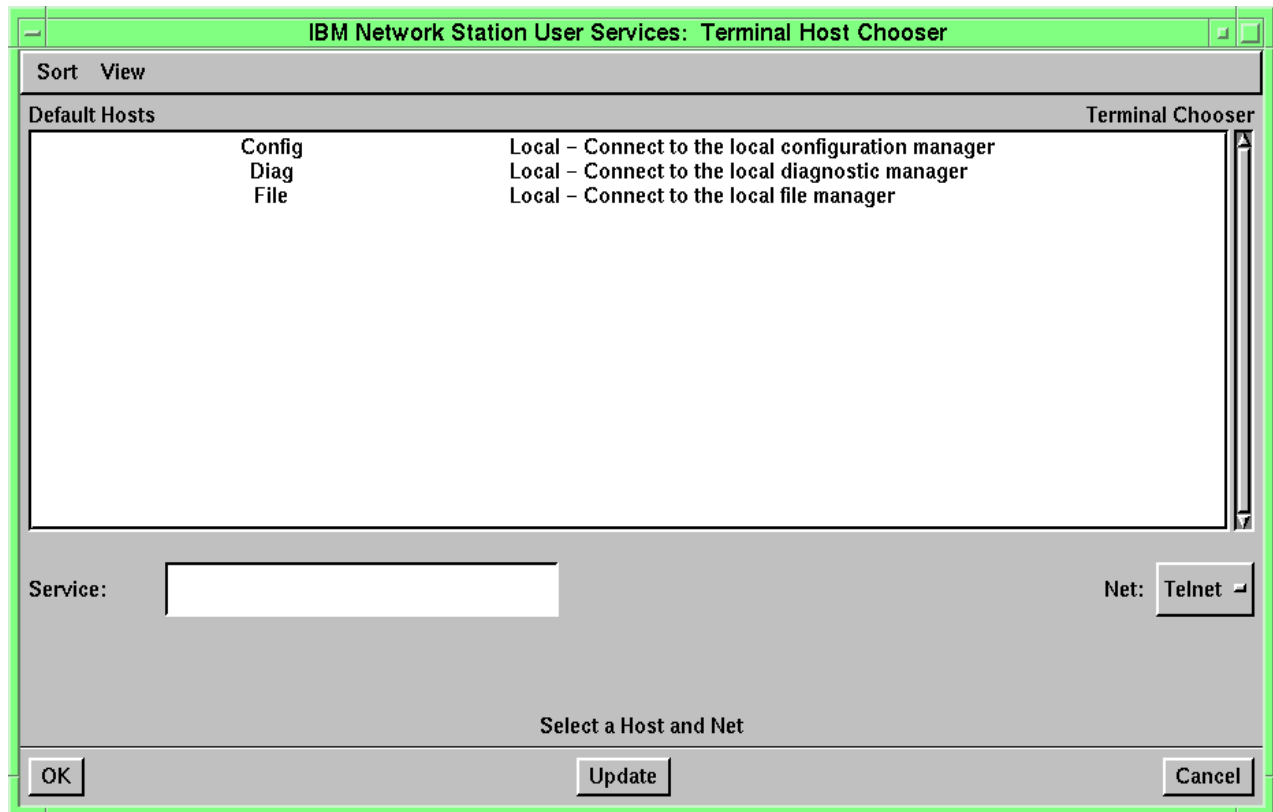


Figure 115. IBM Network Station Console - Terminal/Telnet

In the figure above for example, selecting the DIAG entry actually starts a telnet session using the loopback interface and port 5998, which is the port used to access console messages. Therefore, the result is a listing of the console messages. We find this much more useable than the Console window when looking at messages because the scrolling capabilities are better.

On the other hand, entering an IP host address in the field labeled Service causes the establishment of a telnet session with the designated host.

To have a list of hosts appear in the Terminal Host Chooser list, use the term-default-hosts parameter, and the parameter term-restrict-host-choices would be used if you want to restrict the choice of host to only those appearing in the list.

```
set term-default-hosts = {
  { telnet rs600026.itso.ral.ibm.com "RS600026" }
  { telnet 9.12.14.1 "wtscpok" }
}
```

Figure 116. The set term-default-host Parameter

## 5.2.6 Login

Under this pull-down is the Login Chooser, which when started, issues a broadcast asking all hosts that run the X Display Manager Program to respond. As hosts reply to the broadcast request, they get listed in the window, where the

user can select a specific host. Through the use of configuration parameters, the administrator has some control, however, on which/how hosts get listed in this window.

For example, setting the parameter `login-xdm-broadcasts = use-first` causes the IBM Network Station to use the first host that responds to the broadcast request. Setting the same parameter to a value of `prompt` instead of `use-first` causes all responding hosts to be displayed in the Login Chooser window.

The `login-xdm-broadcast-wait-time` parameter can also be set to specify the amount of time to wait for hosts to respond before displaying the list. Responses received after this wait time has expired are appended to the end of the list at the time that the responses are received. The default wait time is three seconds.

When the user selects one of the hosts listed, or enters a specific host name or IP address in the field labeled Host and chooses OK, a request is sent to the address specified asking for the establishment of an X Display Management Control Protocol (XDMCP) session.

Typically, these hosts would be AIX hosts, which would supply a Common Desktop Environment (CDE) desktop, or they can be WinCenter or MetaFrame servers.

Notice that in the list of available hosts the number of current users is also listed, thereby giving the user the opportunity to choose the least busy host.

Since hosts that are not local to the LAN segment cannot respond to a broadcast request, the administrator can also configure specific hosts to appear in this list. This is done through the `login-default-hosts` parameter. For example:

```
login-default-hosts = {  
  { tcp  wincenter.itso.ral.ibm.com  "Wincenter" }  
  { tcp  RS600026 "RSServer" }  
}
```

*Figure 117. The set login-default-host Parameter*

If you want only these hosts to appear in the list and none of those that may be responding to the broadcast, then set the parameter `login-xdm-broadcasts` to the value `ignore` instead of `prompt`.

Finally, note that the user can always enter a specific host name on the Login Chooser Host field in order to direct a login request to a specific host that does not appear in the table. If you want to prevent the user from doing this, in other words to restrict his or her choice only to those listed in the window, then you can set the `login-restrict-host-choices` parameter to the value `true`.

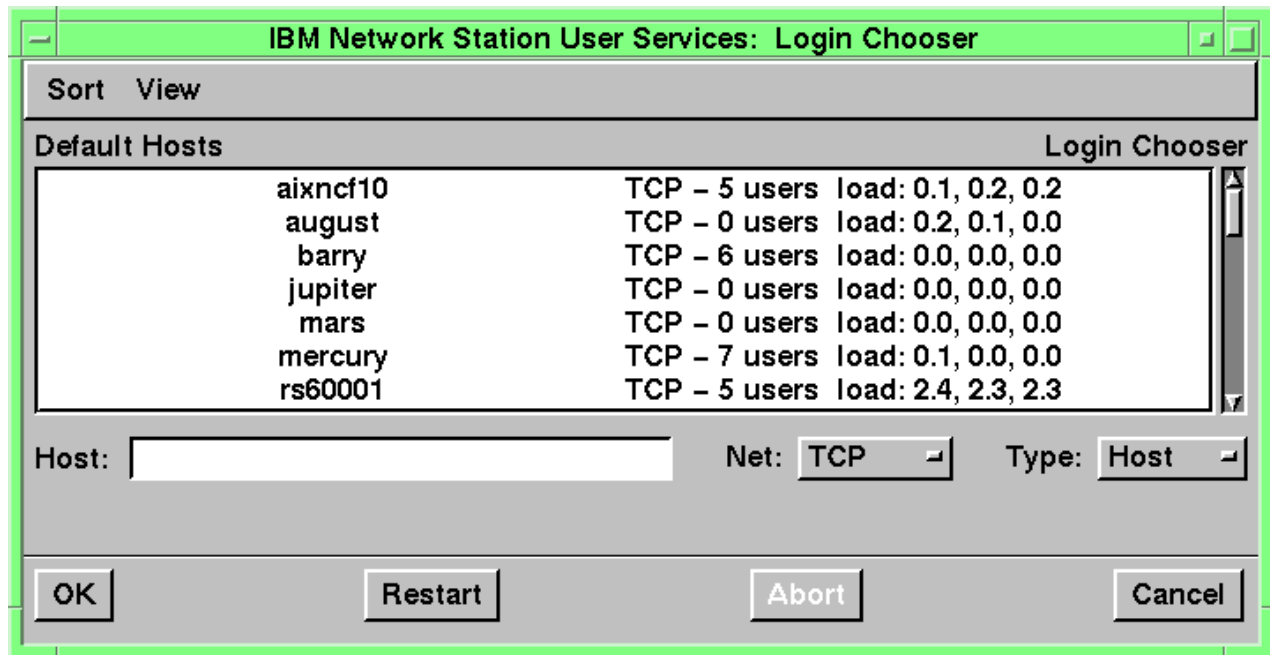


Figure 118. IBM Network Station Console - Login Host Chooser

### 5.2.7 Console

Under this pull-down, the entries are all self-explanatory:

- Clear Messages - Clears the messages in the log.
- Rescan messages - Rescans the messages currently displayed.
- Reboot - Initiates the boot process.
- Close - Closes the console.

### 5.2.8 Messages

A click on the Messages check box opens up the display of console messages. This is your primary problem determination tool and the first place to look for error messages. If the messages you are looking for are much earlier in the log and are not displayed in the window, there are other ways of accessing the message log to look at all the messages since the last reboot. See 19.1, "The IBM Network Station Message Log" on page 363 for additional details.

## 5.3 The Command Pop-Up Menu

There is also a Command Pop-Up Menu facility (this is also referred to as the Local Clients list), which can be used as an alternative to the menu bar. Commands can be configured to appear on this menu, which is displayed by pressing the L-Shift + L-Alt + right mouse button.

The commands that appear in this list are pre-configured using the statement set exec-command-menu as shown in Figure 119 on page 136.

```
set exec-command-menu = {  
    { "Console" "console" }  
    { "Lock Screen" "lock" }  
    { "Show Version" "show version" }  
    { "My3270" "ns3270 9.12.14.1. -graphics" }  
}
```

*Figure 119. The set exec-command-menu Parameter*

In the above example, the entries on the left represent the entry names as they appear in the list when displayed, whereas the entries on the right are the actual commands that get executed when the user clicks on the entry in the list.

The entries made here are similar to those that can be made on a menu bar button, but they are different facilities. Some of the main differences are as follows:

- The command pop-up is not configurable through the IBM Network Station Manager as the menu bar is; it must be configured manually.
- The command pop-up is part of the local window manager, and as such, may be available (through the L-Shift + L-Alt + right mouse button key sequence) before the user does a login. That is, the console and the window manager can be started using the WindowMgr pull-down on the console. The menu bar, on the other hand, does not appear until the user has done a login.
- Because the Command pop-up is considered part of the local window manager, it is not available if the local window manager is stopped.
- The command pop-up applies to all users; it cannot be customized on a per user basis as the menu bar can.



---

## Chapter 6. Configuring the IBM Network Station

After the boot server is installed, the next step is to configure an IBM Network Station so that it can boot from the server.

This chapter identifies the steps that are required in order to use the Setup Utility of the IBM Network Station to enter configuration values into its NVRAM or to set it up so that it gets its configuration data from a DHCP server on the network.

---

### 6.1 Physical Installation

For the physical installation of the Network Station, please refer to the installation instructions supplied with the IBM Network Station.

If these are not available to you, you can get a copy of these instructions from the Web at <http://www.ibm.com/nc/pubs>.

Another source is to refer to the *AS/400 - IBM Network Station - Getting Started, SG24-2153* redbook in which the basic installation instructions are referenced.

---

### 6.2 Setup/Configuration Methods

There are two methods that the IBM Network Station can use to boot from a server:

1. It can use configuration settings stored in its NVRAM (non-volatile RAM).

These settings are entered manually using the Setup Utility panels of the IBM Network Station, as illustrated in the sections that follow.

2. It can use configuration settings that it obtains from a DHCP server on the network.

This is called booting from the network, and requires no configuration settings at the IBM Network Station other than to select this method of boot.

This is the recommended method of booting.

On the other hand, this method requires that an administrator configure a DHCP server somewhere on the network to provide configuration information to the IBM Network Stations on that network.

A DHCP server is sometimes thought of as supplying only IP addresses, but it can also supply other configuration settings, such as boot server address, boot server protocol, etc. See Chapter 10, "Dynamic Host Configuration Protocol (DHCP)" on page 175 for more information on DHCP.

---

### 6.3 Configuration of the IBM Network Station

Once the network station is installed and connected to the network, power on the network station and wait until the Power-On Self Test (POST) completes.

When a message on the screen indicates that the station is accessing the network, press the ESC key in order to enter the Setup Utility.

At this time, the main Setup panel should appear, as shown below:

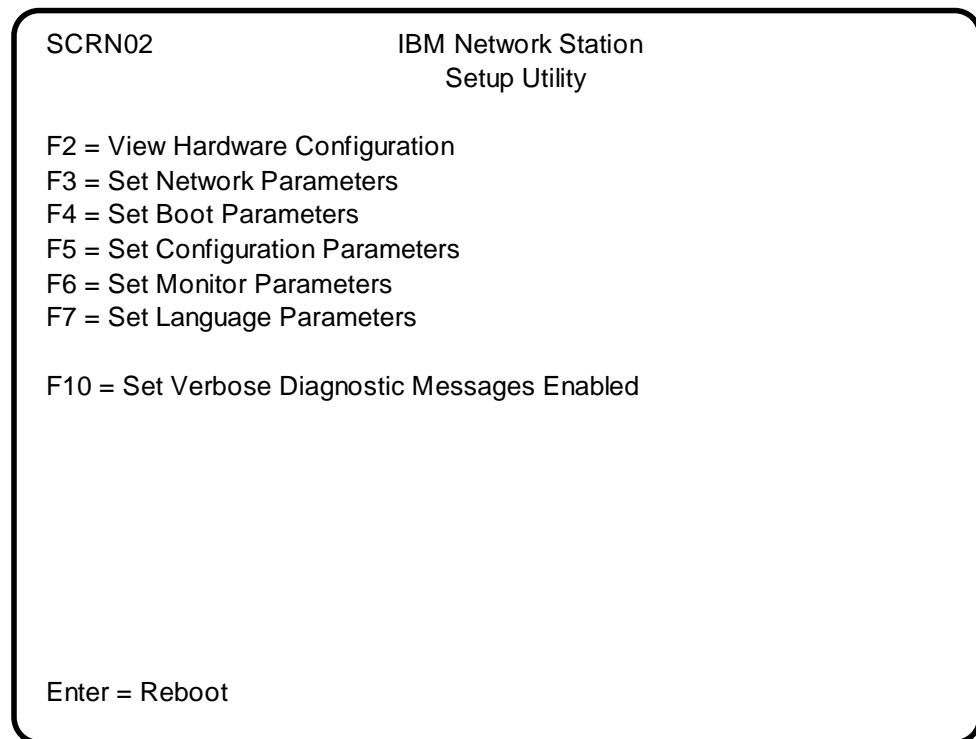


Figure 120. Main Network Station Setup Utility Panel

**Note:** The panel displayed in the above figure is the main setup panel for an IBM Network Station on which the boot monitor has been upgraded to the Release 3 level. It has changed slightly from the previous release. Mainly, the view options (View Boot Parameters and View Network Parameters) do not appear unless a password is set and the user is not allowed to update the configuration settings. There is also an additional Set option (F5) for configuration parameters. This new option relates to the separation of server feature (see Chapter 4, “Separation of Servers” on page 101).

If you need to reset the password because you inherited an IBM Network Station from someone who had set this password, and you were not supplied with the password, your only option may be to physically reset the IBM Network Station. Please refer to 19.12, “Resetting the IBM Network Station Password” on page 390 for instructions on how to reset the password.

See also 19.4.7, “Unit Global Password” on page 375 for instructions on how to set the administrator’s password.

A good practice, at the beginning, is to use the PF10 key to enable the verbose diagnostic message mode so that messages will be displayed on the screen during the boot phase. This might be useful after an initial installation to identify potential problems.

You might also need to set a language by using the F7 key and following the instructions. Language can be set for the keyboard language and the startup language, which governs messages issued to the console during startup.

Similarly, press F6 to set the monitor resolution and follow the instructions supplied, which are self-explanatory.

### 6.3.1 Setting Up for a Boot Using NVRAM

The simplest initial way to verify that your boot server is configured properly and that an IBM Network Station can boot properly from the server is to boot using settings in NVRAM.

Even though using NVRAM settings is not the recommended operational method, it is a simpler way than using DHCP when using only one station to test your server setup, because you do not have to configure a DHCP server.

However, once you have verified that your boot server is indeed operational, we recommend that you configure a DHCP server in order to boot all your IBM Network Stations using DHCP because it provides more flexibility in managing your network and does not require any manual intervention at the actual physical location of the IBM Network Station in order to change configuration parameters.

#### 6.3.1.1 Set Network Parameters

Press F3 to set the network parameters. This action displays the panel shown below:

SCRN05 IBM Network Station  
Set Network Parameters

IP Addresses from ..... Network **NVRAM**

Network Station IP Address ..... 9.24.104.189

Boot Host IP Address:

First Boot Host IP Address ..... 9.24.104.240

Second Boot Host IP Address ..... 0.0.0.0

Third Boot Host IP Address ..... 0.0.0.0

Configuration Host IP Address:

First Host.....0.0.0.0

Second Host.....0.0.0.0

Gateway IP Address..... 9.24.104.1

Subnet Mask ..... 255.255.255.0

Broadcast IP Address ..... 255.255.255.255

Use cursor keys to select option

Enter = Save F12=Cancel F11=Restore Parameter

Figure 121. Set Network Parameters - NVRAM - IBM Network Station Setup Utility

This is the panel where you decide between the NVRAM or NETWORK boot method. Select NVRAM in the IP Addresses From field. This opens up the following parameters, which are not displayed when Network is selected:

- Network Station IP Address

Specify here the IP address that is assigned to you by the network administrator for this unit.

- **First Boot Host IP Address**

This is the IP address of the boot server you just installed. That address is also supplied by your network administrator.

- **Second Boot Host IP Address and Third Boot Host IP Address**

If you have multiple boot servers, you can specify a second and a third server to be tried if the first server is unavailable.

- **Configuration host IP Address - First Host**

Specify here the IP address of the configuration server, if it is different from the boot server. This is new with Release 3 and it allows you to separate the boot server from the configuration sever. See Chapter 4., "Separation of Servers" on page 101 for additional details on separation of servers.

- **Configuration Host IP Address - Second Host**

A second configuration server to be tried if the first server is unavailable.

- **Gateway IP Address**

Supplied by your network administrator, this is the default router or gateway for the subnet on which your network station is installed.

- **Subnet Mask**

Also supplied by the network administrator. This is the subnet mask for the subnet on which the network station is installed.

- **Broadcast IP Address**

Also supplied by the network administrator.

If you are using an Ethernet adapter, you may also need to choose between the Version 2 or IEEE802.3 standard.

— **Use Version 2 if Using WinCenter** —

Please note that if your adapter type is Ethernet and you intend to use your IBM Network Station to go to a WinCenter server, you should ensure that you choose Version instead of 802.3.

If you use 802.3, you will be able to connect to the WinCenter server, and have the WinCenter display appear on the network station, but you will then be unable to use the mouse in any way.

Press Enter to save these parameters.

#### **6.3.1.2 Set Boot Parameters**

Back on the main SCRN02 Setup Utility panel, press F4 to set the boot parameters. This displays the panel shown below:

```

SCRN06                                IBM Network Station
                                      Set Boot Parameters

Boot File .....

TFTP Boot Directory ..... /nstation/

NFS Boot Directory ..... /netstation/prodbase/

Boot Host Protocol:
  TFTP Order ..... Disabled
  NFS Order ..... 1
  LOCAL Order ..... Disabled

                                      Appended to Boot Directory, 64 character limit

Enter = Save  F12=Cancel  F11=Restore Parameter

```

Figure 122. Set Boot Parameters

This is where you specify the files and the path to the files residing on the server that are required to boot the IBM Network Station.

The Boot File parameter can be left blank; it defaults to the value kernel.

In the NFS boot directory, enter the value `/netstation/prodbase/`. This is the path to the kernel file that resides in the `..\nstation\prodbase` directory on the server.

Leave the TFTP boot directory empty, or, if TFTP is to be used, set it to `/nstation/`.

**Note:** This is different from versions prior to Release 3 where TFTP was the preferred method used to load the kernel from a Windows NT server. NFS is now the preferred method. The kernel now resides in `/netstation/prodbase/` instead of `/nstation/`.

Finally, ensure that NFS Order is specified as 1, and the other entries as Disabled. In fact, they could have a value other than disabled, such as 2 for the TFTP order for example, which means that if the NFS method is unsuccessful, the second one to be tried is TFTP.

Press Enter to save these entries. This takes you back to the main Setup panel.

**Note:** If this IBM Network Station is involved in migrating from a previous version, please consult Chapter 3, "Migration from Release 2" on page 71 to determine the proper settings for these configuration parameters when you are retargeting an IBM Network Station client from a Release 2 server to a Release 3 server. Those we identify here apply to when you are fully operational under a Release 3 server, after a new installation or a completed migration.

### 6.3.1.3 Set Configuration Parameters (F5)

Back on the main SCRNO2 Setup Utility panel, press F5 to set the configuration parameters. This displays the panel shown below:

The screenshot shows a window titled 'SCRN25' and 'IBM Network Station Set Configuration Parameters'. It contains several fields for configuration: 'Configuration File' (blank), 'Configuration Directory' with 'First' and 'Second' sub-fields, and 'Configuration Host Protocol' with 'First' and 'Second' sub-fields. The 'First' directory is set to '/netstation/prodbase/configs' and the 'Second' to '/nstation/configs/'. The 'First' protocol is 'NFS' and the 'Second' is 'TFTP'. At the bottom, it says 'Appended to Configuration Directory, 64 character limit' and 'Enter = Save F12=Cancel F11=Restore Parameter'.

```
SCRN25                                IBM Network Station
                                      Set Configuration Parameters

Configuration File .....

Configuration Directory:
  First..... /netstation/prodbase/configs

  Second..... /nstation/configs/

Configuration Host Protocol:
  First..... NFS
  Second..... TFTP

                                      Appended to Configuration Directory, 64 character limit

Enter = Save  F12=Cancel  F11=Restore Parameter
```

Figure 123. Set Configuration Parameters Panel

The Configuration File field can be left blank, in which case the default value is standard.nsm.

Set the First configuration directory to /netstation/prodbase/configs/. Do not forget the trailing / as this path gets concatenated with the file name to produce the /netstation/prodbase/configs/standard.nsm string.

The Second configuration directory depends on the second configuration host that was specified on the Set Network Parameters panel. In the example here, the second configuration server is another Windows NT server, but it is a Release 2.5 level host. The configuration directory is therefore /nstation/configs/ and the protocol used is TFTP.

### 6.3.1.4 Booting

Press Enter to save these entries. This takes you back to the main SETUP panel where you can press Enter again to initiate the boot process.

Assuming that your server is properly configured and is reachable on the network, you should see messages similar to the ones shown below displayed on the monitor of the IBM Network Station:

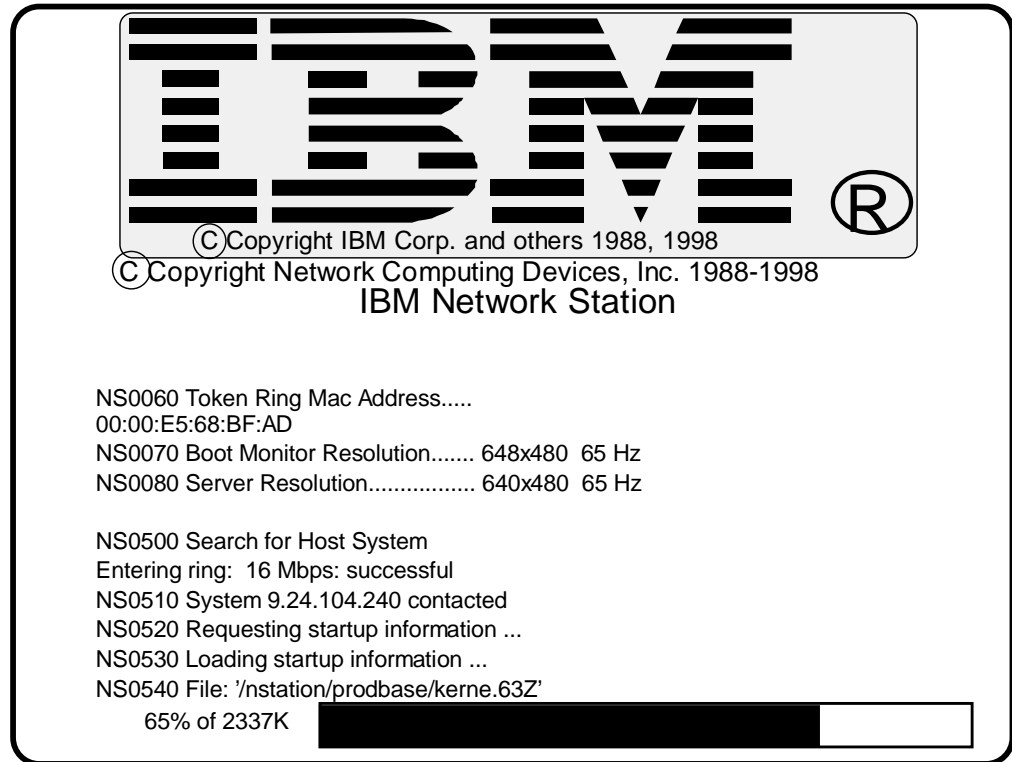


Figure 124. Kernel Loading Process

Note that the Release 3 boot monitor now has the ability to download a compressed version of the kernel and to decompress it after the download.

You might therefore see two successive progress indications on this panel, one for the download and one for the decompression of the kernel file.

### 6.3.2 Logging On

Assuming the boot process is successful, after the kernel is loaded, it takes control and loads the configuration files.

Assuming that the verbose option was turned on using the F10 key on the main setup panel, messages should be displayed on the monitor as each configuration file is read, followed by other files such as font files.

A logon screen is then displayed, asking for user ID and password, as illustrated below:



Figure 125. IBM Network Station Login Screen

Notice that the server that you are logging on to is identified in the NSC3404 message appearing on the above panel.

After you enter a user ID and a password, if the password is expired, the logon is rejected and the user is prompted to enter a new password, as is shown in the next figure:



Figure 126. Password Change Panel



Another option that the user has on the logon screen is to use the Roam button in order to change the target authentication server. If the Roam button is used, an additional small panel is displayed on top of the first one asking for a network address, as illustrated in the next figure:

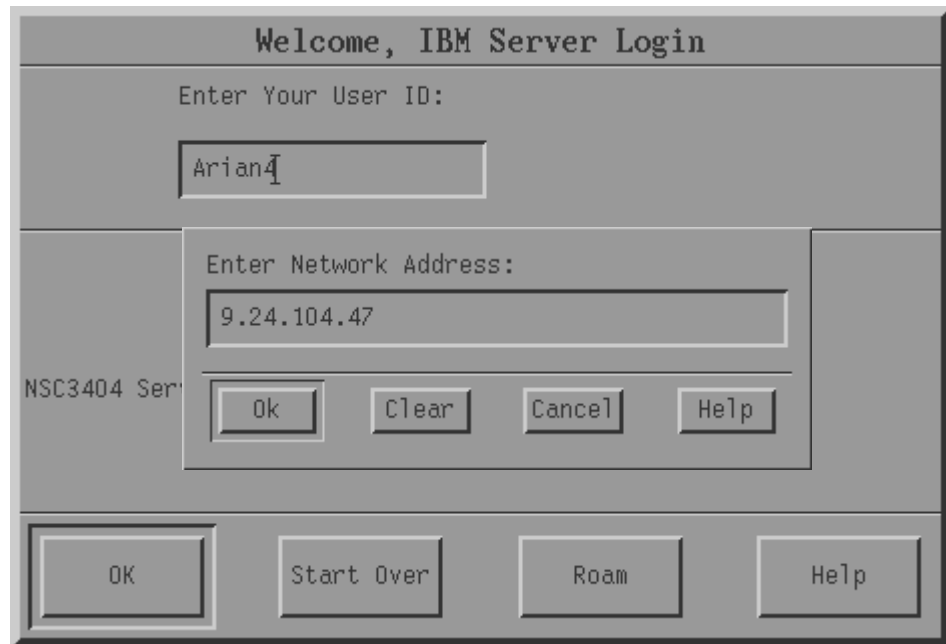


Figure 127. Using the Roam Function

When the new server is contacted, a new logon panel is displayed. See Chapter 4, "Separation of Servers" on page 101 for a description of the role of an authentication server and more details on using the Roam function.

After entering a proper user name and password (these were defined on the server and made part of the NSMUser group), the next display should be a menu bar at the bottom of the screen on the IBM Network Station.

At this point, the boot process is complete and the user can start using applications such as the emulators, or the browser, X-sessions, or Java applets or applications.

### 6.3.3 Setting Up for a Boot Using DHCP

Once you have an NVRAM boot working successfully, you can configure a DHCP server to service DHCP clients. See Chapter 10, "Dynamic Host Configuration Protocol (DHCP)" on page 175 for more details on DHCP.

On the IBM Network Station, setting up for a DHCP boot requires very little information.

After powering up, display the Network Station Setup Utility panel by interrupting the boot sequence, and pressing F3 to enter the Set Network Parameters panel, as shown below:

SCRN04

IBM Network Station  
Set Network Parameters

IP Addresses from ..... Network NVRAM

DHCP IP Addressing Order ..... 1

BOOTP IP Addressing Order ..... 2

Use cursor keys to select option

Enter = Save F12=Cancel F11=Restore Parameter

Figure 128. Set Network Parameters - Network

Select **NETWORK** instead of NVRAM on the IP Addresses from line. This eliminates the NVRAM set of parameters and displays only the network-related parameters.

You only need to ensure that the DHCP IP Addressing Order is set to 1 so that DHCP will be tried first, and, in the case of an Ethernet adapter, select the Version 2 or IEEE 802.3 standard.

Press Enter to save the settings, and press Enter again on the main panel to initiate the boot process.

You should get basically the same messages as with the NVRAM boot, up to the point where the network has been successfully entered. At that point, you should see the words DHCP appear, and after a slight delay, the kernel should load if the station was successful at getting network information from the DHCP server.

If unsuccessful, please refer to Chapter 19, "Problem Determination - Tools, Tips and Techniques" on page 363 for guidance on some of the tools that can be used to do problem determination.

## Chapter 7. Using the IBM Network Station Manager Application

The objective of this chapter is to present only a very brief overview of the IBM Network Station Manager application.

Since this application has a user-friendly graphical interface with good online help for every field that can be configured, there is little point for us to describe all of these in details.

We find that the best way to learn how to use the IBM Network Station Manager is simply to explore at will, hands-on.

### 7.1 What Is IBM Network Station Manager?

The IBM Network Station Manager is a browser-based tool for centrally administering the configuration of IBM Network Stations and of their user's preferences. Using the IBM Network Station Manager, the administrator can make IBM Network Station parameter settings on a system-wide basis, workstation basis, group basis or individual user basis.

Since the IBM Network Station Manager (NSM) is a standard browser application, it can be accessed from any browser from any platform, as long as the browser is JavaScript-enabled.

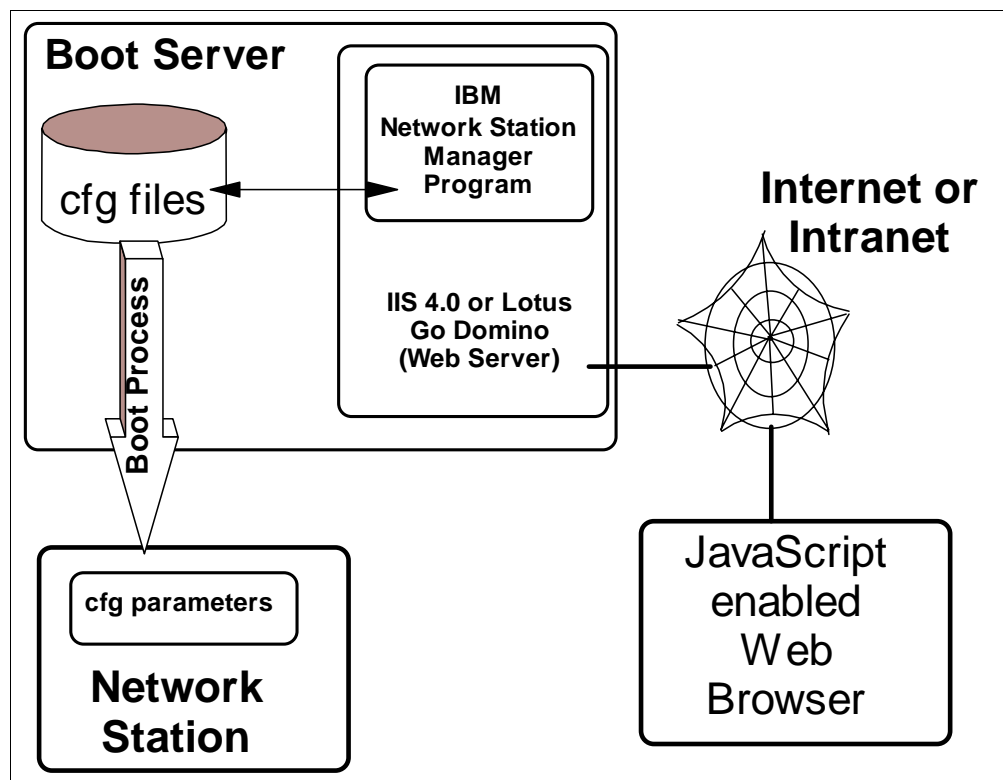


Figure 129. Accessing the IBM Network Station Manager

The IBM Network Station Manager is a configuration tool, presenting a graphical interface to the administrator who needs to administer a network of IBM Network Stations.

Actually, configuration settings and changes made using the IBM Network Station Manager result in an update, by the NSM, of the different \*.nsm configuration files residing on the server. These files are reserved for use by the IBM Network Station Manager and should not be altered in any way by an administrator. Altering these files compromises the ease with which future migrations can be done.

Any required manual overrides should be made by the administrator using the back door files, which are specific configuration files provided for the explicit purpose of manually overriding some parameters settings without the need to alter the actual files that the IBM Network Station Manager uses. See Chapter 13, "Configuration Files Structure" on page 221 for details on the configuration files.

---

## 7.2 How to Access the IBM Network Station Manager

The URL to specify to access the Network Station Manager on an NT server is:

`http://IP address or hostname/networkstation/admin`

If you are using a browser on the server where the NSM is located, you can use the loopback address of 127.0.0.1 instead of a real IP host address.

At this point, you are presented with a User ID/Password prompt panel. The user ID you use here must be defined in the local Windows NT security database and it must belong to either the NSMAdmin or the NSMUser groups.

If the user belongs to the NMSUser group, only a subset of functions is available to him or her, since, as a user, he or she cannot be allowed to change system-wide settings or settings for other users.

If the user belongs to the NSMAdmin group, he or she is then allowed to specify settings for all users and all workstations. The panel illustrated in the next figure is the main IBM Network Station Manager panel, after the user has been properly authenticated.



Figure 130. The IBM Network Station Manager Main Panel

On the left-hand side of the panel is the Setup Tasks list. Some of the tasks have a plus sign, indicating that they are groups of tasks, which can be expanded. These expand into the following tasks:

- Hardware
  - Workstations
  - Printers
- Startup
  - Programs
  - Menus
  - Environment Variables
- Desktop
  - Standard Desktop
- 5250
- 3270
- Internet
  - Network
  - NC Navigator
  - Applet Viewer

If the user logging in to the IBM Network Station Manager application is not part of the NSMAdmin group but only part of the NSMUser group, the list of tasks that

he or she gets is restricted. That user can only change some of the parameters that are applicable only to his or her user ID. The figure below shows the reduced number of tasks accessible to the user.



Figure 131. Tasks Available to the User Authority Level

The allowed tasks for a user are as follows:

- Hardware
  - Workstations
- Startup
  - Environment Variables
- Desktop
  - Standard Desktop
- 5250
- 3270
- Internet
  - Network

Selecting the Hardware/Workstation task displays the panel illustrated below:

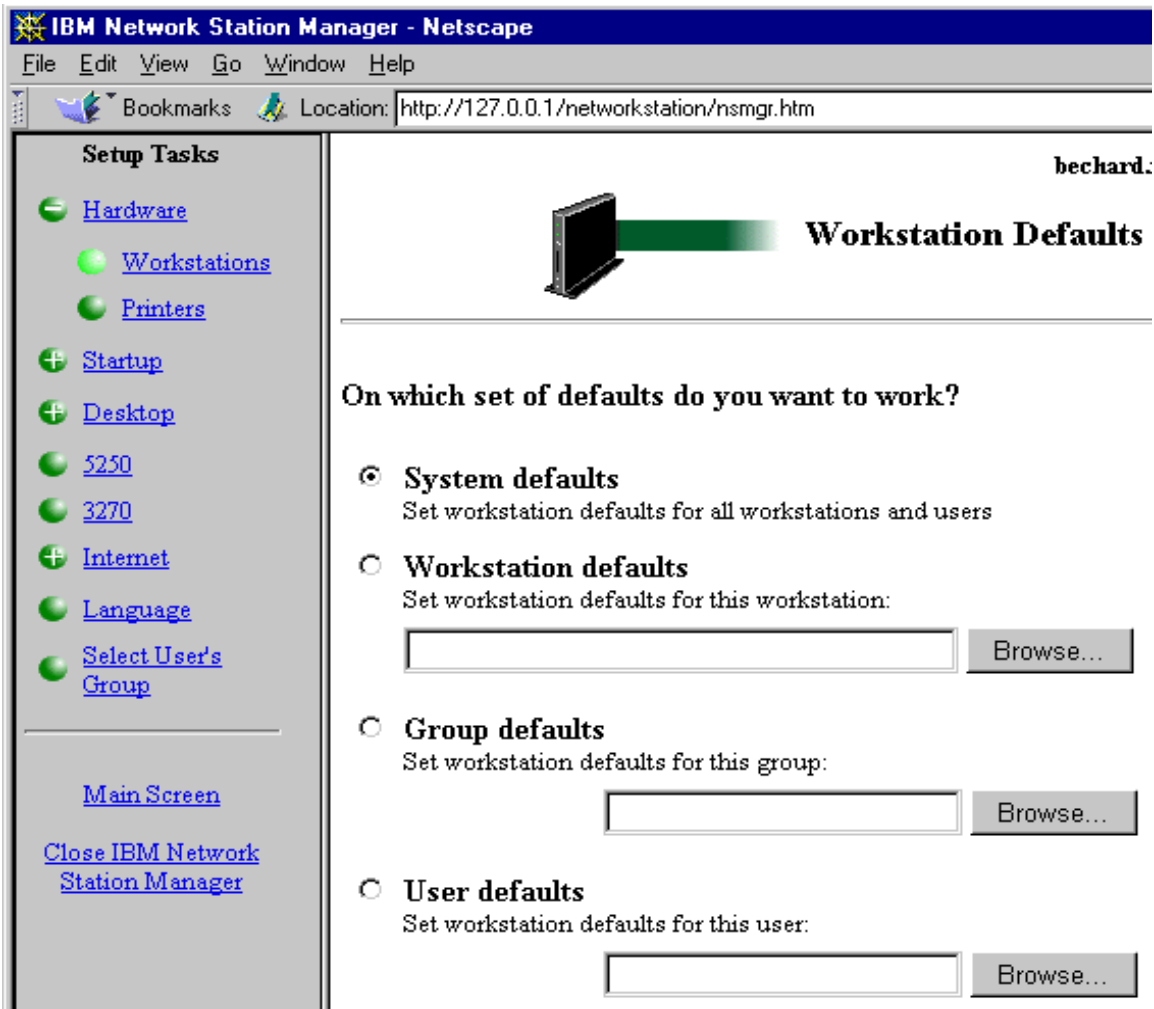


Figure 132. IBM Network Station Manager - Workstation Defaults

The panel above is very typical of many of the panels for the other setup tasks. Notice that there are four levels that can be selected in order to specify parameters:

- **System defaults**

Settings at this level are applicable to all users and all stations, and they override the shipped settings.

- **Workstation defaults**

Settings at this level apply to a particular station. Workstations can be identified using their IP host name, IP address, MAC address or IP address in hex form.

The MAC address is the only fixed piece of data that can be used to identify a particular station and should probably be the parameter used for that purpose.

- **Group defaults (Groups are new with Release 3.)**

Users can be grouped into user groups, which are defined using the User Manager for Domains application on Windows NT, and settings can be specified to apply to a specific group, such as engineers.

For these settings to apply to a user, that user must be a member of that group both at the base operating system group level and at the IBM Network Station Manager level.

- User defaults

Finally, settings made at this level apply only to a specific user.

The best way to get familiar with these settings is to browse the different tasks, explore and see the different elements that can be configured. Most of these tasks are pretty self-explanatory. If not, there is considerable online help available for all the fields.

## 7.3 A Few NSM Typical Configuration Examples

As stated above, there is little point in looking at each individual panel and each parameter that can be configured using the IBM Network Station Manager. However, it is worth giving a few examples for a few typical and common tasks that one would likely need to perform.

You can also consult the official product publication, *AS/400 - IBM Network Station - Getting Started*, SG24-2153.

### 7.3.1 Creating a 3270 Menu Bar Item

A new menu item can easily be added to the menu bar of an IBM Network Station.

For example, assume that you want to put an item on the menu bar labeled WTSCPOK, which starts a 3270 session with a host at address 9.12.14.1. and to use the name PokieA as a session title. You also want that menu item to appear on the menu bar for all users. The procedure to do this is as follows:

1. Log on to the NSM using a user name that is part of the NSMAdmin group.
2. Select **Startup=>Menu=>System defaults**.
3. Scroll down to the **3270 Menu Items** and fill in the three fields as illustrated in the next figure:

Menu item label	System/390	Session title (optional)
* WTSCPOK	9.12.14.1	PokieA

Figure 133. Adding a Menu Item

On the panel displayed above, we have only shown the parameters that we were interested in entering in order to save space, but there are other parameters that can be specified on that panel, as shown on the display below.



Figure 134. Adding a 3270 Menu Item - Additional Parameters

### 7.3.2 Autostarting an Application

In addition to building a menu bar item for that 3270 application, we also want to autostart that same application for all users when they log on.

The data to be entered here is the same, except that in this case, we do not need to supply a menu item label.

The procedure to follow is:

1. Log on to the NSM as an administrator.
2. On the Setup tasks, select **Programs=>System defaults** and scroll down to the **3270 Sessions to AutoStart** item.
3. Under System/390, enter 9.12.14.1 and under session title, enter PokieA, as illustrated in the figure below:

Figure 135. Autostarting an Application

### 7.3.3 Adding a Remote Program Menu Item

Assume that you need a menu bar button to start an aixterm application on a RS/6000 and reroute the display output to your IBM Network Station's monitor. This time, let's make this applicable only to a specific user.

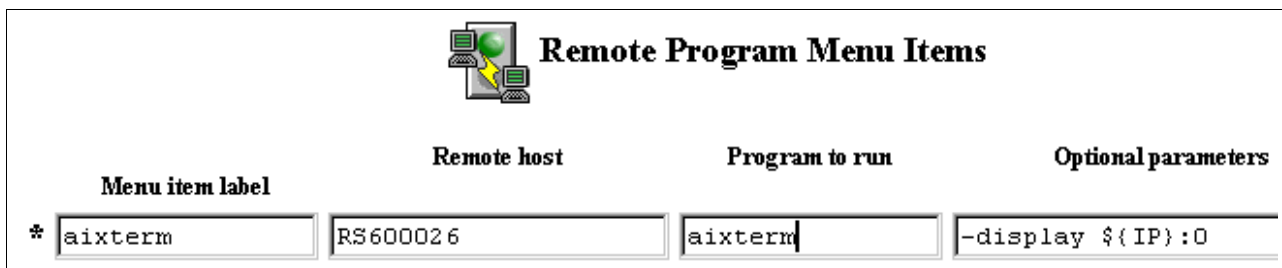
The procedure is:

1. Log on to the NSM as an administrator.
2. On the Setup Tasks, select the **Startup=>Menu**.
3. Select a specific user (by browsing or by entering the name).
4. Scroll down to **Remote Program Menu Items**.
5. Add a Menu item label called aixterm.

The target host name is rs600026, the command is aixterm, and the optional parameter is -display \${IP}:0.

The -display \${IP}:0 parameter instructs the application to export its display to the host represented by the IP address specified; the \${IP} here is a variable that is replaced with the IP address of the IBM Network Station when it issues the command.

This way this command is valid for any IP address that the workstation might be using so that if you are using DHCP and using different IP addresses for stations, then it is useful to make the command independent of the IP address.



Menu item label	Remote host	Program to run	Optional parameters
* aixterm	RS600026	aixterm	-display \${IP}:0

Figure 136. Adding a Remote Program Menu Item

The result of the above definition is that NSM creates an entry on the menu bar that when clicked, issues an RSH command to the remote host specified to execute the command specified in the Program to run field. It also places the name of the host in the access control list for the authorized hosts that have access to the local x-server so that the remote application is allowed to display its output on the station issuing the command.

#### 7.3.4 Adding a Local Program Menu Item

A local program is some function that you want to execute on the IBM Network Station itself, but since there is no command line equivalent, one way to do this is to set up menu item that can start local functions.


We have two examples here:

1. Local telnet session

We want to open a telnet session to display our message log instead of looking at the messages on the console. Since this is a telnet session with ourselves, we enter a menu item label as Messages, the program to run is telnet, and the parameters are 127.0.0.1, which is our own address, and port 5998 which is the port for messages.

2. Local command

The Show Version command is the equivalent of using the Statistics pull-down on the Console and selecting Show Version. To do the equivalent from a menu bar, choose a label (we used Version), enter `show` as the command and `version` as the parameter, as displayed in the figure below:



### Local Program Menu Items

Menu item label	Program to run	Parameters
* Messages	telnet	127.0.0.1 5998
* Version	show	version

Figure 137. Adding a Local Program Menu Items

See 19.5.1, “Commands” on page 377 for an idea of some of the commands that can be issued locally.

### 7.3.5 Adding a Terminal Menu Item

The Messages menu item that we added above can be added in another way. Since this is a telnet session, there is also a Terminal Menu Item configuration available that can be used.

This is illustrated in the next figure where we enter the label `diag2`, the remote host as `localhost` (which is the same as specifying 127.0.0.1) and the parameter 5998. In this case, we did not have to specify the telnet command since this is the command that is assumed in this configuration item.



### Terminal Menu Items

Menu item label	Remote host	Other parameters (optional)
* diag2	localhost	5998

Figure 138. Adding a Terminal Menu Item

**Note:** This command can also be issued from the browser by using the URL `telnet://hostname`.

### 7.3.6 Starting a Java Applet

This example puts a menu item on the menu bar to start a Java applet. Let’s call it `java-blink` and use the blink demo application from the Java Development Kit (JDK), and let’s make it available to all users.

The procedure is:

1. Log on to the IBM Network Station Manager as an administrator.

2. Under the Setup Tasks, select **Startup=>Menu=>System defaults** and scroll down to the **Java Applets** menu.
3. Add an item, calling it java-blink.
4. Specify the Applet URL as  
/netstation/prodbase/javademo/blink/example1.html.
5. Create a \javademo\blink directory under the \nstation\prodbase\ directory.
6. Copy the blink.class and example1.html modules from the demo/blink directory under the JDK directory to the directory you just created (because this must be a directory accessible by the IBM Network Station).



Menu item label	Applet URL
Blink	/netstation/prodbase/javademo/blink/example1.html

Figure 139. Adding a Java Applet Menu Item

Remember that you can run multiple Java applets simultaneously but that you cannot run both an applet and a Java application at the same time.

### 7.3.7 Adding a Java Application Menu Item

The procedure for adding a Java application is similar to the procedure for an applet:

1. Log on to the NSM as an administrator.
2. Select **Startup=>Menu=>System defaults**.
3. Scroll down to the **Java Application Menu Items**.
4. Add an item, calling it javaAppl for example.
5. Specify the class name. We used Claude (case-sensitive), which was a simple application printing out Hello World.
6. Specify the classpath.

In our case, we put our class in a directory called  
\nstation\prodbase\javademo\appl.

Remember that the directory specified must be accessible by the IBM Network Station. Since we know that the \nstation\prodbase directory is already accessible though NFS, we put our javademo directory under that directory.

Notice as well that we specify /netstation/prodbase/javademo/appl as the classpath, using forward slashes since this is the local directory name used on the IBM Network Station and not the actual Windows NT path with reverse slashes.

Our sample entry is illustrated in the next figure:



### Java Application Menu Items

Menu item label	Application (class) name	Arguments (optional)	Class path
JavaAppl	Claude		/netstation/prodbase/javademo/appl

Figure 140. Adding a Java Application Menu Item



---

## Chapter 8. Emulators, Browser and Java

This chapter provides only a summary highlight of the new functions in the emulators, browser and Java support in Release 3.

It is only meant as a quick guide to the main differences from the previous version.

---

### 8.1 5250 and 3270 Emulators

The main changes in the 3270 and 5250 emulators are described below.

See *IBM Network Station Manager Installation and Use, SC41-0664* for a description of how to use the emulators.

#### 8.1.1 Converged 3270 and 5250 Emulators

The 3270 and 5250 emulators have been converged, which means that there are two separate executables but they share the same source code. This provides the 3270 emulator with many of the functions that were previously available only in the 5250 emulator, such as:

- Customized menu bar pull-downs, which can be controlled within the IBM Network Station Manager configuration panels.
- The initial emulator window location and size can be set in IBM Network Station Manager.
- The status (OIA) line has Shift/Caps indicators, input inhibited indicators and cursor position.
- The presentation space can be printed (screen print) to PostScript, PCL and ASCII printers. Note that GDDM graphics are not printed and host print (TN3270E) is not supported at this time.
- Record/Playback, including auto-logon.
- Copy/Cut/Paste using the Edit menu. (Linear and rectangular copy/paste are available.)
- 3270 miscellaneous preferences can be set.
- A rule line is available.

#### 8.1.2 Additional 3270/5250 Emulator Enhancements

There are also enhancements that are provided that apply to both emulators. These are:

- Ability to specify group preferences in IBM Network Station Manager.
- Printing the emulator screen to a network printer that is configured through IBM Network Station Manager.
- A 5250 display and print (PCL and PostScript) of monochrome image and fax (3489 emulation). The 3489 128K image/fax size limitation has been removed; the default of 400K can be changed in IBM Network Station Manager.
- There are now pop-up and pull-down keypads that can be customized by the user, including playback files.

- Hot Spot highlighting is now available.
- The browser can now launch a 3270 emulator by using a URL of tn3270://hostname where hostname is, for example, wtscpok.itso.ibm.com or an IP address such as 9.12.14.1.

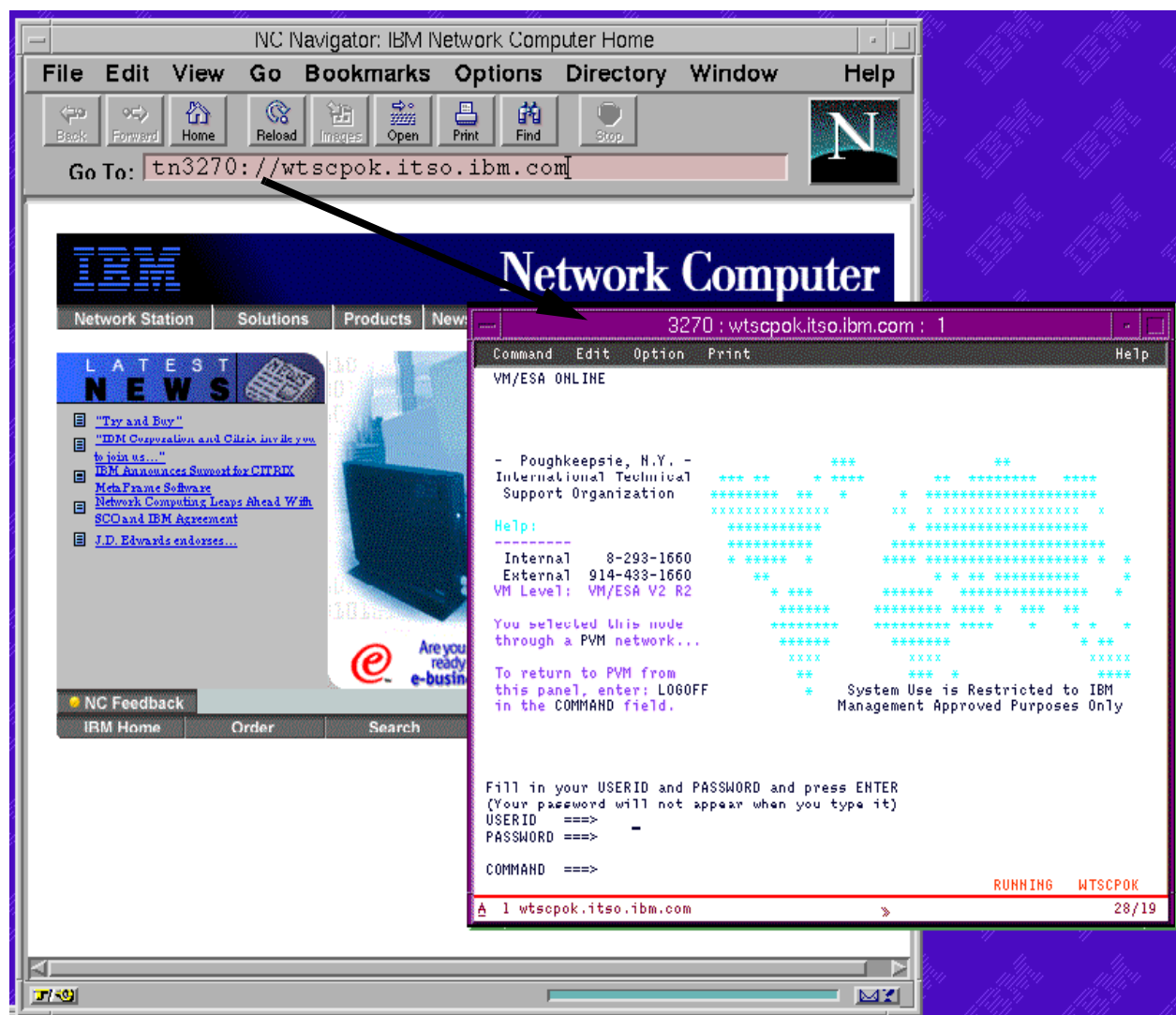


Figure 141. Using TN3270 from the Browser

- The browser can also launch a telnet session by specifying telnet://host.
- The 3270 window characters are now available in any screen size, with graphics on or off.
- Use of the Maximize button now changes to the best font.
- Any key (defined in the keyboard remapping) can now start a playback file.
- Keyboard remapping files can be named to allow the administrator to set up multiple default keyboard remapping files for different users.
- Advanced keyboard mapping is available for 3270 light pen emulation.



### 8.1.3 Additional NLS Enhancements

A few additional National Language Support enhancements have been included.

There is now support for upwards of forty languages. The list can be obtained in the IBM Network Station Manager Language Setup task.

This means that the emulator menu bar, pull-downs, dialog boxes, online help text and emulator assist programs such as keyboard remapping, color mapping and record/playback, are now available in the language of your choice.

There are also many additional keyboards that are supported in this release.

### 8.1.4 Emulators and Java

The emulators now support the Host Access Class Library. This is a support, similar to what was provided by HLLAPI, that allows a Java applet or application to take over the emulator window and interact with the presentation space. This allows a way of automating interactions with the emulator using a Java-based program.

Java access is provided but the application itself must be provided by the user.

These Java class libraries provide the following functions:

- Access (read/write) to the emulator presentation space (screen data)
- Send events when the host updates the emulator window
- Send events when the user presses a key/mouse in the emulator window

The IBM Network Station HACL interface is as close as possible to the Java Host On-Demand (HOD) 3270/5250 emulators.

Note that HACL supports multiple 3270 or 5250 sessions, but not the combination of both at this time.

Support for HACL must be enabled when the session is started by including the -ECL option. This can be entered in the NSM Startup Programs or Menus in the Other Parameters field.

### 8.1.5 Terminal (VT320) Emulator

VT320 emulator support configuration is now provided in NSM so that a terminal emulator session can be launched from the menu bar or autostarted.

This is configured in Startup Programs or Menus, as illustrated in the next figure, where we have configured a diag2 menu item that starts a local session to port 5998 in order to display the console messages and another one called To w3 which telnets into an AIX host at w3.itso.ral.ibm.com.


 <b>Terminal Menu Items</b>		
Menu item label	Remote host	Other parameters (optional)
diag2	localhost	5998
To W3	w3.itso.ral.ibm.com	

Figure 142. Terminal Menu in NSM

The next figure shows the parameters that can be specified in the Other parameters field. This list is obtained by doing a help on the term command:

```

NCDterm VT320 terminal emulator
The available options are:
  -/+132          enable/disable 132 column mode
  -b              <margin>    inner margin
  -bd            <color>     border color
  -bg            <color>     background color
  -bw            <border>    border width
  -cr            <color>     cursor color
  -ctype         <conntype>  connection type to start, valid ones:
                           telnet lat cterm serial
  -/+cu          enable/disable curses emulation
  -fg            <color>     foreground color
  -fn            <fontname>  specifies the font name for normal text
  -geometry      <geometry> where to place NCDterm and size
  -help          this help text
  -host          <hostname> specify the host to start on
  -iconic        start in iconic form
  -/+j           enable/disable jump scrolling
  -/+mb          enable/disable margin bell
  -ms            <color>     pointer color
  -n             <icon_name> icon name
  -name          <classname> classname for the window
  -nb            <number>    margin bell in characters from right end
  -rv            reverse video
  -/+rw          enable/disable reverse-wraparound
  -/+sb          enable/disable scrollbar
  -title         <titlebar> title for the window (single token)
  -/+vb         enable/disable visual bell
  -xrm           <resource_string>

```

Figure 143. The Terminal (VT320) Emulator Command Options

The previous way of starting a terminal using the IBM Network Station console is still available.

The current limitations are that this terminal facility generally supports only the languages in the Latin 1 category and only offers hand-edited keyboard mappings.

---

## 8.2 NC Navigator Browser

The NC Navigator browser provided in this release is a version of Netscape Navigator based on the UNIX version of Navigator 3.04.

See *IBM Network Station Manager Installation and Use, SC41-0664* for a description of how to use the browser.

Use the Help button on the top right-hand corner of the browser session for a list of new features and for the answer to frequently asked questions. What is provided here is a quick summary of the information available through these help panels.

**Note:** The IBM Network Station browser, available in the previous version, has been discontinued. Existing bookmarks for that browser, however, are automatically migrated to NC Navigator bookmarks if present on the system being migrated. See Chapter 3, "Migration from Release 2" on page 71 for information on migrating.

It is compatible with Netscape Navigator 3, has the same look and feel as the UNIX version, the same level of HTML 3.2 and JavaScript 1.1.

The 40-bit version is always installed by default as part of the IBM Network Station Manager installation process. For North America, there is an option of installing the 128-bit version, which must be subsequently enabled by including an environment variable called NAV\_128SSL=TRUE. See 2.5.4.5, "NC Navigator Selection" on page 31 for more details.

In IBM Network Station Manager, use the Internet Setup task to configure items such as:

- Proxies for FTP, HTTP, Gopher, HTTPS
- Exclusion domain ranges for FTP, HTTP, Gopher
- Servers for SMTP, POP3, NNTP, Socks
- Personal preferences such as user name, ID, e-mail address, reply to and home page

In IBM Network Station Manager, use the NC Navigator setup task to configure items such as:

- The proxy's setup method
- The rate for mail check
- Enabling/disabling JavaScript and Java
- Setting up navigator directory buttons

What has been added is:

- E-mail and News Reader clients so that mail can be received and sent to a POP3 server and news can be read from a NNTP server. It uses POP3 for incoming mail and SMTP for outgoing mail.
- Java 1.1. and network support

- New helper applications such as TN3270 and TELNET can be invoked from the browser. In fact, the browser calls local native applications to perform the function.
- Remote printing, so that PostScript level 1 output can be sent to any printer that has been defined by the administrator.
- National language support for a few languages such as Japanese, Korean and German.

The features that are not supported are:

- LiveConnect (Java integration with JavaScript and plug-ins).
- Plug-ins, hence no audio, video, Shockware, PDF, etc.
- Non-PostScript printing. Use Anyprint on a server to transform to other data streams if necessary. See *IBM Network Station Printing Guide, SG24-5212* for details on how to use transform.

Note that memory requirements have increased relative to the previous release because of the additional functions included, and is now set at 32 MB, and probably more if running large Java applets.

---

## 8.3 Java

What is new in Java for this release are the following items:

- The JRE has now been upgraded from 1.1.2 to 1.1.4, which provides some fixes, internationalization support (i18n) and full Year 2000 compliance.
- Performance improvements by some reduction in memory usage and allocation and reducing class load time.
- Support for JIT, which must be explicitly configured in IBM Network Station Manager, in order to help with computer-intensive applications.

For details on how develop thin-client Java applications in a network computing environment, please refer to *Java Thin-Client Programming for a Network Computing Environment, SG24-5115*.

---

## Chapter 9. NFS, TFTP and Time Servers

The eNetwork On-Demand product replaces what was called the IBM TCP/IP Services in Release 2. It includes the following functions:

- A Dynamic Host Configuration Protocol (DHCP) Server
- A Dynamic Domain Name (DDNS) Server
- A Network File System (NFS) Server
- A Trivial File Transfer Protocol (TFTP) Server
- A Time Server
- A Remote Procedure Call (RPC) Portmapper Server

All of these servers are installed automatically as NT Services by the eNetwork On-Demand Server installation process, except for the DHCP and DDNS servers, which can optionally be selected by the user during the install process.

They are the required basic services to be present on a server so that an IBM Network Station can connect into the server and request files to be downloaded.

This chapter provides a brief overview of these different servers, their role, and their configuration interface. The objective is not to provide an in-depth tutorial on each of these servers but to provide the user with enough information to allow him or her to get up and running quickly and to do basic problem determination on his or her own.

The DHCP server and DDNS server are discussed in separate chapters: Chapter 10, "Dynamic Host Configuration Protocol (DHCP)" on page 175 and Chapter 11, "Dynamic Domain Name Services (DDNS)" on page 199.

---

### 9.1 Trivial File Transfer Protocol (TFTP) Server

With this release of the IBM Network Station Manager, since NFS has become the preferred method of booting, there is probably little use for the TFTP server anymore.

However, it can still be used to provide TFTP access to files on the boot server if required by applications, and it is used in the migration process during retargeting of the client stations, which are still configured to access their server through TFTP.

#### 9.1.1 TFTP Configuration

To start the TFTP Server Configuration interface, select **Start=>Programs=>eNetwork On-Demand Server=>TFTP Server Configuration**, which brings up the following panel:

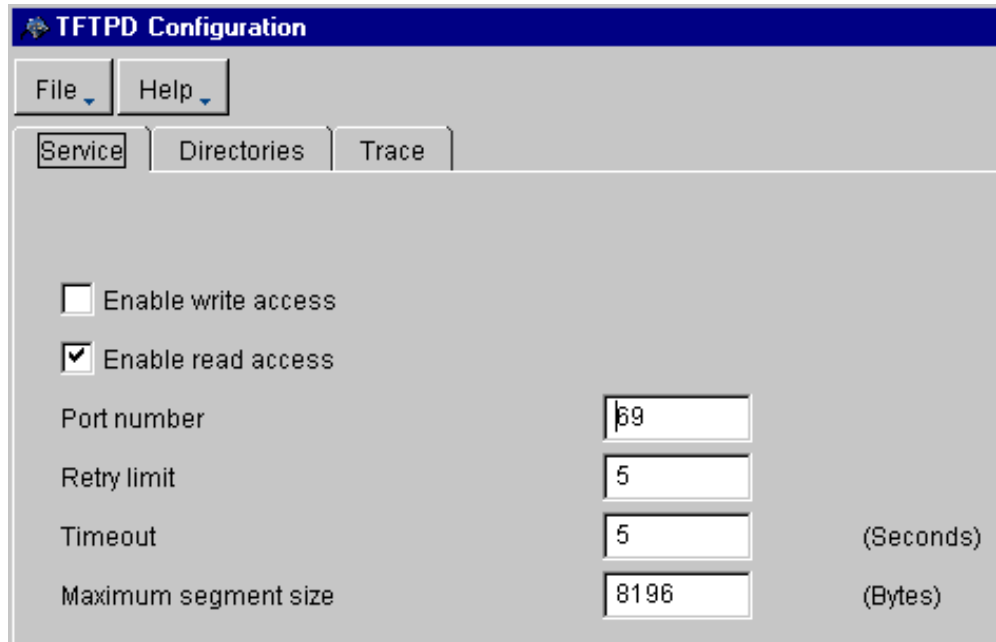


Figure 144. TFTP Configuration Panel - Service

Notice that the read or write access defined here applies to all the directories defined on the next tab. In other words, this server does not allow you to specify a read or write permission on a file-by-file basis, as NFS can.

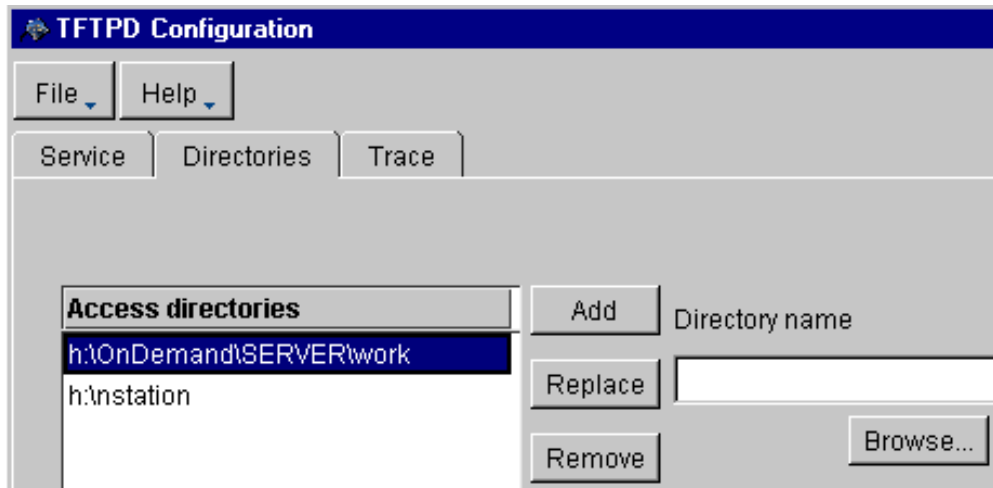


Figure 145. TFTP Configuration Panel - Directories

The figure above displays the directories that are configured by default when the TFTP server is installed.

The x:\instation directory is there mainly for backwards compatibility reasons, as this was the required Release 2 configuration, and for migration reasons.

The x:\OnDemand\SERVER\work directory might be used, for example, if you wanted to upload a dump file from the IBM Network Station; however, since the

access is specified as read only, you will need to change this to write before you can use this function.

### 9.1.2 TFTP Tracing and Logging

The Trace tab allows you to enable the trace function, and to specify which trace options and trace file name you want to use.

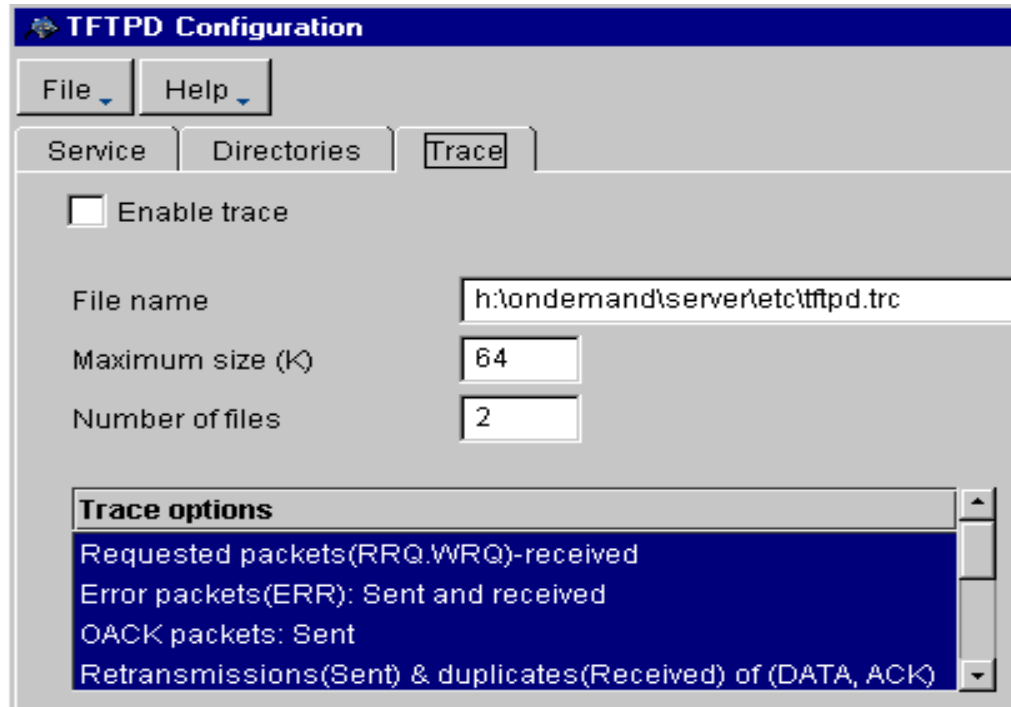


Figure 146. TFTPD Configuration Panel - Trace

### 9.1.3 TFTP Help

The Help button can be used to take you to what is termed the Product Documentation, which means the on-demand server documentation that covers all the other servers (NFS, DHCP, etc.) as well. This is an HTML-based facility that brings up the panel illustrated in the next figure in your default browser.

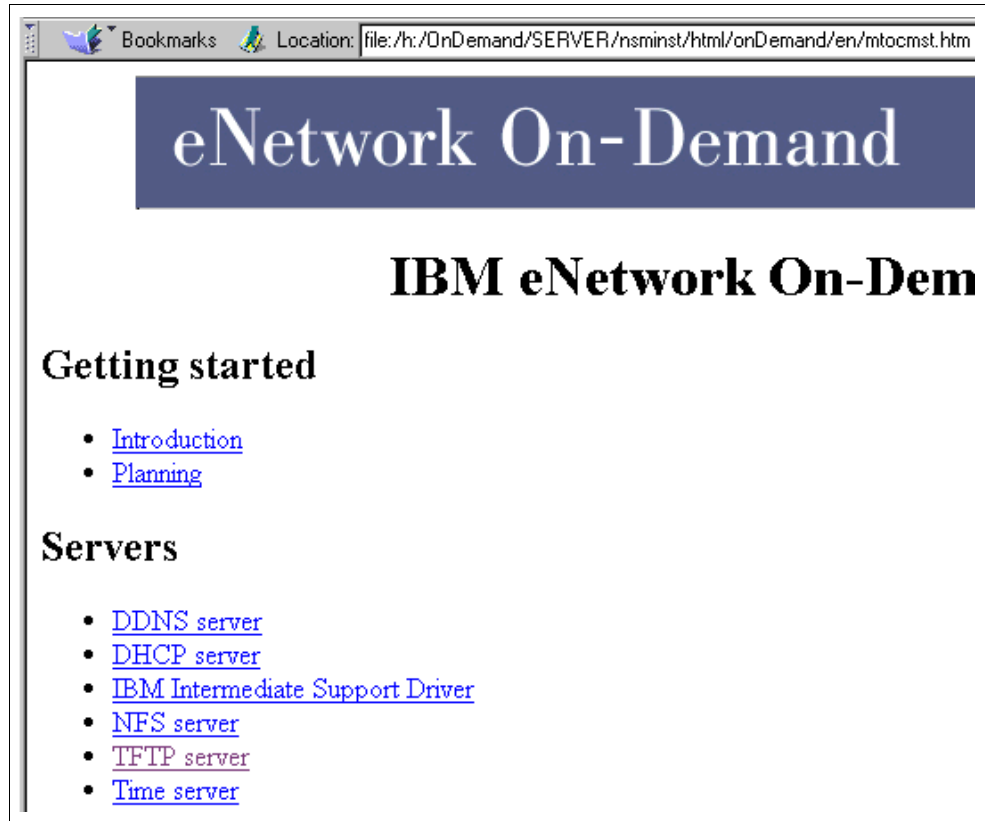


Figure 147. eNetwork On-Demand Server Product Documentation

If you select Contents instead of Product Documentation in the Help pull-down while in the TFTP server configuration interface, it brings up the same HTML interface but it is then already positioned at the TFTP server information section, as illustrated below.

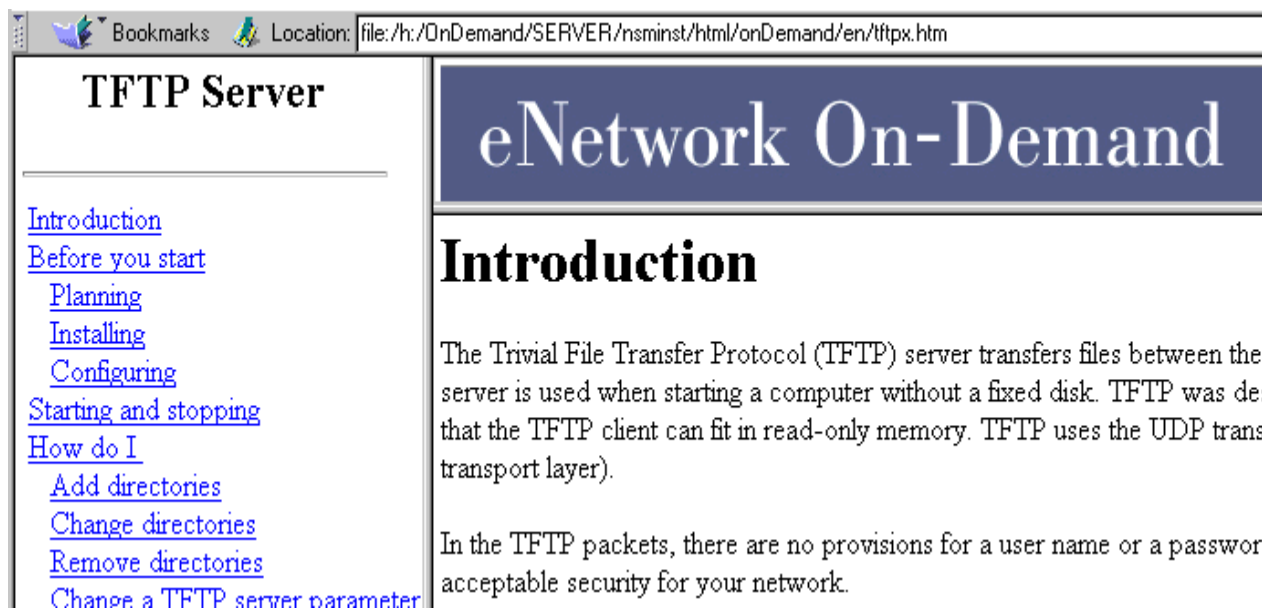


Figure 148. TFTP Server Documentation



## 9.2 Time Server

Because the IBM Network Station does not have a local clock, it needs to get the time from a server, which is what the time server provides.

The time is sent from the server to the IBM Network Station at boot time, after which the time is managed by the IBM Network Station.

By default, the time server is the same as the boot server. However, the time server can be specified as any other server using the `set time-server = IP address` parameter.

The server can send Greenwich Mean Time (GMT) or local time, dependent on what is configured on the time server.

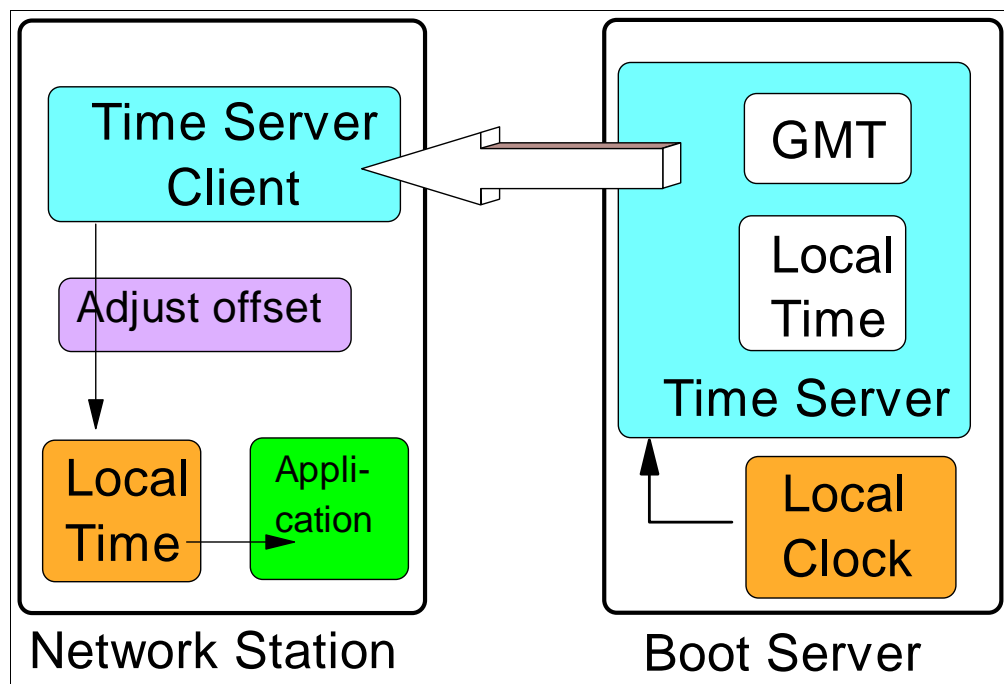


Figure 149. The Time Server

### 9.2.1 Time Server Configuration

This offset adjustment can be made either on the server or on the client:

- If the check box **Adjust to local time** is checked on the server, local time is what the server sends to the client, otherwise GMT is sent.

To start the TIMED Configuration, select **Start=>Programs=>eNetwork On-Demand Server=>Time Server Configuration**.

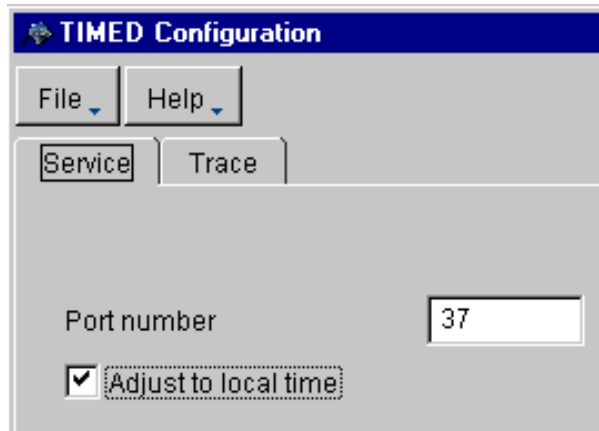


Figure 150. Timed Configuration Panel - Adjust to Local Time

- The client can also be caused to adjust the time itself with an offset to GMT by using the parameter set time-offset-from-gmt = (-719 to +720) where -710 to +720 represent minutes. The default is -480 (8 hours west of GMT).

The figure below shows the time settings as displayed on the IBM Network Station itself using the Setup pull-down from the console.

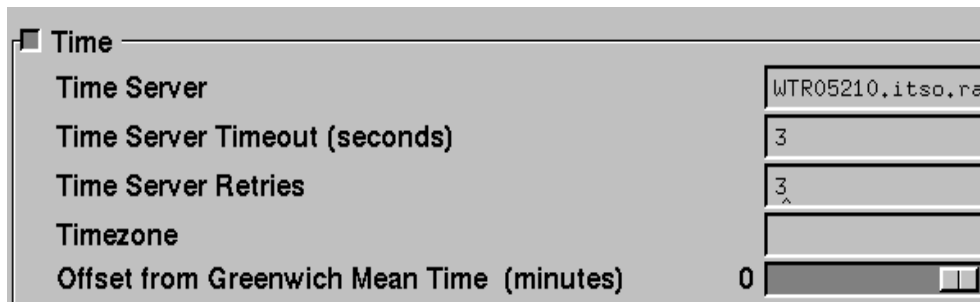


Figure 151. Time Settings on the IBM Network Station

When a change is made to the time server configuration, the server is automatically restarted and the message below is issued.

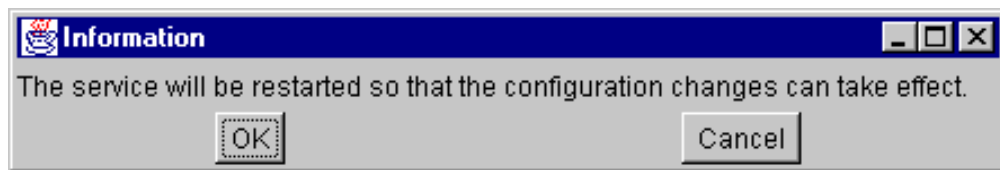


Figure 152. Time Server Restarting Message

## 9.2.2 Time Server Logging/Tracing

On the Time Server Configuration panel, there is also a Trace tab that is used to enable/disable a trace for the time server and to specify the location of the trace file.

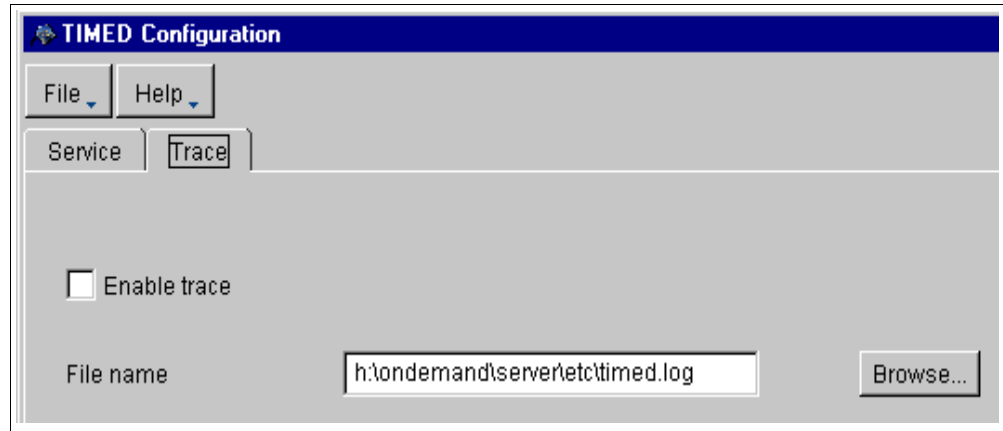


Figure 153. Time Server Log File

## 9.3 Networking File System (NFS) Server

The NFS server has changed only slightly since the last release, and the configuration panels contain mainly the same information although their appearance has changed slightly.

### 9.3.1 NFS Configuration

NFS is automatically configured as part of the installation process, so there might not be a need to use this interface.

However, if you need to make changes, you can start the configuration by selecting **Start=>Programs=>eNetwork On-Demand Server=>NFS Server Configuration**.

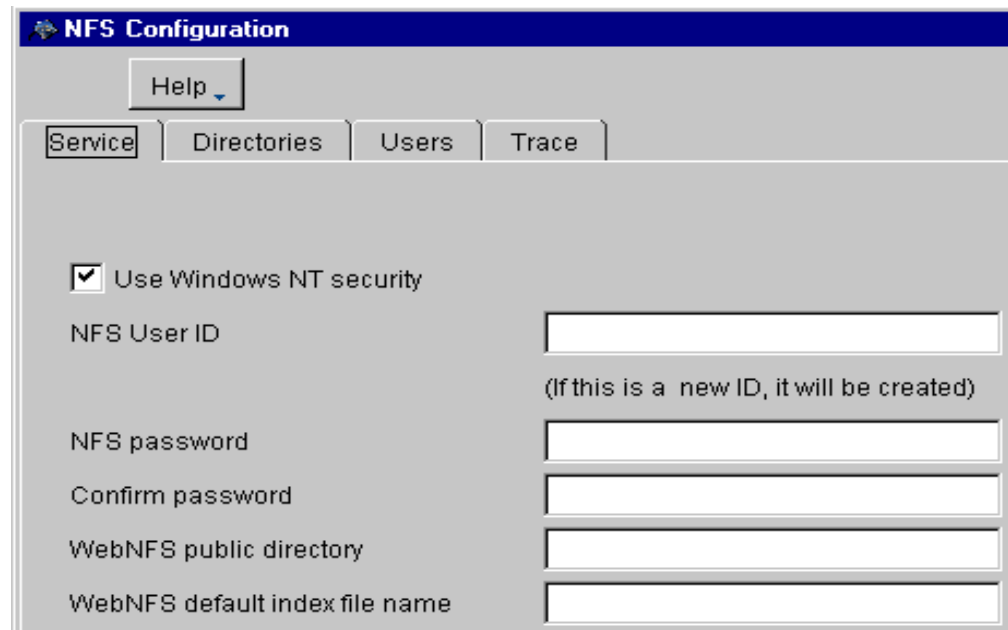


Figure 154. NFS Server Configuration - Main Panel

As in the previous release, if Windows NT security is to be used in addition to the NFS security mechanism, then ensure that the Use Windows NT security check box is marked. It is the default.

This means that the security of NFS and of Windows NT are additive and the most restrictive applies. In other words, if you specify a directory as read-write in NFS but it is read-only in Windows NT, then the level that applies is read-only.

The next tab is Directories, as illustrated in the next figure, and it contains three directories already pre-filled. The first and last are defined as read-write but the middle one is read-only.

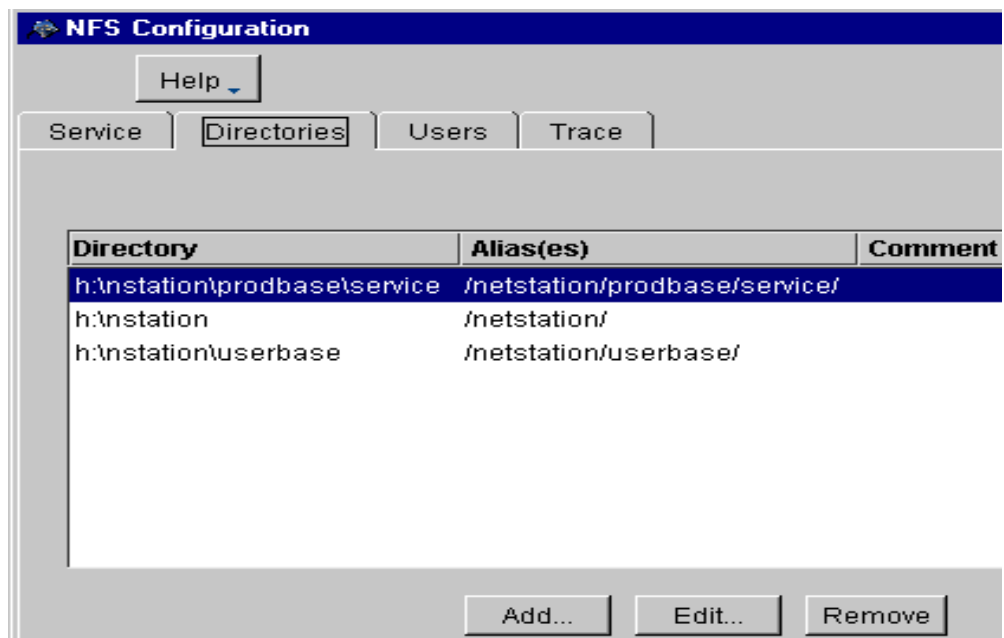


Figure 155. NFS Server Configuration - Directories

To view how any of these directories is defined, select it and then the **Edit** button, which brings up the panel illustrated below:

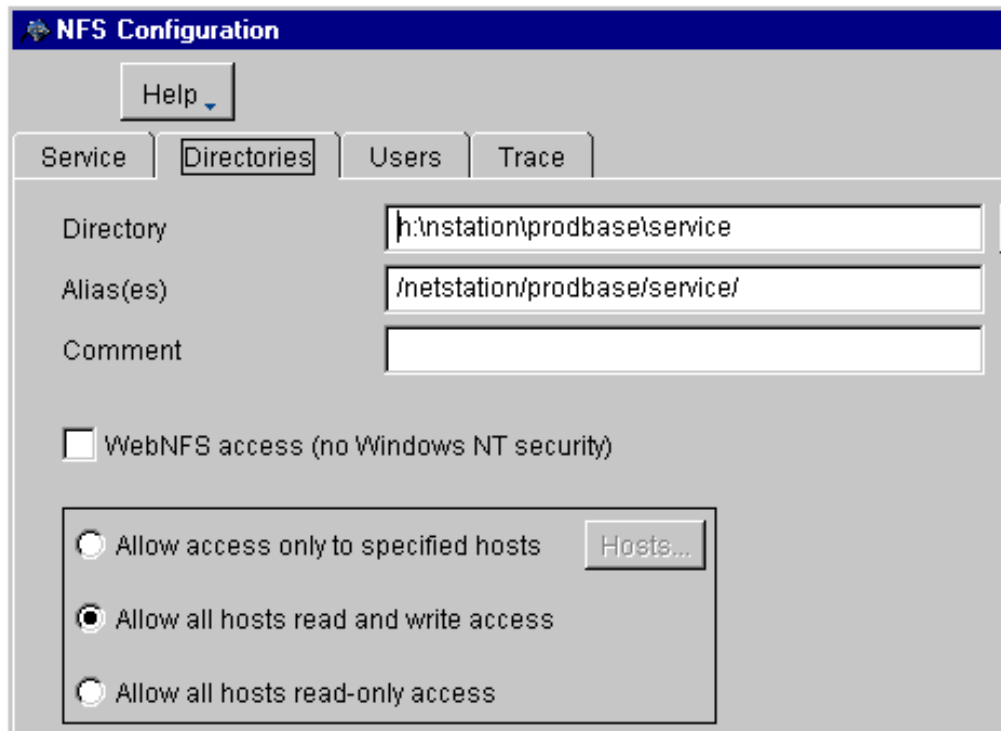


Figure 156. NFS Server Configuration - Directories - Edit

If you want to restrict access on a host basis, select **Allow access only to specified hosts**, which opens up the Hosts button and brings up a panel where you can enter the hosts information.

The next tab, Users, displays the currently defined users. For IBM Network Station Manager, it is easier to simply let users be defined automatically by the NFS server based on the Windows NT users.

As new users log in, they are added automatically and assigned a user ID which gets incremented by 1 for every new user.

The NSMNFS\_USER with user ID of -2 was added automatically by the IBM Network Station Manager installation process.

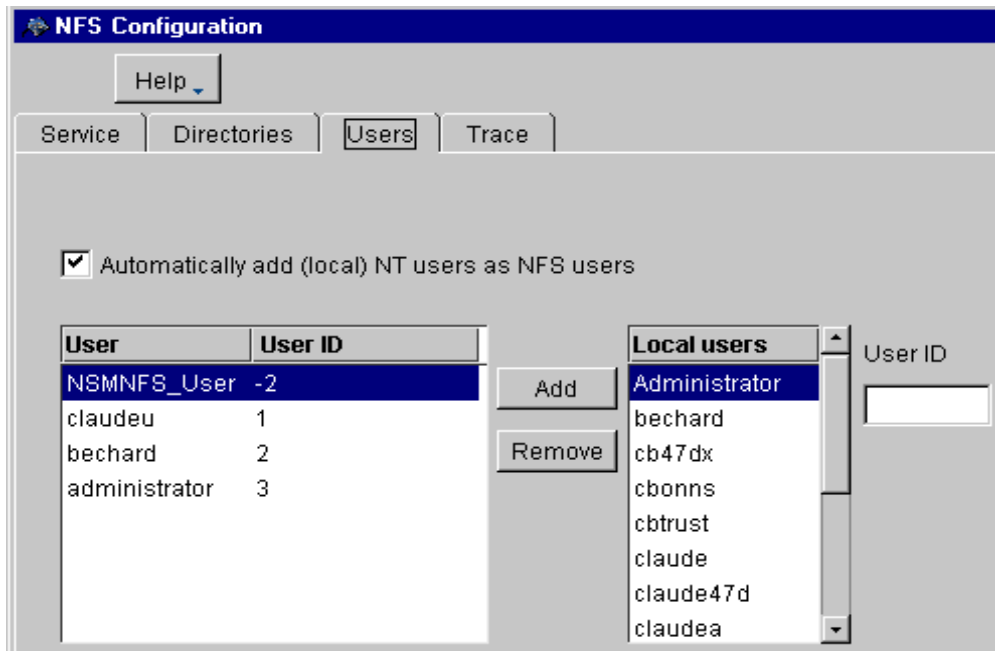


Figure 157. NFS Server Configuration - Users

### 9.3.2 NFS Logging/Tracing

The next tab is Trace, which brings up the panel in the next figure, which allows you to enable the trace, specify a trace file to be used, and one of three levels of details to be traced.

The default trace file location is as shown in the figure below:

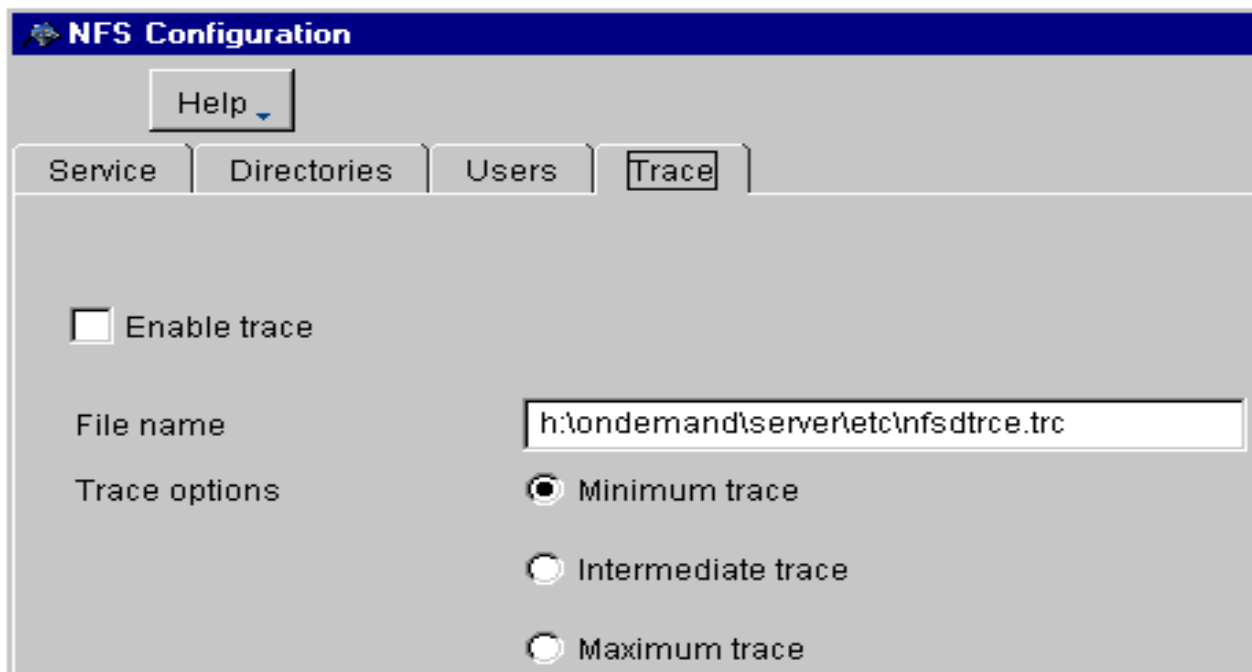


Figure 158. NFS Server Configuration - Trace

---

## Chapter 10. Dynamic Host Configuration Protocol (DHCP)

This chapter provides a brief overview of the Dynamic Host Configuration Protocol (DHCP). The objective is to provide a general tutorial, especially for those who might be new to DHCP, aimed at understanding the role of a DHCP server and how it can be used in the context of a network of IBM Network Stations.

The DHCP server itself has changed little since the last release. The changes are mainly that:

- The DHCP configuration user interface has changed slightly, although the functions are the same.
- Additional DHCP options have been added to support the separation of servers function.

For a more in-depth look at DHCP and DDNS, please refer to *Beyond DHCP - IBM's Guide to Network Communications with TCP/IP*, SG24-5280.

The product publication *IBM Network Station Manager Installation and Use*, SC41-0664 provides specific examples on how to use the DHCP configuration panels to define a specific network example, so we do not repeat such an example here.

---

### 10.1 What Is DHCP?

Dynamic Host Configuration Protocol (DHCP) is a mechanism that allows a server to allocate IP addresses to clients (IP hosts) that are inserting into the network.

In other words, an IP host inserts into the network, and broadcasts a request on the network, identifying itself with its MAC address and asking any DHCP server on the network for an IP address that it can use to become active on the network.

Once a DHCP server responds positively to the client, giving it an IP address to use for a specified period of time, the client becomes operational and uses the allocated IP address to communicate on the network.

IP addresses are therefore managed and allocated by the DHCP server to clients based on the configuration parameters of the server. Addresses can be given out on a first come first served basis, or they can be reserved for specific clients, and clients can be required to be pre-defined, or not, or a combination of all of these.

This is illustrated, in a simplified fashion, in the next figure:

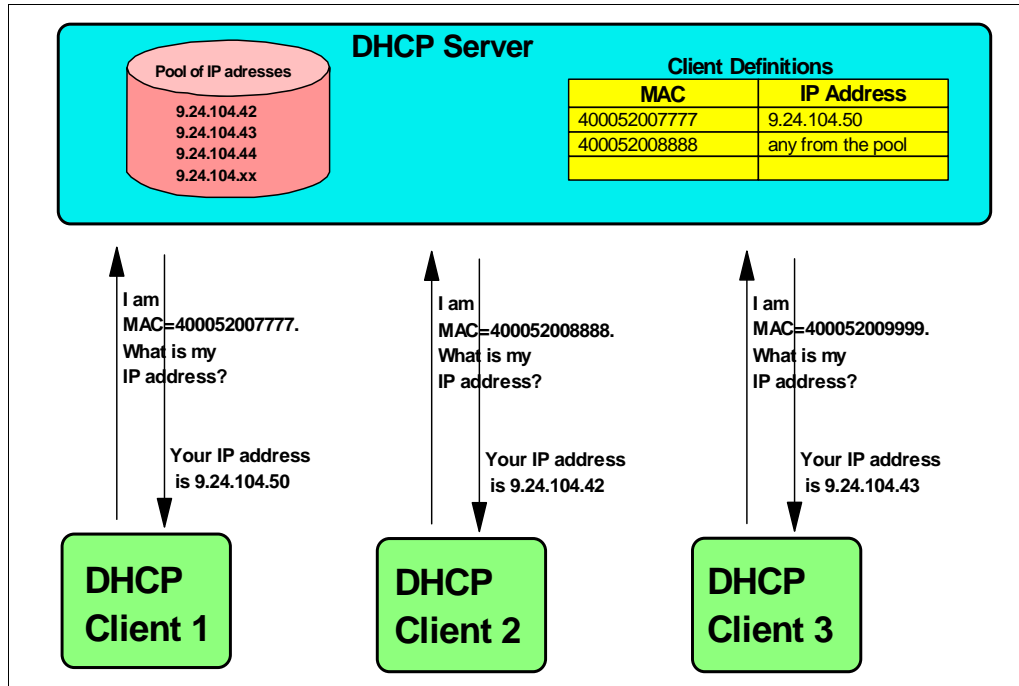


Figure 159. DHCP Overview

In the figure above:

1. DHCP client 1 contacts the server and identifies itself with its MAC address, in this case 400052007777. The server looks up its configuration table and finds out that this client is a specifically defined client and that it has a reserved address of 9.24.104.50, so this address is what is allocated to this client.

In other words, this client always get this same IP address whenever it contacts this DHCP server.

2. DHCP client 2 also identifies itself with its MAC address, in this case 400052008888, and the server finds that there is also a specific client definition for this MAC address, except that there is no specific reserved IP address stated but only an entry that says that this client can be given any address out of the pool.

Therefore, the server allocates the next available address out of the pool, which is 9.24.104.42.

3. DHCP client 3 also identifies itself with its MAC address (400052009999) but there is no definition for this client anywhere. The server has two choices here: either give out the next available address out of the pool, which is 9.24.104.43 if the server configuration parameter indicates that it is allowed to respond to unlisted clients, or if the unlisted client support is turned off then no response is generated and the client does not get an address from this server.

The two primary benefits of this approach are that:

1. As users become more mobile and take their portable computers with them to multiple sites, it becomes much more efficient for the user to be able to just connect into any local network and dynamically request an IP address compatible with the physical location the user is to use for the duration of the connection.



2. As these users may also often not require an address for more than a certain period of time, available addresses can be more efficiently managed by being constantly re-used.

### 10.1.1 Static vs. Dynamic IP Address Allocation

For a static IP address assignment, the MAC address of every potential IBM Network Station is defined in the DHCP server configuration file, along with an IP address that is reserved for the station with this MAC address. When the station sends a request into the DHCP server, identifying itself with its MAC address, the DHCP server returns the IP address associated with that specific MAC address.

The MAC address is the IBM Network Station's unique identifier; it is either hard coded in the network adapter, or it can be configured by an administrator.

**Note:** In the case of the IBM Network Station, the MAC address is displayed during the power on phase, or is available from the IBM Network Station console if you select **Statistics=>Show Version** from the console menu bar.

In large network environments, static assignment of IP addresses can become difficult if the rate of change is high and in that case, it becomes more efficient to have a mechanism for assigning IP addresses to clients in a dynamic fashion.

For dynamic IP assignment, the DHCP server is configured with a pool of available IP addresses. When it receives a client's request, it can still identify a client by its MAC address, but instead of using a fixed IP address assigned to that MAC address, it allocates an address out of the pool of available addresses. In fact, it leases one of the available IP addresses to this client for a specified period of time, and returns the address to the pool when it is either released by the client or when the lease runs out without being renewed by the client.

The DHCP server also supports the notion of unlisted clients, where it allows any client, even if its MAC address is not defined in the DHCP configuration, to request an IP address. In that case, the DHCP basically offers an IP address out of its pool of available addresses to any client. This is very useful in an environment where you do not want or need to keep track of MAC addresses. The advantage is a much lower maintenance burden.

Re-use of IP addresses can be a significant advantage when clients only use their IP address for a short duration, because a smaller number of IP addresses are then sufficient to service a larger number of clients. As long as there are enough addresses to satisfy the peak demand, every client will be able to get an address when he or she needs it.

In practice, a combination of both static and dynamic assignment is used because there are many IP hosts that must have a fixed and permanent IP address, such as DNS servers or other types of servers.

However, having a different IP address assigned to an IP host every day brings up an additional problem, that of making sure that the host name, which is often used to identify an IP host, is resolved to the correct IP address when this IP address is likely to change often. We discuss this aspect of DHCP in the next chapter when we discuss DDNS. See Chapter 11, "Dynamic Domain Name Services (DDNS)" on page 199 for additional details.

---

## 10.2 How a Client Obtains Information via DHCP

As discussed previously, a client obtains an IP address and configuration information through DHCP requests. Following is a short description of the different types of DHCP requests and how they work.

We provide these descriptions as they can be of help when doing problem determination and tracing frames between an IBM Network Station and a DHCP server.

### 10.2.1 DHCPDISCOVER

As an IBM Network Station boots, the boot monitor program reads its configuration information from the station's NVRAM to determine whether to obtain all of its boot information also from NVRAM or from the network by contacting a DHCP server.

If it is told to find information via the network, the station announces its presence by sending a broadcast frame that includes its MAC address. This is called a DHCPDISCOVER frame. If DHCP relay is implemented on the network routers, the DHCPDISCOVER request can be relayed to a specific DHCP server that resides outside of the clients' subnetwork. If DHCP relay is not enabled, the request does not cross routers and therefore all clients and their DHCP server must be located on the same LAN segment.

### 10.2.2 DHCPOFFER

Each DHCP server that receives a DHCPDISCOVER request may respond with a DHCPOFFER to the client. A DHCP server responds to either all requests if it is configured for unlisted clients, or it responds only to those clients that are defined in its configuration files, or a combination of both.

The offer includes a client IP address (for the IBM Network Station) and also includes the IP address of itself (the server). Before issuing an offer, the server may check for duplicate addresses on the network and it checks the configuration file to see if the address allocation should be static or dynamic.

In the case of dynamic allocation, the server chooses an IP address from a pool, selecting the least recently used address. If static IP allocation is used, the server uses the client statement from the configuration file to determine which IP address to send. (In other words, a specific IP address can be specifically pre-assigned to a client so that the client always gets the same address.) Upon making the offer, the DHCP server reserves the offered address (and keeps it in reserved status until it gets a confirmation back from the client that the client accepts use of this address).

### 10.2.3 DHCPREQUEST

This frame flows from the client to the server, indicating acceptance of a particular offer.

The client can receive offers from many servers and it will accept the first acceptable offer received. If none of the offers are acceptable, the client caches the offers received, restarts the process of asking for offers, and discards any offers that are similar to the one it cached.

As soon as it has one acceptable offer, the client broadcasts (a broadcast so that all servers will receive this message) a message indicating the server it selected and requesting use of the IP address from the selected server.

#### **10.2.4 DHCPACK**

If a server receives a DHCPREQUEST indicating that its offer has been selected, the server marks the previously reserved address as leased, and sends an acknowledgment frame (DHCPACK) to the client.

If a DHCPREQUEST indicates that the client has selected a server other than itself, it returns the reserved address to the pool. If the server does not receive an answer within a given amount of time, the address is returned to the pool.

#### **10.2.5 DHCPDECLINE**

After receiving the DHCPACK, the client determines whether the configuration information just received is valid. The client sends an Address Resolution Protocol (ARP) request to the supplied IP address to see if that address is in use. If the address is in use, the client declines and sends a DHCPDECLINE message back to the server. In this case, the request process begins again. If the address is valid, the client now enters a BINDING state with the server and proceeds to use the IP address and options provided.

The following diagram summarizes the process.

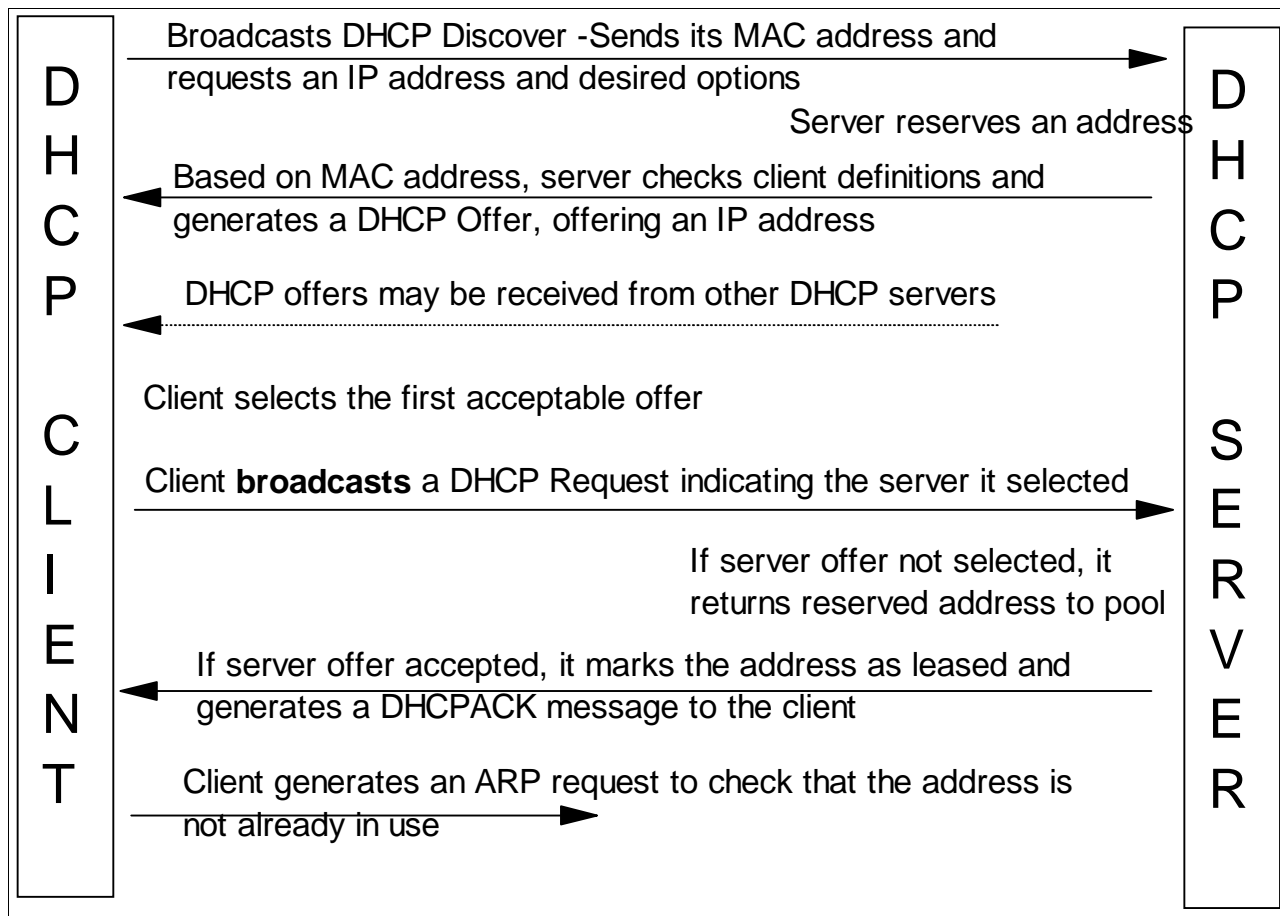


Figure 160. DHCP Boot Sequence Summary

Below is a set of records taken from an NT Network Monitor trace illustrating these activities. In fact, this particular example shows that there were two DHCP servers on this LAN segment and that the station accepted the first offer that was made.

In the records below, the station is called itsonct1, the first DHCP server is 0004AC33DBE5 and the second DHCP server is ThinkPad Claud. The events are:

- itsonct1 broadcasts a DHCP discover (frame 1).
- The first server makes an offer (frame 2).
- The station checks the validity of the address (frames 3-4).
- The second server echoes the station (frame 6).
- The second server also issues an offer (frame 7).
- itsonct1 accepts the first offer (DHCP request) (frame 8).
- The first server acknowledges the request (frame 9).
- The station checks again that the address is still valid (frame 10-11).

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
1	68.577	itsonctl	*BROADCAST	DHCP	Discover
2	68.875	0004AC33DBE5	itsonctl	DHCP	Offer
3	68.876	itsonctl	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.106.44
4	69.578	itsonctl	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.106.44
5	70.311	itsonctl	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.106.15
6	70.334	ThinkPad Claud	itsonctl	ICMP	Echo From 9.24.104.175 To 9.24.104.189
7	70.344	ThinkPad Claud	itsonctl	DHCP	Offer
8	74.586	itsonctl	*BROADCAST	DHCP	Request
9	76.715	0004AC33DBE5	itsonctl	DHCP	ACK
10	76.717	itsonctl	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.106.44
11	77.386	itsonctl	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.106.44
12	78.105	itsonctl	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.106.15
13	0.000	000000000000	000000000000	STATS	Number of Frames Captured = 12

Figure 161. An Example Trace of DHCP Discover/Offer Activities

### 10.3 What Are DHCP Options?

In the process of communicating with one another, a DHCP client and a DHCP server exchange more than just an IP address, but many other pieces of data as well, such as server address, gateway address, boot file name, etc.

Many of these pieces of data, or fields, have been pre-coded, and assigned a name and number that they can be referenced by. These are called DHCP options, and these fields are carried in DHCP frames or records that get exchanged between the client and the server.

Some typical option numbers, for example, are as follows:

- Option 1 - Subnet Mask
- Option 3 - Default Router
- Option 4 - Time Server
- Option 6 - Domain Name Server
- Option 12 - Host Name
- Option 15 - Domain Name
- Option 28 - Broadcast Address
- Option 50 - Requested IP Address
- Option 51 - IP Address Lease Time
- Option 67 - Boot File name

If there is a need for options that are not already in existence, these can be created on the DHCP server, and as long as the client and server agree on what the option numbers mean, communication is possible.

For more information on DHCP Options, please consult the online documentation.

We illustrate in the figure below a sample DHCP record. You can also reference Figure 362 on page 413 for a sample DHCP record as seen in a trace.

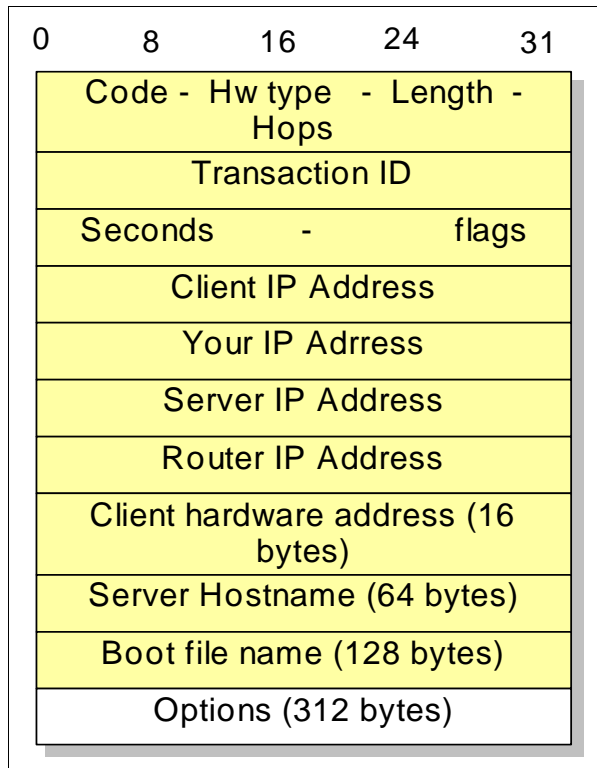


Figure 162. A DHCP Frame/Record

In fact, new options have been added in IBM Network Station Manager Release 3 in order to allow for the separation of server function, as an example.

The new options are:

- Option 211 - Base Code Server Protocol
- Option 212 - Configuration Server Address
- Option 213 - Configuration Files Directory
- Option 214 - Configuration Server Protocol

Figure 163 on page 183 illustrates how these correspond to the NVRAM Setup Utility parameter. A DHCP server can control, from a central site, key configuration parameters that determine how the IBM Network Station behaves when it boots by setting these parameters through these options.

Please refer to Chapter 4, "Separation of Servers" on page 101 for more details on how these new options are used.

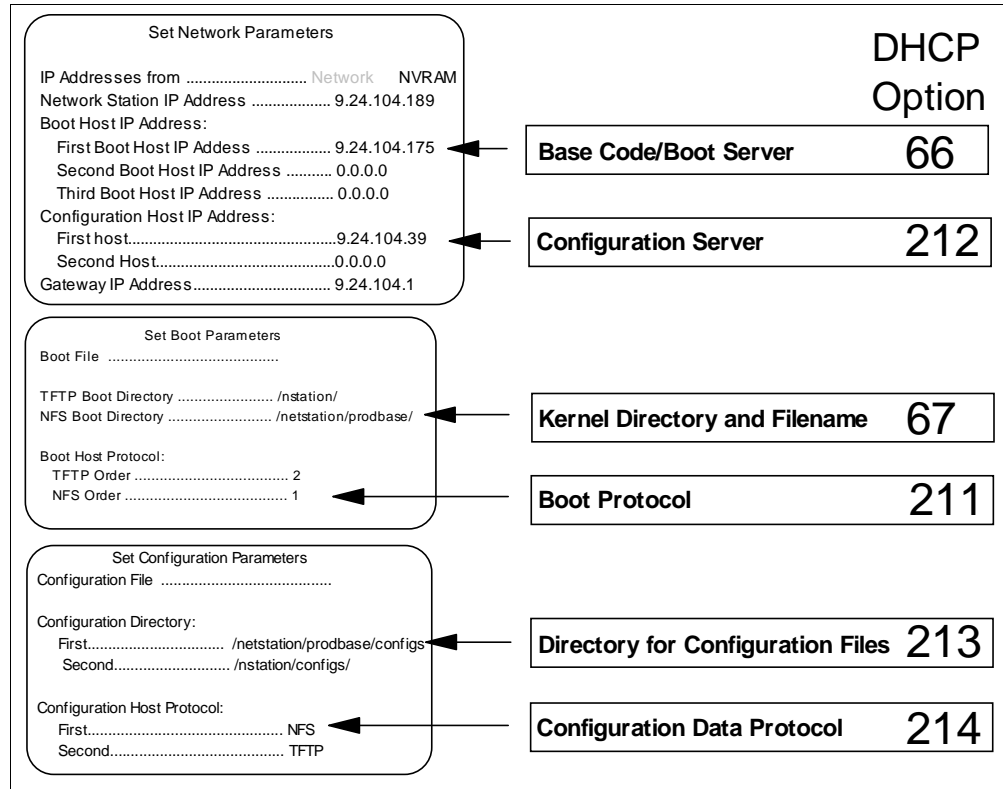


Figure 163. New R3 DHCP Options

## 10.4 How to Configure the DHCP Server

DHCP server configuration consists mainly of defining and identifying clients, grouping them into subnets and classes (a sort of a group) and assigning values to these options that are to be transmitted to the clients. These values can vary greatly for each client, or they can be very similar, dependent on the scope and complexity of the network controlled by a DHCP server.

To access the DHCP server configuration program, click on **Start=>Programs=>eNetwork On-Demand Server=>DHCP Server**, which brings up the panel illustrated in the next figure.

For those who were familiar with the DHCP configuration interface of the last release, the main visual difference is that the Network Hierarchy is displayed at the top of the panel which options are displayed at the bottom instead of having the network on the left and the options on the right. Apart from this visual difference, most of the panels present the same information in a fashion pretty similar to the last version.

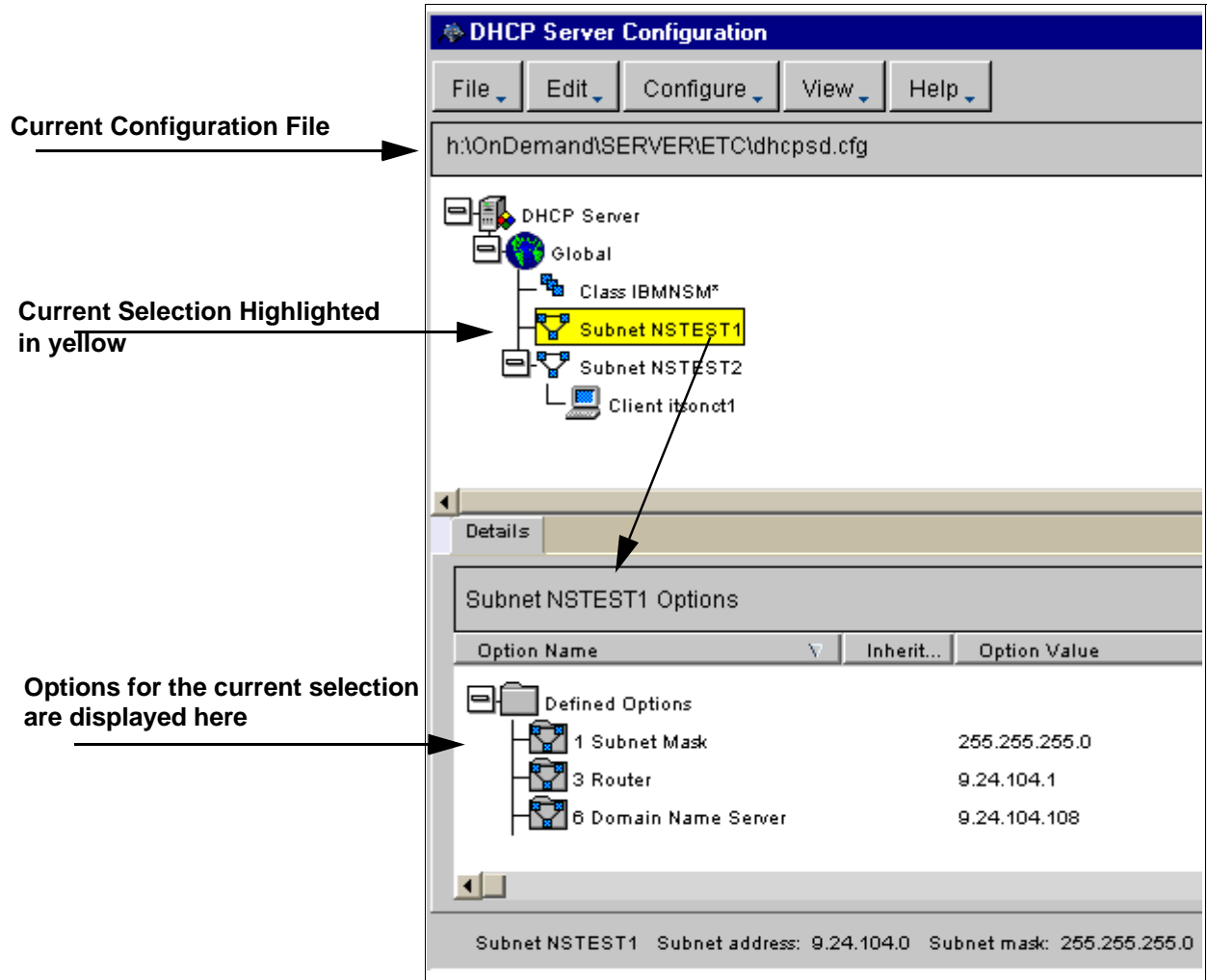


Figure 164. The Main DHCP Configuration Panel

In the figure above, notice the following:

1. The path/name of the configuration file that is being displayed at the moment is shown just below the task bar.

The x:\OnDemand\server\etc\dhcpsd.cfg file is the main configuration file where configuration information regarding the DHCP server and clients is stored.

**Note:** This file can also be manually edited if one prefers not to use the GUI configuration interface, but that process is more error prone than using the interface.

2. The top part of the screen displays a network, in a hierarchical fashion, that represents all of the subnets and clients managed by this server. The network is actually divided into entities and you can think of each of these entities as containers into which we can define options. The entities that can be in this network are:

- Server



Here we define parameters that affect the way the server operates, such as settings for lease periods, logging options, DDNS, and miscellaneous definitions that control the operation of the DHCP server.

- Global

Here we define options that are applicable to all the clients, no matter what subnet or class they belong to.

Defining an option at this level avoids having to repeat the definition in any other container and is therefore more efficient, provided that it applies to all clients.

- Class

A class is sort of a group. Clients can identify themselves as being part of a specific class. (IBM Network Stations have a special class.) Therefore, if a client is part of class, such as IBMNSM\* as defined here, this client inherits the options that are defined in the IBMNSM\* class.

- Subnet

A subnet is a grouping of clients according to a range of addresses. Any options defined here apply to any client which is part of that range of addresses.

- Client

A client is the lowest and most specific definition. A client is identified by its MAC address. Any option defined at the client level applies to that client only. If the same option is defined at both the client level and the subnet level for example, the client level takes precedence and overrides the higher level.

3. When you select any one of these entities its contents are displayed in the lower half of the panel. (Currently, the subnet NSTEST1 is selected, indicated by the yellow square.)

In this case, we see that subnet Test1 contains options 1, 3 and 6, and the current settings (value) of these options appear to the right of these options.

At the very bottom of the panel also appears the name of the subnet, the subnet address and the subnet mask.

What this means is that when a client that is identified as belonging to that subnet contacts the DHCP server, options 1, 3 and 6 that are defined here are part of the options that will be transmitted to this client.

#### 10.4.1 Default DHCP Configuration File

You can modify and save configuration files under different names. However, the operational default file (the file that the DHCP server uses when it starts) remains dhcpd.cfg, located in the OnDemand\server\etc directory.

In the last release, this default configuration file could be changed by entering a configuration file name in the first configuration panel that was presented. In this release, the graphical configuration interface does not seem to have this capability.

Therefore, if you create other configuration files, in addition to dhcpd.cfg, then there are two ways we know of to start the DHCP server:

1. Save the current dhcpd.conf under another name and rename your other configuration file to dhcpd.conf before starting the DHCP server.

**Note:** The DHCP server is an NT service that should normally be started using the **Start=>Settings=>Control Panel=>Services**.

2. Use the command line interface to start the DHCP server, using the following command:

```
dhcpd -e -v filename.conf
```

### 10.4.2 Server Parameters

If you choose to serve addresses to any requesting client, you must configure the DHCP server to respond to unlisted clients.

To do this highlight **DHCP Server** from the DHCP Server Configuration window, then select **Configure** and **Modify selected object**. On the DHCP Server Parameters window, select the **Miscellaneous** tab, which brings up the panel illustrated in the next figure:

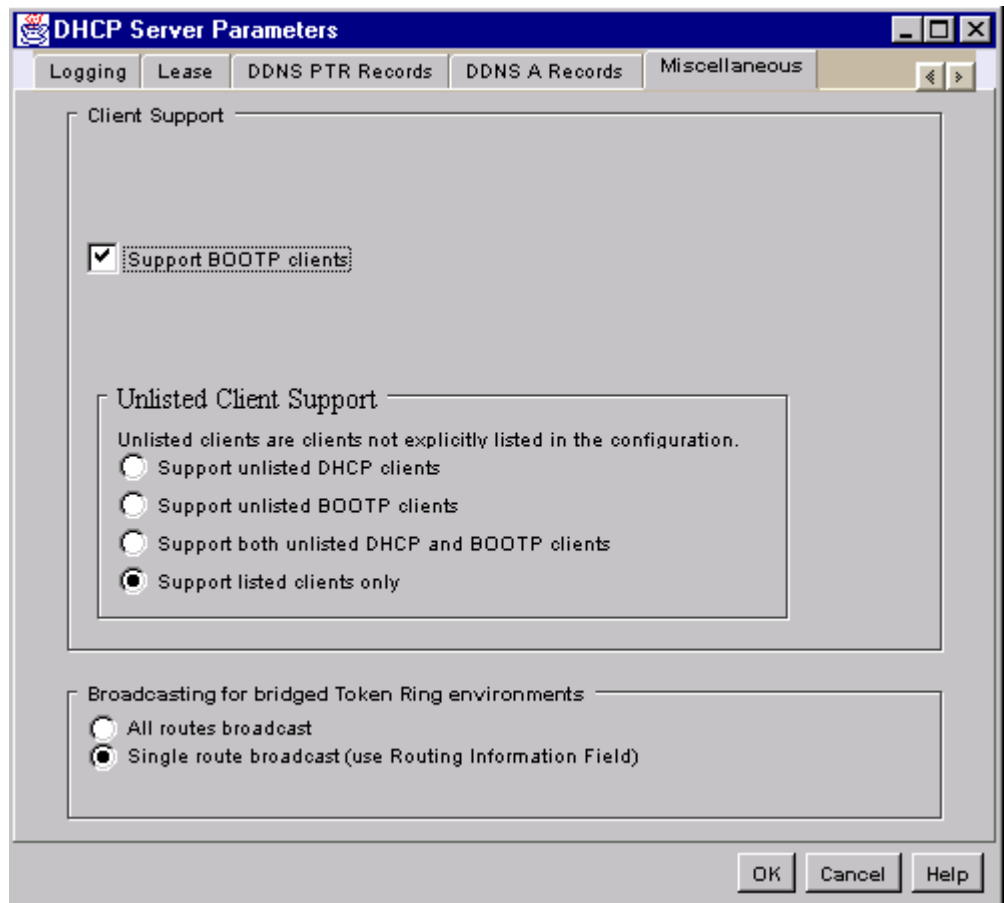


Figure 165. DHCP Server - Miscellaneous Parameters

**Note:** In the panel above, we selected Support listed clients only because we wanted to avoid allocating addresses unless we had specifically defined a client.

To change this to support unlisted clients, check one of the three Support unlisted clients boxes.

### 10.4.3 Global Definitions

To modify the Global options, begin by highlighting **Global** on the DHCP Server Configuration window. From the menu bar select **Configure** and **Modify selected object**. This displays the Global Configuration window. Select the **DHCP Options** tab. Use this screen to define options at the global level. These values will be common to the entire network.

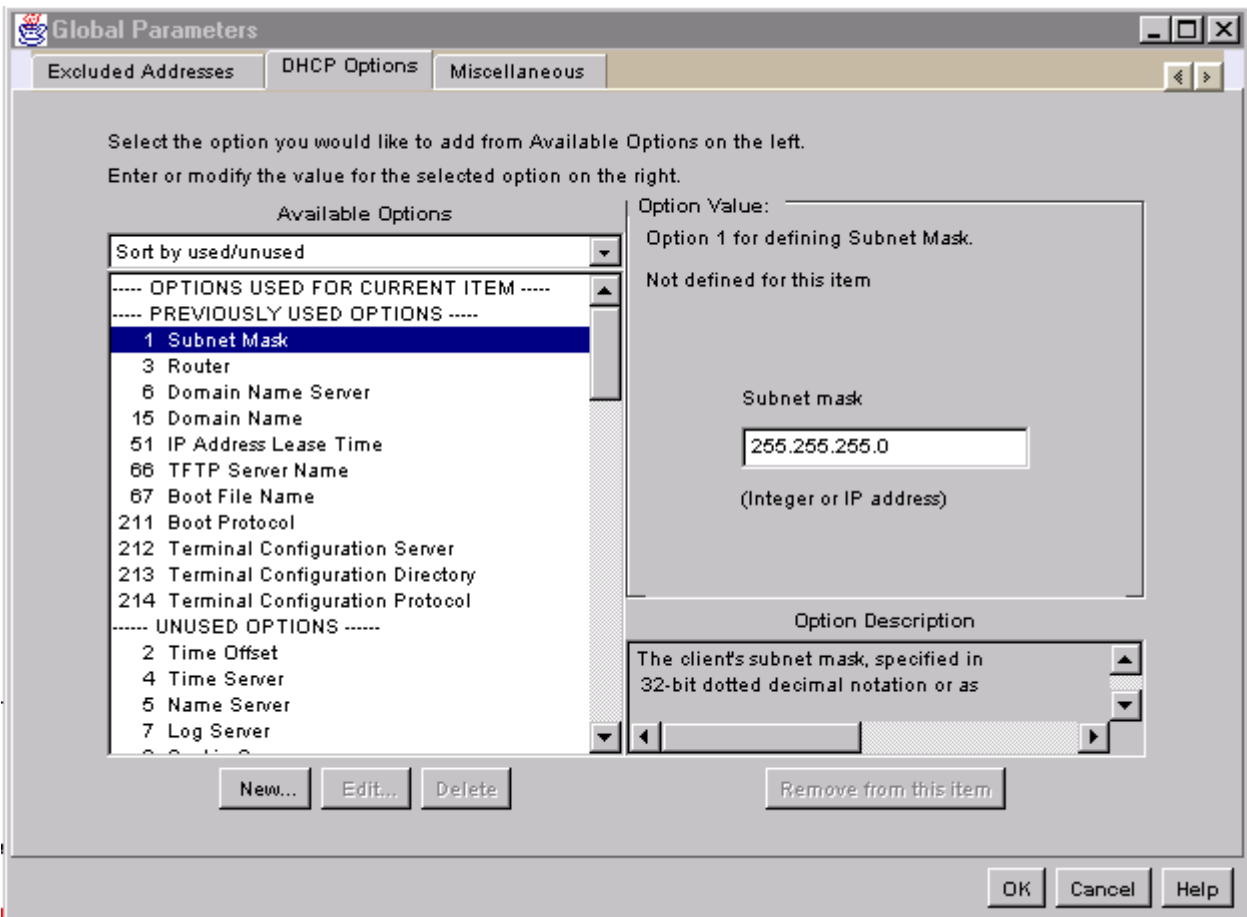


Figure 166. Configuring Global DHCP Options

The DHCP Options window is divided into several sections:

- Available Options

This section on the left side of the panel allows sorting of the options list. The options list has all of the DHCP server's configurable options and each option is associated with a number. The options list can be sorted by used/unused options, by used/unused number, by option number or alphabetically.

- Option Value

This section (top right quadrant) lists the current value of the selected option if it already has a value, or a blank entry field if the option has not yet been configured.

- Option Description

This section (bottom right quadrant) gives a short description of the selected option.

#### 10.4.4 Subnet Definition

Sometimes, you wish to define options at a level other than global. Some options are applicable only to clients within the same subnet.

To modify subnet options, highlight **Subnet** from the configuration panel and select **Configure=>Modify selected object** from the menu bar.

Figure 167. The Subnet Configuration Panel

The Subnet Definition window is divided into three sections:

1. Address Range for Subnet

Here is where you can specify the subnet address, and mask, as well as the range of IP addresses you want to make available within the IP address pool.

2. Addresses Excluded from Range

Use this field to exclude a range of IP addresses. This will prevent the specified addresses from being assigned to a client.

3. Lease Time and Comment

Use this field to set lease characteristics. A lease is the time period during which a client can use an IP address.

#### 10.4.5 Client Definition

A client definition is not required if you only use unlisted clients. The reason for defining a client specifically is a need to identify a particular unit, through its MAC address, in order to either assign specific options to this client or to assign a specific IP address for example.

A client can be added at either the global level or the subnet level, so with any one of these categories selected, from the menu bar select **Configure=> Add Client** and the panel illustrated below appears:

The screenshot shows the 'Client' configuration window with the 'Client Definition' tab selected. The 'Name' section contains the following fields: 'Client name' with the value 'tsont1', 'Client hardware type' set to '6 IEEE 802 Networks', 'Client ID' with the value '0000E5D4200B', and 'IP Address' with the radio button 'Assign this address' selected and the value '9.24.104.189' entered. The 'Lease time and comment' section has the 'Enter a lease time:' radio button selected, with the lease time set to 0 years, 0 months, 6 days, 0 hours, 20 minutes, and 0 seconds. A 'Comment:' text area is located below the lease time settings. The window has standard Windows-style controls (minimize, maximize, close) in the title bar and 'OK', 'Cancel', and 'Help' buttons at the bottom right.

Figure 168. DHCP Client Configuration Panel

The Client Definition panel is divided into two sections:

- Name
- Lease time and Comment

Use the Name section to define:

- Client name

Used for ease in identifying the network station by name. This name appears on the DHCP Server Configuration main window in the left column and represents your client in the network topology.

- Client hardware type

Use client type 6 for token-ring or Ethernet 802.3 networks.

- Client ID

This is the MAC address of the client.

- IP address

Here you can specify an IP address for the client, or you may choose to assign any address from the address pool.

Use the Lease Time section if you need to specify a lease time at the client level to override the defaults.

### 10.4.6 Class Definitions

A class definition is used when you want to define options that are to be served only to clients that identify themselves as part of that class.

The class is an option sent by the client (option 60 - Class identifier) that allows it to identify itself as part of a special group and therefore possibly receive a pre-determined set of options applicable to that group.

The screenshot shows the 'Class' dialog box with the 'Class Definition' tab selected. The 'Name' section includes a 'Class name' input field and a checked 'Wildcard supported' checkbox. The 'Lease time and comment' section has three radio buttons: 'Default lease time: 24 hours' (selected), 'Enter a lease time:', and 'Permanent lease:'. The 'Enter a lease time' option is accompanied by spin boxes for years, months, days, hours, minutes, and seconds. A 'Comment' text area is located below the lease time options. The dialog box has 'OK', 'Cancel', and 'Help' buttons at the bottom right.

Figure 169. DHCP Class Definition

The DHCP client on an IBM Network Station identifies itself as part of the following classes, dependent on the model:

Table 7. DHCP Classes - IBM Network Station

Type - Model	Description	Class
8361-100	Series 100 - Ethernet - 8 MB	IBMNSM 2.0.0
8361-200	Series 100 - Token-Ring - 8 MB	IBMNSM 2.1.0
8361-110	Series 300 - Ethernet - 16 MB	IBMNSM 1.0.0
8361-210	Series 300 - Token-Ring - 16 MB	IBMNSM 1.1.0
8361-341	Series 300 - Twinax - 1 MB	IBMNSM 3.4.1
8361-A22	Series 1000/32 MB-TRN	IBMNSM A.2.0
8361-A23	Series 1000/64 MB -TRN	IBMNSM A.2.0
8361-A52	Series 1000/32 MB - ETH	IBMNSM A.5.0
8361-A53	Series 1000/64 MB - ETH	IBMNSM A.5.0

See the *IBM Network Station Manager Installation and Use, SC41-0664* for additional details.

## 10.5 DHCP Server Administration

With this release, there is a new DHCP Server Administration graphical interface, which facilitates the management of the DHCP server resources.

The interface is started from **Start=>Programs=>eNetwork On-Demand Server=>DHCP Server Administration**, which displays the panel illustrated in the next figure:

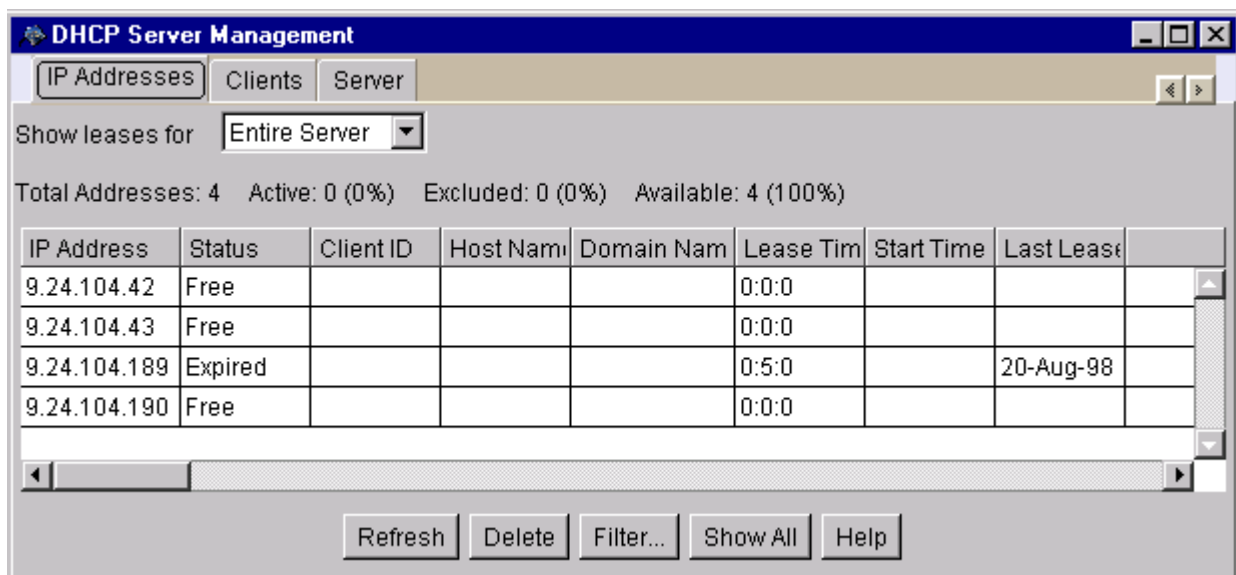


Figure 170. DHCP Server Administration - IP Addresses

The first tab, labeled IP Addresses, gives a quick view of the status of the available addresses, whether free or leased or expired, etc., and information as can be seen in the panel above.

The Filter button brings up another panel that allows you to restrict the number of entries shown based on chosen criteria.

The display can be changed to a per clients view, using the Clients tab, as illustrated below.

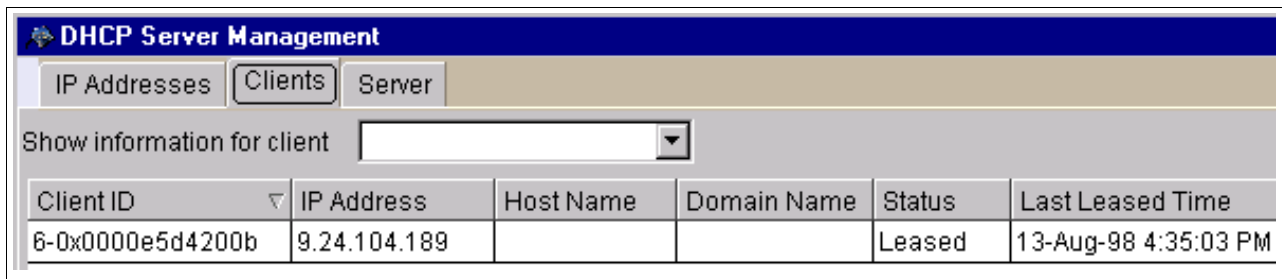


Figure 171. DHCP Server Administration - Clients

The tab labeled Server displays the panel shown in the next figure, which gives a summary of the server activity.

From this panel, the DHCP server can be re-initialized with a simple click on the **Reinitialize Server** button. This causes the server to re-read its configuration file and is normally used after an update to the configuration file that needs to be put into effect immediately.

This used to be done using the `dadmin -i` command, which is still available to perform the same function, although the availability of the GUI interface probably renders it much less useful, except in cases where you might want to use this command in some automated procedure.

To display information about the command syntax, type `dadmin -?` on a command line.

```
C:\>dadmin -i
PLEASE WAIT....Gathering Information From the Server....Please WAIT
Server successfully reinitialized
C:\>
```

Figure 172. The `dadmin -i` Command

Notice the Start/Stop Trace button as well, which dynamically adds the TRACE events to the log file with a simple click.



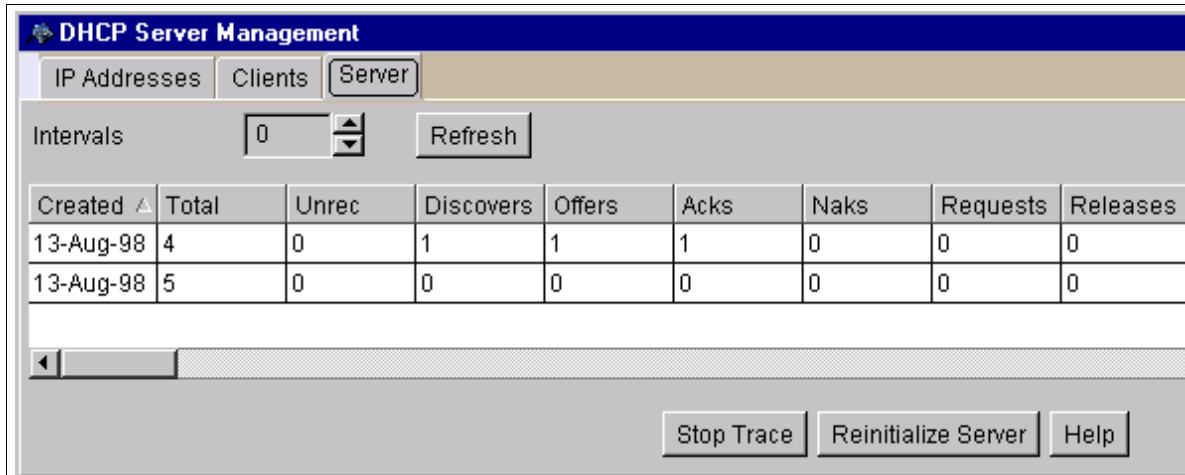


Figure 173. DHCP Server Administration - Server

## 10.6 Online Documentation

The online documentation for the eNetwork On-Demand Server can be accessed through **Start=>Programs=>eNetwork On-Demand Server=>Documentation**.

It is HTML-based and the master file called by this shortcut is located at `x:/OnDemand/SERVER/NsmInst/HTML/OnDemand/en/mtocmst.htm`.

The primary panel displayed is as shown in the figure below:

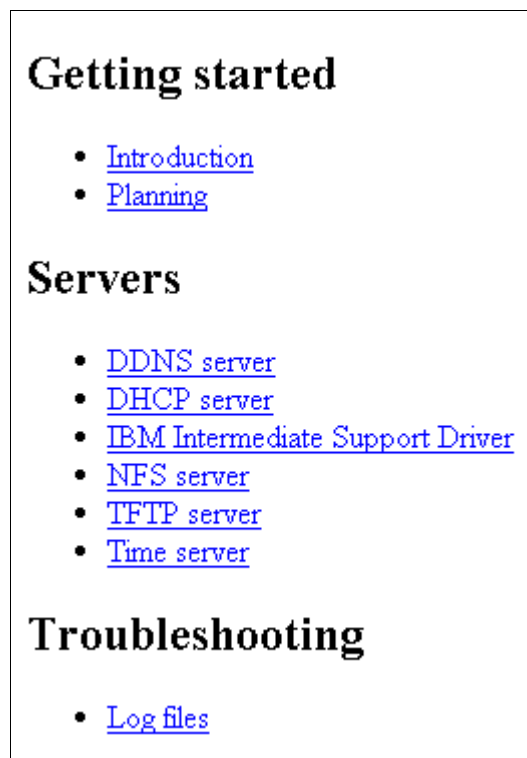


Figure 174. eNetwork On-Demand Server Online HTML Documentation

---

## 10.7 Using DHCP with IBM Network Stations

What are the issues to take into consideration when considering using DHCP with a network of IBM Network Stations?

IBM Network Stations are different from regular PCs in the sense that they do not have permanent IP configuration data, such as IP host names. Configuration data is supplied to the IBM Network Station either through DHCP options or through the configuration files read from a boot server or configuration server, and that brings a few special considerations.

### 10.7.1 Summary

Before we get into detailed explanations, here is a summary of a few important considerations on the use of DHCP with IBM Network Stations:

- Use of multiple DHCP servers is not practical unless they all serve the DHCP options required by IBM Network Stations.

Because an IBM Network Station always selects the first acceptable DHCP offer that it receives, and because it does not have the ability to select the one offer that has the number of options closest to what it is requesting, it is probably not practical to have multiple DHCP servers on the same network where IBM Network Stations are, unless all these servers serve the DHCP options required by the IBM Network Stations.

In other words, it is not practical to have a DHCP server that offers unlisted client support to serve IP addresses dynamically, without any of the required IBM Network Station-related DHCP options, because if that server's offer happens to be the first one received by an IBM Network Station, the station will use it and will not be able to boot since the offer does not contain a boot server address.

- If a DHCP server is used to serve IBM Network Stations, it probably is not practical to use the unlisted client support.

This is because we must retain the capability of assigning an IP host name to a particular IBM Network Station, and this can only be done if we assign the host name as a DHCP option, which then means that we cannot use the unlisted client support to do this.

Each IBM Network Station must be identified with a client definition in order to be able to be served not only an IP address and a boot host address but also an IP host name.

This still allows use of dynamic IP, in the sense that we can still assign a different IP address to a station, as long as we also served a specific host name (option 12) and then use the DDNS facilities to dynamically update the DNS with the proper information.

### 10.7.2 Why Is Using DHCP Better Than NVRAM?

Generally, it is recommended to use DHCP to manage IBM Network Stations because it allows a less costly and better centralized management of these stations and it avoids manual intervention at the physical location of the stations.

As an example, suppose that you want to change the target boot server that the IBM Network Stations are currently using. If you are using the NVRAM method of booting, there are probably two ways to accomplish this:

1. Go to every IBM Network Station and change the NVRAM settings to point to the new server. This is an acceptable way for a network of a few stations but very costly for any significant number of stations.
2. Set up a parameter, such as `set boot-tcpip-desired-server = "x.x.x.x"` in one of the configuration files so that all stations that reboot will be set so that the second time they reboot, they will go to a new server.

This does work but it applies to all the stations and requires a couple of reboots to take effect.

A much simpler way with DHCP is to simply send DHCP option 66 to a station, which causes the station to boot from the server address indicated in option 66.

### 10.7.3 IP Configuration of a Typical PC

On a typical PC, you normally configure, among other things, the following IP data:

- An IP address
- An IP host name
- An IP default domain name
- A domain name server

This configuration data is permanently recorded in the PC's configuration files so that every time the PC is powered up and connected to the network, this configuration data applies.

Possibly, the IP address might be dynamic, in the sense that the PC can be configured not to use a permanently assigned IP address but to request a new address from a DHCP server every time the PC connects to the network.

However, in that case, the same IP host name is kept, the same domain name and the same DNS server are used and a Dynamic DNS is used to ensure that the IP host name gets resolved correctly to the new IP address assigned to the PC.

### 10.7.4 IP Configuration of an IBM Network Station

An IBM Network Station uses the same IP configuration data as a regular PC, except that (some of) this data disappears as soon as the station is powered off, and the data is re-acquired from a DHCP server or a boot server at the next power on.

What this means is that a particular station must be specifically identified by the DHCP server, or the boot server, in order to be able to re-acquire the same configuration data every time.

Where does an IBM Network station gets its IP configuration data from?

- IP address

This is obtained from a DHCP server (or manually entered in the Setup panels if booting from NVRAM).

- IP host name

This is obtained either from a DHCP server (Option 12) or from a DNS server by using the IP address and doing a reverse DNS lookup after obtaining the IP address from the DHCP server.

- Default IP domain name

This is obtained from either a DHCP server (Option 15) or from a configuration server (set tcpip-dns-default-domain="itso.ral.ibm.com" in the hosts.nsm configuration file).

- Domain name server

This is obtained from either a DHCP server (Option 6) or from a configuration server (set tcpip-name-servers= { "9.24.104.108" } in the hosts.nsm configuration file).

In fact, this particular parameter is actually saved in NVRAM and can therefore be used at the next boot even if it is not supplied through DHCP or through a configuration file. However, resetting NVRAM erases this particular value.

Let's take a look at a few cases or examples to understand the behavior of the IBM Network Station.

### 10.7.5 Case 1- Permanent IP Address

If we have a case where a station must have a permanent IP address, for whatever reason (maybe it has a printer attached that is shared by other users and we need a fixed IP address, like a server usually has), then this station must be identified by its MAC address and defined on the DHCP server.

The client record on the DHCP server contains the permanent IP address of the station, and most likely as well the IP host name, domain name and DNS server.

Because this station has a permanent IP address, it is likely that it also has a static definition in a DNS associating this IP address with a host name. In that case, an alternative to supplying the IP host name through HDCEP is to not supply the name and let the station then do a reverse DNS lookup in order to find out its IP host name (assuming the DNS supports reverse address lookup).

**Note:** The behavior of the station, as it concerns setting its IP host name, is as follows:

- If the station does not get an IP host name from the DHCP server, it uses the IP address to do a reverse name lookup on the DNS.
- If there is no DNS specified, it uses the boot server address by default as the DNS address and tries to do a lookup there.
- If the boot server does not provide DNS support and the station is not able to resolve the IP address into a host name, it then uses the decimal IP address notation as the host name.

In other words, an IBM Network Station gets its IP name either by receiving a DHCP option 12 from a DHCP server or by using the IP address received from the DHCP server and doing a reverse address query to a DNS.

In such a case, if we also need to specifically identify this station in the IBM Network Station Manager configuration, we have a choice of using the IP address

of the station as the identifier, or the MAC address or even the IP host name. However, since we have used the MAC address as the identifier for the DHCP server, it would probably be more consistent to use the MAC address here as well.

### **10.7.6 Case 2 - Variable IP Address - Fixed IP Name**

In the case where the station is not required to have a fixed IP address, but still needs to use a fixed IP host name, the DHCP server can assign any IP address from a pool of available IP addresses.

However, since we need the station to conserve a fixed IP host name, then we cannot use the unlisted client support of a DHCP server because we must have a client definition in order to be able to serve each specific client with a specific IP host name.

So, use a client definition to assign a host name, and domain name, and DNS server, but specify that any IP address can be used. In this case, we need the services of a DDNS server so that we can dynamically update the DNS to reflect the fact that a specific host name is now associated with a different IP address.

Again, if we need to specifically identify the stations in IBM Network Station Manager, the MAC address should be used as the identifier because it is the only piece of data that is constant. Using the IP address is not possible in this case since it may change every time the station boots.

**Note 1:** Please see 13.5.1, "Hardware Files Download" on page 234 for a description of how the initial configuration file is sought.

**Note 2:** Use of dynamic IP addresses might not be suitable either if stations use X.11 to connect to a Windows NT Server 4.0, Terminal Server Edition with the UNIX Integration Services product. This is because the UIS licensed connections are defined using IP addresses and the station must have an IP address that corresponds to one of the defined addresses in order to be allowed to connect.

### **10.7.7 Case 3 - Variable IP Address - No Host Name**

In the rare case where an IP host name is not required, then the unlisted client support of a DHCP server can be used, and this is probably a rare case where using unlisted client support applies.

When the IBM Network Station contacts the DHCP server, it is given any IP address. It then tries to do a reverse name lookup to a DNS in order to get the IP host name corresponding to the IP address it is to use. If it happens that it gets a positive response, because that particular IP address happened to have a host name associated with it and defined at one point in time, the host name is used by the unit. Otherwise, the IP address ID decimal dotted notation is used as the host name if none other are available.

In this case again, if we need to specifically identify the stations in IBM Network Station Manager, the MAC address should be used as the identifier because it is the only piece of data that is constant. Using the IP address is not possible in this case since it may change every time the station boots.

### 10.7.8 Using Multiple DHCP Servers

If there are multiple DHCP servers involved, then the following issues are to be considered.

It is not possible to have both a DHCP server that has unlisted client support to serve a population of regular PCs and a DHCP to serve a population of IBM Network Stations.

This is because the DHCP client on the IBM Network Station accepts the first offer that it receives (assuming the offer is acceptable). Therefore, if it happens to accept an offer from the DHCP server that serves IP addresses to PCs, which does not have the options that are applicable to an IBM Network Station, the station will not be able to boot properly.

You could always include in the DHCP configuration file of the server that is meant to serve only PC exclude statements for every MAC address of every IBM Network Station, but this is not a very practical approach.

A better solution would be to make *all* DHCP servers serve both regular PCs and IBM Network Stations. In this case, there are a few ways to proceed:

1. Either have a client definition for every IBM Network Station client so that they are recognized and given a specific IP address and specific options (such as 66 and 67). This is the most likely and practical case.
2. If the stations can be given dynamic IP addresses, you can use a class definition to cause IBM Network Stations to be served DHCP options that are not served to other clients.
3. You could define all options for all clients, and PCs would simply ignore the options that they have no use for, such as 66 or 67, but that are vital to an IBM Network Station in order to boot.

An added advantage of this solution is that you can design the servers so that they back each other up in case of failure of one of them.

Of course, there is probably a myriad of other solutions that can probably be designed as DHCP is very flexible in the ways that it can be set up. We only wanted to point out a few issues that may come up as you start including IBM Network Stations in an existing DHCP environment that may not have been designed initially to serve IBM Network Stations.

## Chapter 11. Dynamic Domain Name Services (DDNS)

Up to now, we have been discussing DHCP without looking into the problems caused by the fact that an IBM Network Station might possibly use a different IP address every time that it boots from a DHCP server.

This situation creates a problem in an environment where there is a static name server that must be updated manually when there is a change in the host name that is associated with an IP address. The solution to this problem is to use a Dynamic Domain Name Server (DDNS) that has the ability to dynamically update the IP address associated with an IP host name.

So, let's examine the problem from the start, in a simplified fashion, for those readers for whom this might be the first exposure to this topic.

### 11.1 What Is a Domain Name Server (DNS)?

A domain name server is a server whose responsibility it is to keep track of host names and IP addresses.

Essentially, it works just like a telephone information service. You can call the phone company and ask for Mary's telephone number, and you get a number back such as 919-123-1234.

A DNS server does the same thing. You call the DNS and ask for Mary's IP address. The DNS looks up its configuration and return Mary's IP address as 9.24.104.199. In this case in fact, you can even do the reverse and ask who 9.24.104.199 is and you get the reply indicating that this number is used by Mary.

This process is illustrated in the next figure in a simplified fashion.

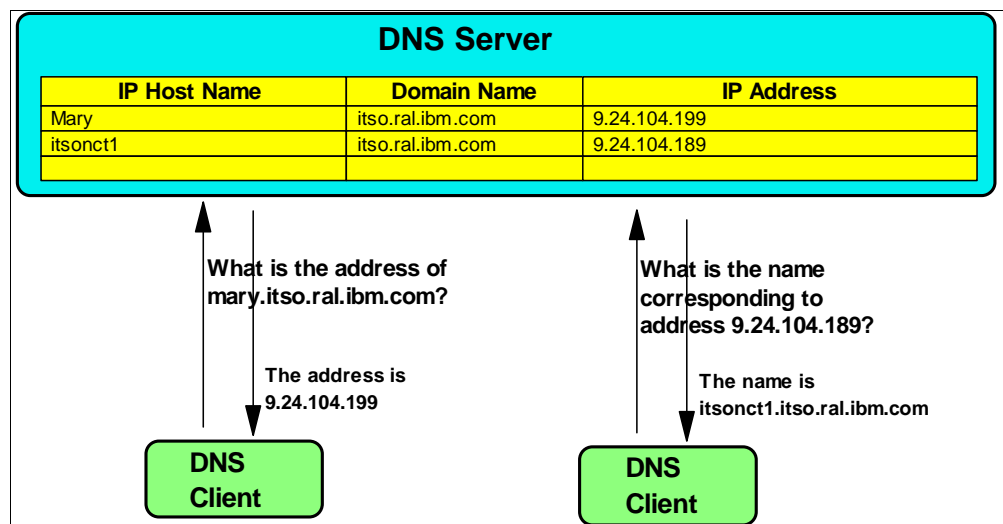


Figure 175. What Is a DNS Server?

---

## 11.2 Why Is a DNS Required?

Actually, we could probably do without a DNS if we had the ability to remember numbers as easily as we can remember names.

The primary reason for using a DNS is that it is very easy for us to remember the name Mary, especially when Mary represents the name of a colleague, than it is for us to remember 9.24.104.189.

Having a DNS therefore allows us to use names when we want to communicate with another machine and let the DNS automatically convert the names into actual IP addresses.

This was initially implemented with a list of names and an associated address (these are called A records, for address records) that had to be manually maintained by an administrator.

If a new employee came in and needed an address for his or her machine, he or she was given a name and an address, and a record was added to the list to reflect this new member. Similarly, if someone left, his or her name was deleted from the list.

---

## 11.3 Why Is a Dynamic DNS Required?

Having an administrator manually update a list of names and addresses might be manageable in a very small environment with a somewhat low rate of change, but it quickly becomes unmanageable in large networks and in networks that have a number of mobile workers who move quickly from one location to another and need to retain the same name, yet have a different address every day or every week, or whatever might be the case.

This is why a facility is required to allow a dynamic update to the list of names and addresses maintained by a domain name server.

This methodology is based on the fact that a machine is usually defined with a fixed name, and that it uses the same name all the time. So, when Joe, a newly hired accountant, is given a machine for his use (a portable laptop because Joe has to move around to the different branch office in the corporation to do his work), it is configured with the name Joe as the IP host name, and it is expected that this name will not change. However, it is expected that this machine will be assigned many different addresses as Joe either moves around the company or simply because the network has been set up such that IP addresses are allocated dynamically even for hosts that do not physically move around.

---

## 11.4 Can There Be Multiple DNS Servers?

Indeed, there are normally multiple DNS servers, and they are organized in a hierarchical fashion, both within a company and outside corporations in the Internet world.

However, dealing with the intricacies of how these DNS servers are organized and structured, and how they communicate with each other is outside the scope of this particular chapter. For additional details on this subject, please refer to



## 11.5 How Does It Work?

The diagram in the next figure illustrates the simplified process of dynamically updating a DNS server.

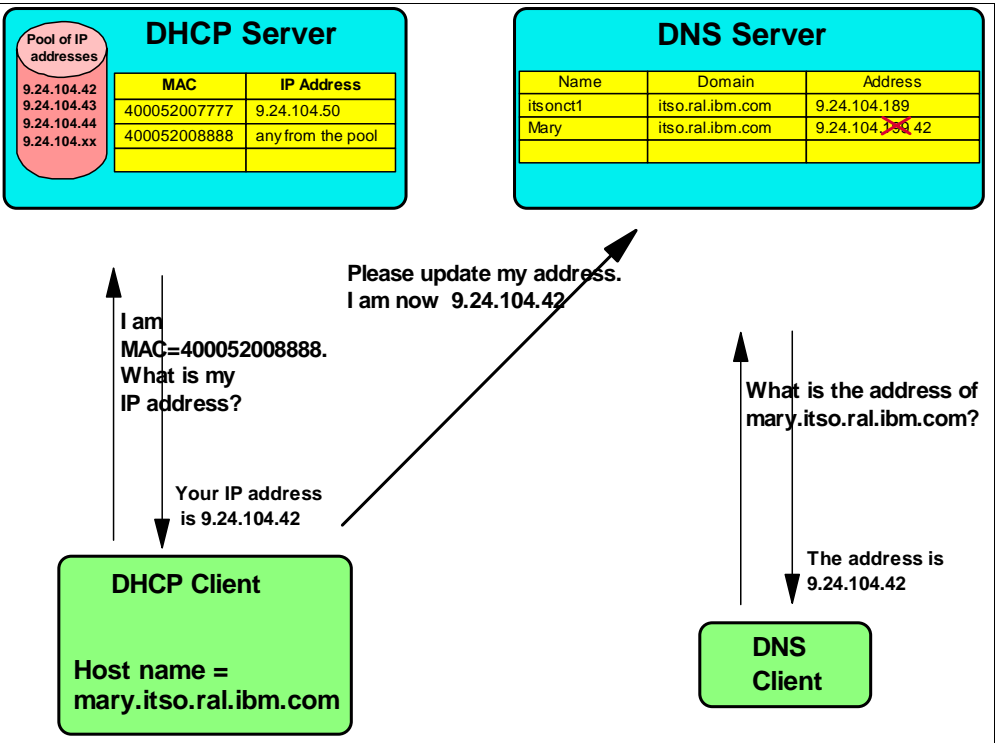


Figure 176. A Dynamic Domain Name Server

In the figure above, the DHCP client on the left has a host name of mary.itso.ral.ibm.com. When it contacts the DHCP server to get an IP address that it can use, it gets a new address of 9.24.104.42 for today to replace the address that it was using yesterday, which was 9.24.104.199 (as an example).

If the record in the DNS server does not get updated, any client asking the DNS server for the address of Mary will get a wrong address (that is, 9.24.104.199). So Mary sends a request to the DNS server to update its address record to show that Mary is now using 9.24.104.42.

As you might suspect, the client must provide the proper authentication to the DNS server in order for this update to be accepted because the server cannot allow anyone to update address records. If you need to read the details on the security aspects, please refer to *Beyond DHCP - IBM's Guide to Network Communications with TCP/IP, SG24-5280*.

Given proper authentication, Mary's address record is updated and any client sending a DNS query to the DNS now gets the updated address of 9.24.104.42.

What if the client cannot update the DNS by itself, which is the case of an IBM Network Station for example? In that case, there is a mechanism by which the client can ask the DHCP server to do the update on its behalf.

In fact, the DNS update can consist of two updates: one for the address record (called an A-record, that is host name = IP address) and one for the reverse of the address, which is called a pointer record (PTR record, that is IP address = host name).

Typically, the DHCP client sends a request to the DDNS server to update its address record and the DHCP server updates the PTR record. However, the DHCP server can also update both the address record and the pointer record on behalf of the client, which is what happens in the case of the IBM Network Station as illustrated in the next figure.

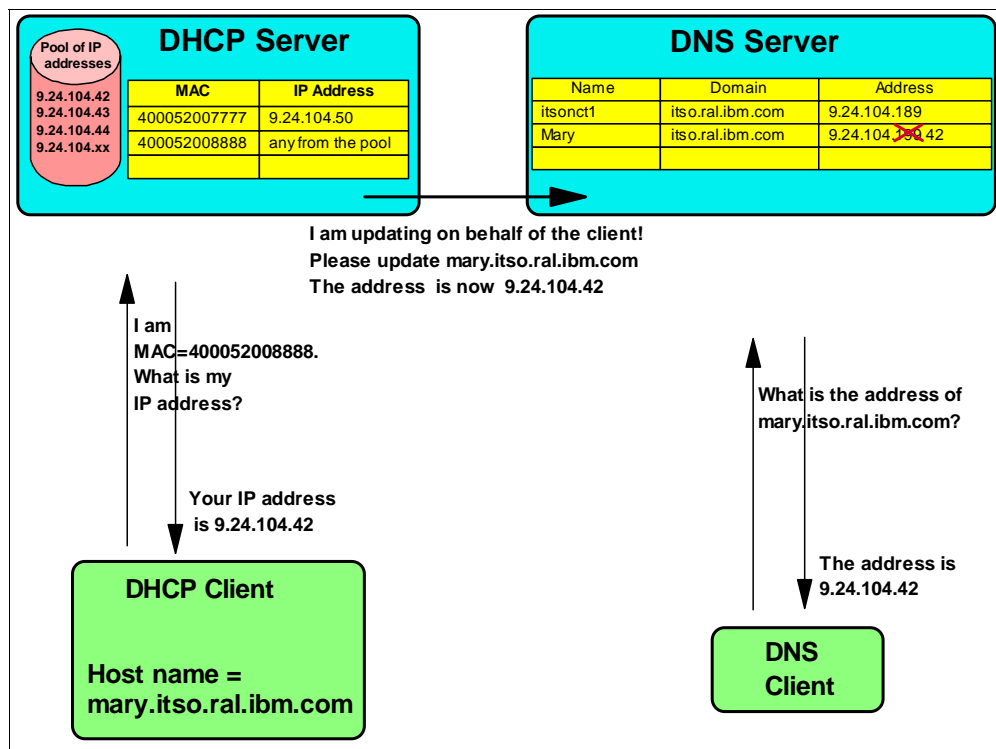


Figure 177. DHCP Server Updating DDNS on Behalf of Client

## 11.6 How to Configure for DDNS?

In this section, we provide a few simple examples of what needs to be configured in order to enable DDNS.

This is mainly for the benefit of those who might not have done this before and who might want to use the easy interface provided by the eNetwork On-Demand Servers on the Windows NT platform to try this out. We therefore outline only a few of the basic configuration steps required to enable use of DDNS.

We create a dummy domain called nsdom2 and just use a few entries to show the workings of a DDNS. We do not tie this DDNS into other DNS servers as would normally be done, because this is outside the scope of this chapter.

### 11.6.1 Configuring the DNS Information on the IBM Network Station

Before we get into configuring DDNS itself, we must take a look at how an IBM Network Station acquires its DNS configuration to start with.

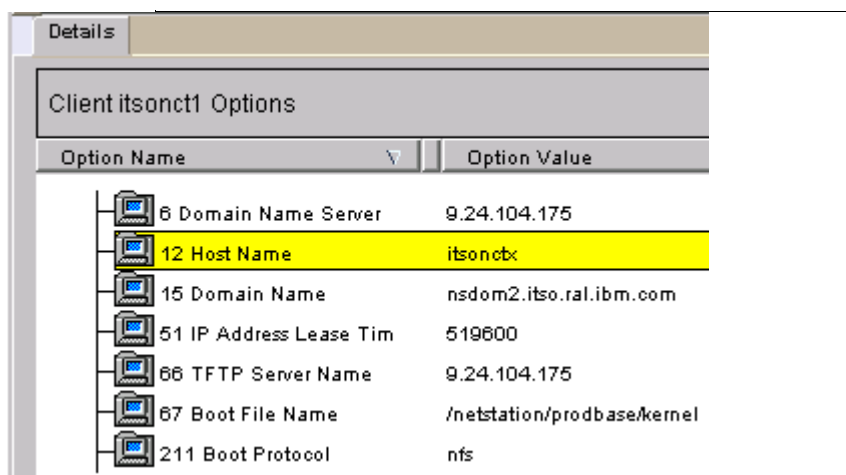
There are two ways that the IBM Network Station can get its domain name server configuration information:

1. From a DHCP server

This method is only applicable of course if the station boots using DHCP.

In that case, the DHCP server must be configured to send DHCP option 6 (domain name server) at a minimum, as well as option 15 (default domain name) and possibly option 12 (host name). This is illustrated in the figure below where we display the DHCP options that are sent to a client we call itsonct1.

This shows that client itsonct1 has a host name of itsonctx, belongs to domain nsdom2.itso.ral.ibm.com and its name server is at address 9.24.104.175 (which happens to be the same as the boot server, but that is really a coincidence in our test network).



Option Name	Option Value
6 Domain Name Server	9.24.104.175
12 Host Name	itsonctx
15 Domain Name	nsdom2.itso.ral.ibm.com
51 IP Address Lease Tim	519600
66 TFTP Server Name	9.24.104.175
67 Boot File Name	/netstation/prodbase/kernel
211 Boot Protocol	nfs

Figure 178. DHCP Configuration - DNS Information

2. From the configuration files loaded at boot time

This method can be used when booting from NVRAM or when using DHCP.

In this case, the information is contained in a configuration file called hosts.nsm which is managed by the IBM Network Station Manager and read by the station at boot time.

**Note:** If this method is used, and at the same time the same options are specified in DHCP options, the DHCP options are overridden by the parameters specified in the hosts.nsm file.

The DNS server information and the default domain name that are coded into the hosts.nsm file are taken from the system on which the IBM Network Station Manager is running.

The figure below shows the sample contents of a hosts.nsm file.

```
#version R3M0
set tcpip-dns-default-domain="itso.ral.ibm.com"
set tcpip-name-servers={
{"9.14.1.30"}
{"9.24.104.108"}
}
set tcpip-name-local-cache={
{"bechard" "9.24.104.175" 0}
{"bechard.itso.ral.ibm.com" "9.24.104.175" 0}
}
```

Figure 179. A Sample hosts.nsm File

**Note:** There are no parameters available to supply the IP host name when using the configuration files. The only way to supply that IP host name is therefore through either DHCP option 12 or by the IBM Network Station doing a reverse name look up on the DNS.

### 11.6.2 Choosing between DHCP or NSM DNS Data

The next question we need to examine is whether the IBM Network Station obtains its DNS configuration data from the DHCP server or from the configuration files served by the boot server?

This choice is determined by the administrator and configured using the IBM Network Station Manager. In the Setup task, select

**Hardware=>Workstation=>System Defaults** and then **Domain Name Server**, which brings up the panel illustrated in the next figure:

<b>Domain Name Server:</b>	
Domain name server to use:	<input checked="" type="radio"/> DNS Configuration from BOOTP or DHCP server <input type="radio"/> DNS Configuration created by Network Station Manager <input type="checkbox"/> Update Network Station Manager DNS file

Figure 180. Domain Name Server Configuration Panel in IBM Network Station Manager

In the panel above:

- Selecting DNS Configuration from the BOOTP or DHCP server causes NSM to erase the hosts.nsm file (if it exists) from the \nstation\prodbase\configs\ directory so that this file does not get loaded into the station at boot time and therefore does not overwrite the DNS values that have been sent by the DHCP server.
- Selecting DNS Configuration created by the Network Station Manager causes the creation of a hosts.nsm file that contains the DNS configuration information as shown in the sample hosts.nsm above. This information overrides any information that might be supplied by a DHCP server and this option *must* be used if you are not using DHCP as a boot method, otherwise the IBM Network Station will not have the required DNS information to operate properly.

Notice the Update Network Station Manager DNS file button. This is used to cause NSM to update the contents of the hosts.nsm file based on the DNS

information of the server on which NSM is running. This is used if you make changes to the DNS information on the server and need to update the NSM configuration file (hosts.nsm) to reflect these changes.

The figure below summarizes these choices.

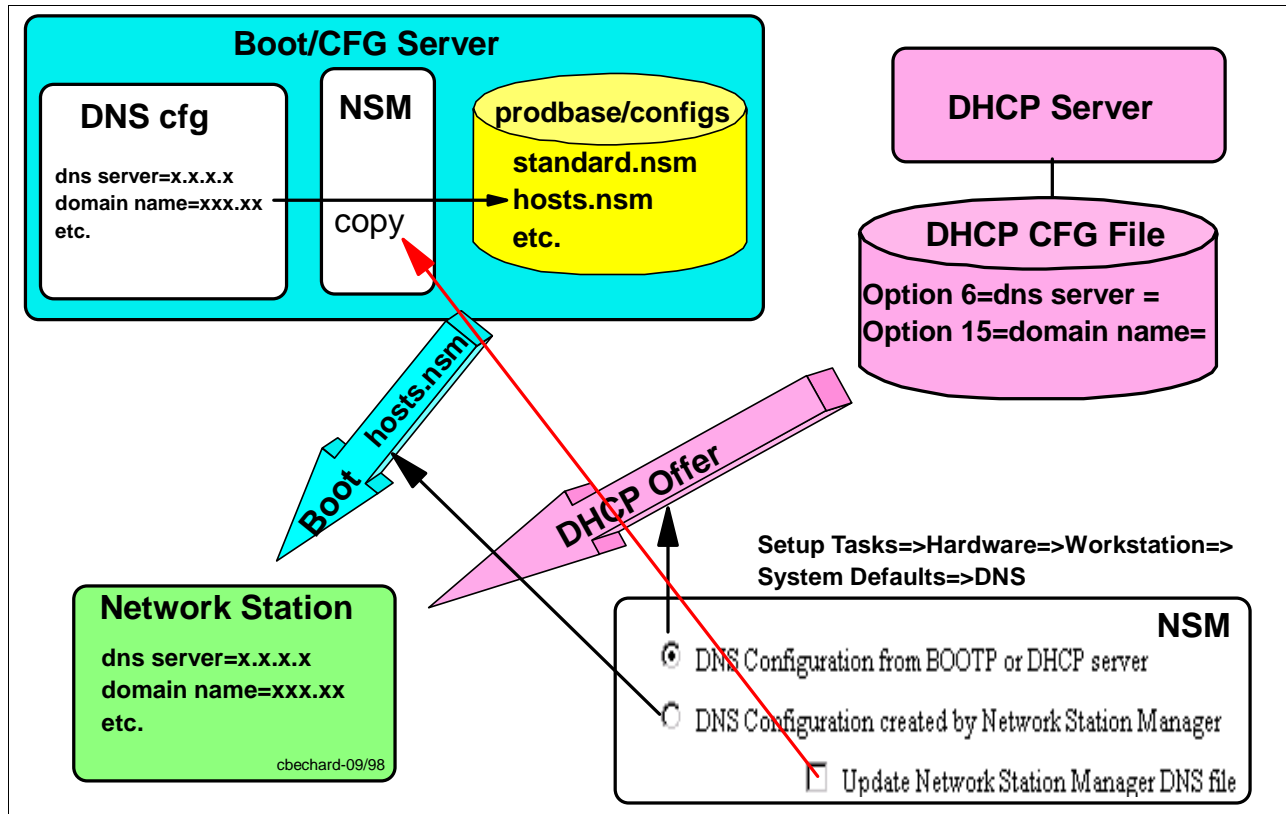


Figure 181. Configuring NDS in NSM

### 11.6.3 Configuring the DHCP Server to Perform DDNS Updates

Now that we have configured the IBM Network Station to use a DNS, we need to configure the DHCP server to update the DNS information on behalf of the IBM Network Station since the station (a DHCP client) cannot do this on its own.

#### 11.6.3.1 Configuring to Update Address Records (A Records)

Using the DHCP Configuration interface, double-click the DHCP server, and select the **DDNS A Records** tab, which we illustrate below:

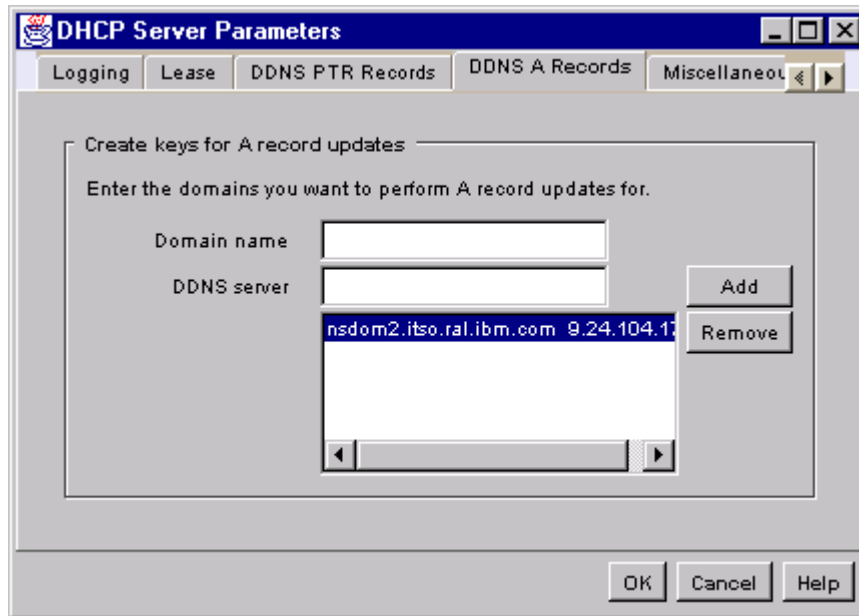


Figure 182. The DDNS A Records Panel on DHCP Server Configuration

In this panel, you enter each domain name for which you want this DHCP server to perform A record updates, and the address of the DDNS server that should receive these updates.

In the example above, we said we wanted updates for the nsdom2.itso.ral.ibm.com domain to be sent to the DNS server at address 9.24.104.175.

This only enables the function. One more step is required to specify whether you want this function to be performed or not. This can be done at either a global level or subnet level. The panel in the next figure shows the enabling of this function at the subnet level by selecting **Always Yes for this item** under the heading of Automatically update DDNS A record on client's behalf if requested? on the Subnet Miscellaneous tab.

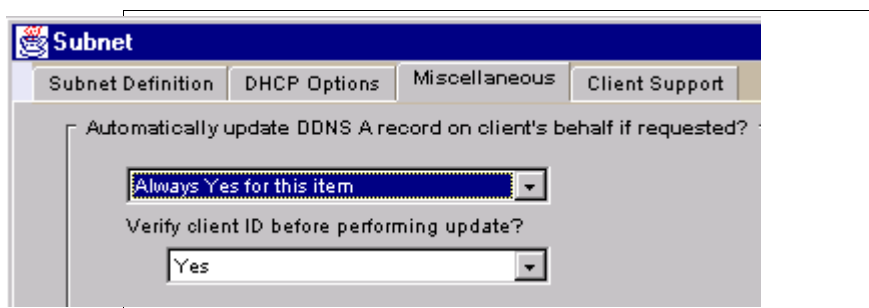


Figure 183. Requesting DDNS A Record Update

### 11.6.3.2 Configuring to Update Pointer Records (PTR Records)

In order to also get an update of the PTR records, which provide an IP address to host name mapping, select the **DDNS PTR Records** tab located to the left of the

DDNS A Records tab on the DHCP Server Parameters panel, which brings up the panel shown in the next figure:

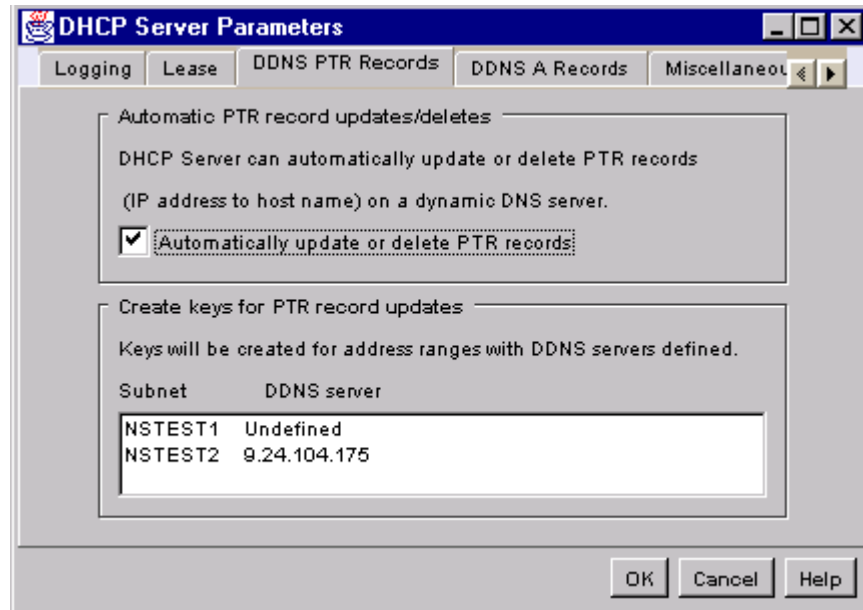


Figure 184. The DDNS PTR Records Panel on DHCP Server Configuration

In this case, place a check mark in the Automatically update or delete PTR records check box. This step enables the update function, but you also need to indicate for which subnet this is desired and which DDNS server is associated with the subnet, as displayed above in the box labeled Create keys for PTR record updates.

The entry labeled NSTEST2 9.24.104.75, appearing in the panel above, is created by specifying entries in the subnet definition panel, under the Miscellaneous tab, as illustrated in the next figure:

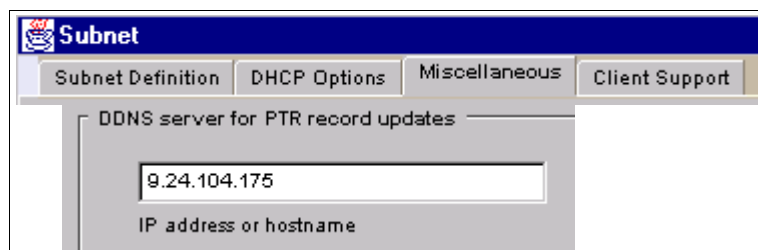


Figure 185. DDNS Server for PTR Record Updates in Subnet Definition

The above entries now enable dynamic updates to be performed by the DHCP server on behalf of the client for PTR records.

When an update is performed, the NSUPDATE window displays the activity taking place. This also gets logged in the NSUPDATE.LOG file.

In the example illustrated in the figure below, we first caused a dynamic update for a host called itsonct1.nsdom2.itso.ral.ibm.com, which appears in the first few

lines. We then changed the name to itsonctx and monitored the second update being done, as is displayed in the last few lines shown below.



```
MS NSUPDATE
-----
InitDDNSUpdate ..... succeeded ...
DDNSUpdate_PTR <Delete *> ...succeeded
DDNSUpdate_PTR <Add itsonct1.nsdom2.itso.ral.ibm.com> ...succeeded
DDNSSignUpdate ...succeeded
DDNSSendUpdate ...succeeded
Posting semaphore
--- NSUPDATE Utility ---
-----
InitDDNSUpdate ..... succeeded ...
DDNSUpdate_HINFO <Delete IBMDDNS-PROXY Ni0weDAwMDB1NWQ0MjAwYg==> ...succeeded
DDNSUpdate_HINFO <Add IBMDDNS-PROXY Ni0weDAwMDB1NWQ0MjAwYg==> ...succeeded
DDNSUpdate_A <Delete *> ...succeeded
DDNSUpdate_A <Add 0xbd681809> ...succeeded
DDNSSignUpdate ...HINFO was checked, rc = 0
succeeded
DDNSSendUpdate ...succeeded
--- NSUPDATE Utility ---
-----
InitDDNSUpdate ..... succeeded ...
DDNSUpdate_PTR <Delete *> ...succeeded
DDNSUpdate_PTR <Add itsonctx.nsdom2.itso.ral.ibm.com> ...succeeded
DDNSSignUpdate ...succeeded
DDNSSendUpdate ...succeeded
```

Figure 186. NSUPDATE Monitor Window

The fact that we kept the same IP address but only changed the IP host name by changing DHCP option 12 is a bit unusual and probably not representative of a real situation (the reverse would normally be done), but we used this mechanism just to cause a change and an update.

## 11.7 The DDNS Server Administrator

Next, we take a look at the DDNS Server Administrator interface, the main panel of which is displayed in the next figure.



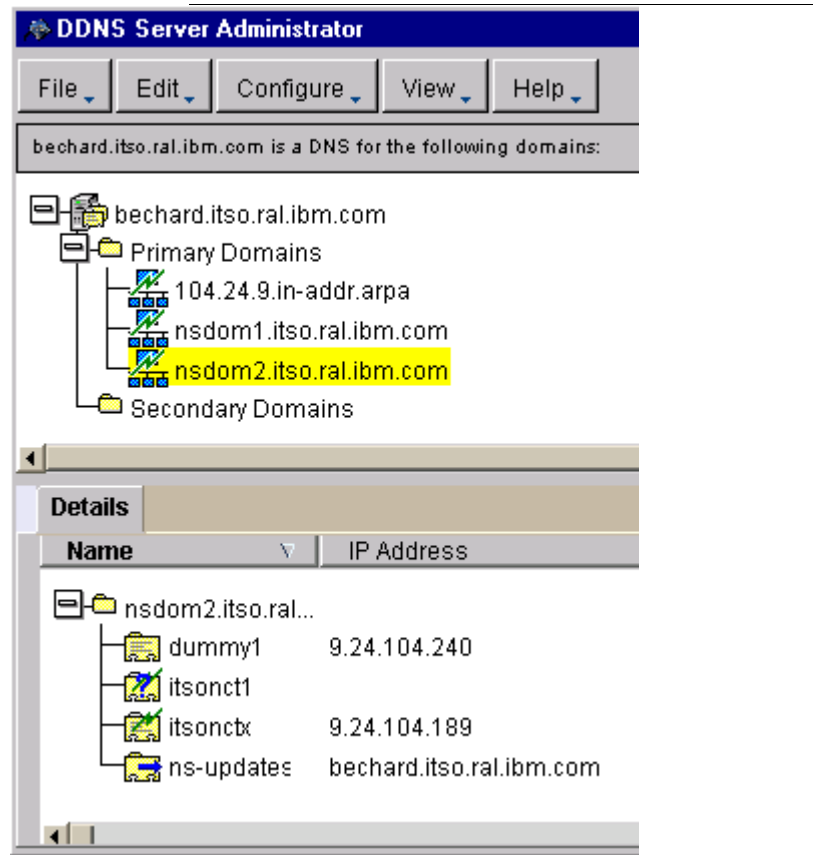


Figure 187. The DDNS Server Administrator Main Panel

First, we added a primary domain, called nsdom2.itso.ral.ibm.com, by selecting **Configure** and then **Add Primary Domain**, and specifying a domain type of dynamic. We also added a second primary dynamic domain called nsdom1.

This generated the two icons displayed as the fourth and fifth lines in the top part of the panel. The lightning bolt in the icon signifies that this is a dynamic domain type (as opposed to static).

The first icon labeled 104.24.9.in-addr.arpa was added automatically to represent the reverse mappings (PTR records).

**Note 1:** The DDNS Server Administrator panel is not refreshed automatically when new records are added through an incoming dynamic update from a client or DHCP server. The GUI also does not have a manual refresh capability. The only way to see entries that have been added dynamically since you started the DDNS Server Administrator is to exit and restart it again. Therefore, if you expected entries to appear because you know an update was just made, and it does not, just restart the Administrator. Manually added entries however do appear immediately.

**Note 2:** Most configuration changes that you make do not require you to stop and restart the DDNS service. Just saving the file is sufficient to make the changes active. Any changes that do require a restart of the DDNS server (the NT service) cause a message to be issued that prompts the user to restart the server.

We then manually added a host entry to the NSDOM2 domain by selecting the **nsdom2** domain, then **Configure** and then **Add Host**. We called this host **dummy1.nsdom2.itso.ral.ibm.com** and assigned the address 9.24.104.240 to that host, just to see an entry appear in the bottom portion of the panel, representing the hosts that are part of this domain.

We then caused our DHCP client **itsonct1** to contact the DHCP server, which caused the DHCP server to send updates to the DDNS server and the entry **itsonct1** to appear in the bottom portion of the panel. Notice that the icon for **itsonct1** has a lightning bolt in it indicating that this is a dynamically created entry whereas the icon for the entry labeled **dummy1** does not, indicating that this is a static entry.

**Note:** In fact, these entries did not appear dynamically; we had to exit the server administrator interface and restart it to have the new dynamically created entries appear. If there is a refresh option, we couldn't find it.

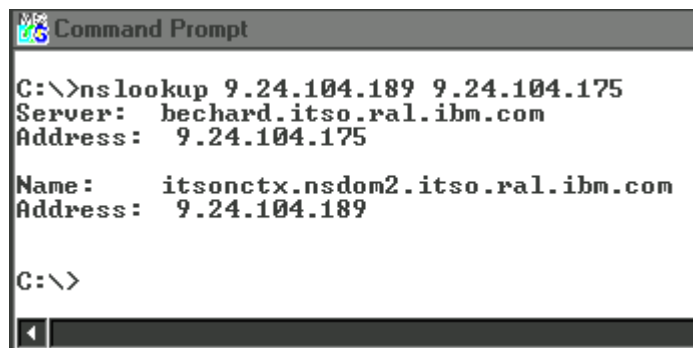
The reason that the panel currently illustrated below does not show any address besides the **itsonct1** entry is that we caused that address to be updated and changed to **itsonctx**, which is shown below with the address 9.24.104.189, and then deleted **itsonct1** because we then had two names pointing to the same address (which is not a problem, since aliases are allowed anyway). The **itsonct1** entry should disappear when garbage collection is done by the server.

If we contact this DNS server to find out the address of **itsonctx**, it should return the 9.24.104.189 address, which we had previously assigned to **itsonct1**.

In fact, we used the NSLOOKUP command to ask the DDNS for the name associated with the 9.24.104.189 address, and it correctly returned the value **itsonctx**, which was the last update we did, as illustrated in the figure below.

Issue NSLOOKUP -? if you are unfamiliar with the parameters of this command.

In this case, 9.24.104.175 represents the target DDNS server to which we are sending this lookup request.



```
C:\>nslookup 9.24.104.189 9.24.104.175
Server:  bechard.itso.ral.ibm.com
Address:  9.24.104.175

Name:    itsonctx.nsdom2.itso.ral.ibm.com
Address:  9.24.104.189

C:\>
```

Figure 188. NSLOOKUP Command Output

If we select the 104.24.9.in-addr.arpa entry, the details of the reverse mapping appear in the Details section of the panel, as shown below:

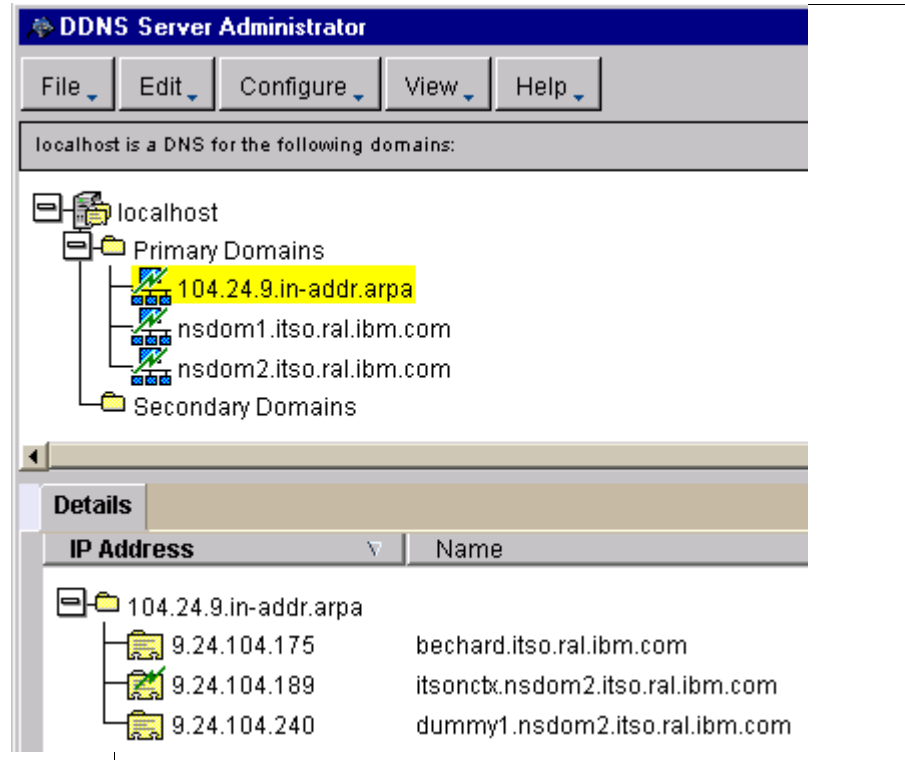


Figure 189. DDNS Server Administration - Reverse Address Details

Of course, there is a lot more to this than we have described here, but our objective was only a quick introductory discussion to get you on your way to understanding DDNS if this is your first exposure.

As mentioned previously, please refer to the online documentation and the *Beyond DHCP - IBM's Guide to Network Communications with TCP/IP*, SG24-5280 redbook for more details.

## 11.8 DDNS Logging/Tracing

DDNS logging is enabled by default after installation.

To change the logging options, double-click on the server icon or name on the main panel and select the **Logging** tab, displayed in the next figure.

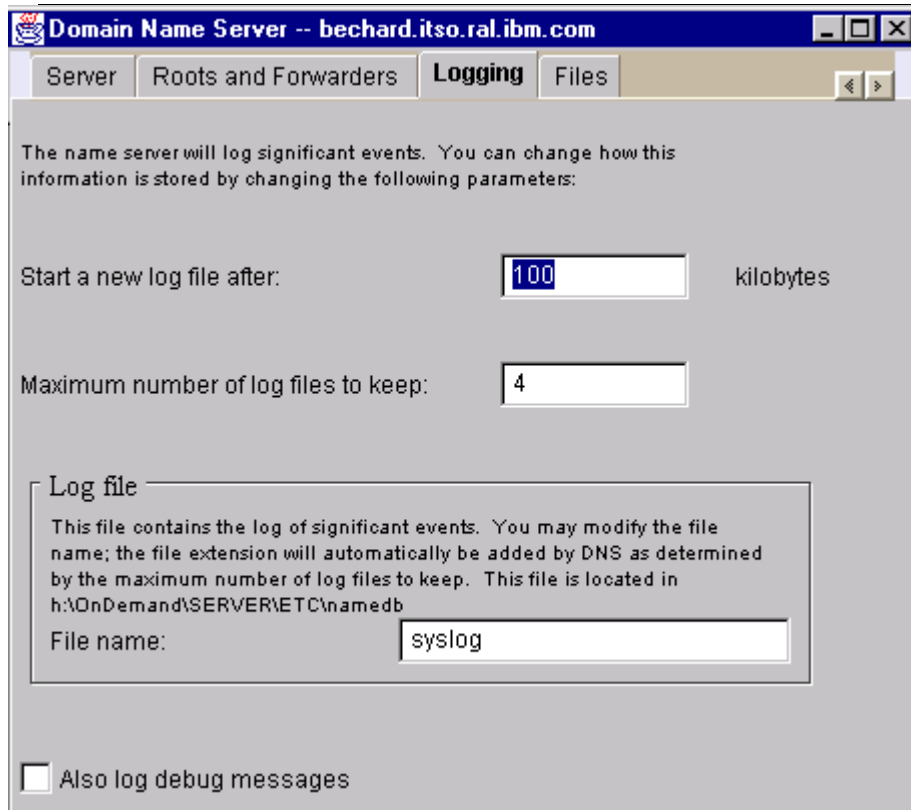


Figure 190. DDNS Logging

The default log file is named syslog and is located in \OnDemand\server\etc\named.

An additional level of details can be specified by selecting the Also log debug messages check box when doing problem determination.

If asked by IBM Service personnel, there is also a trace check box that can be selected. This is accessed by selecting **Properties** on the Edit pull-down on the menu bar, which brings up the panel shown in the next figure. The trace check box is in the bottom left-hand corner of the panel on the General tab.

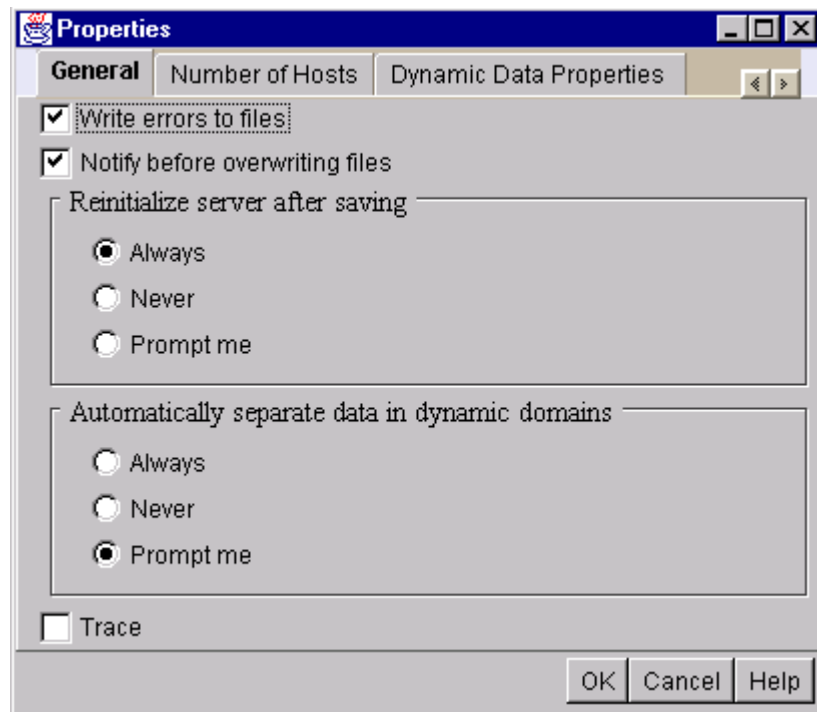


Figure 191. DDNS Trace Enabling



---

## Chapter 12. Full-Screen Solutions

The normal behavior of the IBM Network Station, after the boot process has completed, is to display a login screen for the user to enter a user ID and password.

That login information (user ID and password) is then used to complete the boot process by authenticating the user and by loading additional configuration and preference files based on the identity of the user wishing to use the IBM Network Station.

However, in many cases, we may want an IBM Network Station to behave exactly as a 3270 terminal would for example. In other words, when a user powers up a 3270 terminal, the next thing that he or she sees is a logo or a 3270 application screen only.

Even though the IBM Network Station has the ability to run a 3270 application, the process is normally not as simple as turning the power on, because the user still has to identify himself or herself on the IBM Network Station login screen before he or she can get a 3270 application screen displayed on the IBM Network Station.

Simulating a real 3270 can be accomplished by configuring a special file (kiosks.nsl) that causes the IBM Network Station to operate in what is called kiosk mode.

---

### 12.1 Full-Screen Solutions in Release 2.5

In the previous release (2.5), it was also possible to implement full-screen solutions through proper customization of the configuration files and by-passing or eliminating entirely the login process.

Because the login process was being by-passed, it was necessary to include in the customized files statements that set environment variables normally set by the login process.

Instructions on how to customize the Release 2.5 files for full-screen solutions can be found at the following Web site under Advanced User Information, Full-Screen Solutions:

<http://www.ibm.com/nc/pubs>

---

### 12.2 Full-Screen Solutions in Release 3

In Release 3, full-screen solutions are implemented by suppressing the login panel as opposed to by-passing it, which still allows the login process to proceed in a near normal situation, except for the display of the login panel.

This method allows more flexibility in taking advantage of the functions performed by the login process, such as being able to customize a session, to a certain extent, on a per user basis.

Full-screen solutions are available, in R3, for five different environments:

1. 3270 Emulator
2. 5250 Emulator
3. PC Desktop (Windows Applications)
4. UNIX Common Desktop Environment
5. NC Navigator

Instructions on how to implement these in Release 3 are also found at the following Web site under Advanced User Information, Full-Screen Solutions:

<http://www.ibm.com/nc/pubs>

For that reason, we only present a summary and one example here to illustrate the process. Please refer to the above Web site if you need more details.

### 12.2.1 How Are Full-Screen Solutions Implemented in R3?

In summary, here are the elements of the solution in a Release 3 environment:

1. During the pre-login phase, the presence of a special configuration file called `kiosks.nsl`, which is created by the administrator, triggers the login client on the IBM Network Station to examine the file to see if it should behave in kiosk mode.

**Note:** If you are using a separate boot server and an authentication server, you must ensure that the `defaults.dft` file on the authentication server (or the terminal configuration server if you are using a separate one as well) contains `set exec-startup-commands = { { mcuis } { "actlogin -authserve x.x.x.x" } }` where `x.x.x.x` is the address of the authentication server, so that the `kiosks.nsl` file located in `\nstation\prodbase\configs\` on the authentication server is read. Without this statement in the `defaults.dft`, the authentication server is, by default, the boot server, which does not work since a `defaults.dft` file does not exist there.

Installing the authentication server with the `/as` switch on the `setup.exe` automatically provides you with the correct statement in the `defaults.dft` file. See 2.14, "Authentication Server Special Install" on page 59 and also Chapter 4, "Separation of Servers" on page 101 for details on using separate servers.

2. The presence in the file of a record with the station's own IP address or IP host name causes the station to start behaving in kiosk mode.
3. If there is no record in the file with the station's IP address, the login proceeds normally and a login panel is displayed to the user.
4. If there is a record in the `kiosks.nsl` file with the station's IP address, that record also contains, associated with that address, a user ID and a password. This user ID is called a kiosk user ID, and it is this user ID/password combination that the station uses to do a login to the server instead of displaying a login screen to the user.
5. This special kiosk user ID is created as any other Windows NT user through User Manager for Domains, and it is configured, just like any normal user ID, through the IBM Network Station Manager application, and this allows you to perform customizations on a per user ID basis if required.
6. Note that with a full-screen solution, the user does not have any control over the desktop of the IBM Network Station; therefore, if a problem occurs during the session, the station must be rebooted in order to restart the session.



If the user exits the 3270 session, he or she gets a black screen (assuming the background desktop was set to black) and nothing happens. The only way to restart the 3270 session is to reboot the station.

### 12.2.2 A 3270 Full-Screen Example

Here is an example of the steps required to set up a 3270 full-screen solution:

1. Create a user ID on the NT server to be used as a kiosk user ID.

As an example, let us use the name kiosk1 and password full3270.

2. Add the kiosk user ID to the NSMUser group.

3. Use the IBM Network Station Manager to configure the kiosk1 user:

- Disable the window manager.

Select **Startup=>Environment Variables=>User Defaults** and set RUNWM to NO.

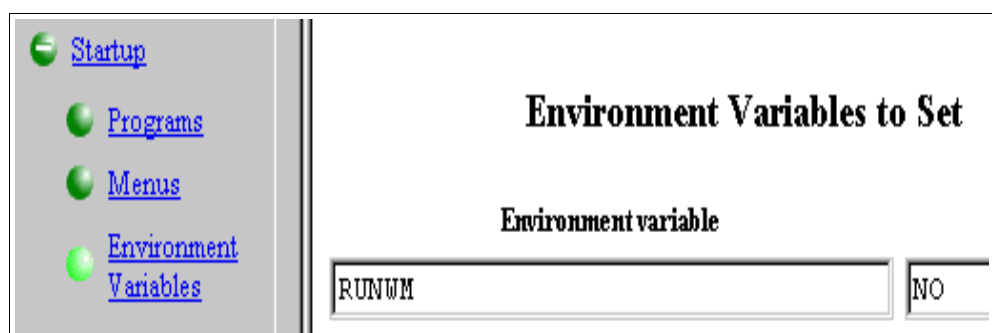


Figure 192. RUNWM Environment Variable

- Remove the menu bar.

Choose **Startup=>Menus=>User Defaults** and select **Standard desktop without menu bar**.

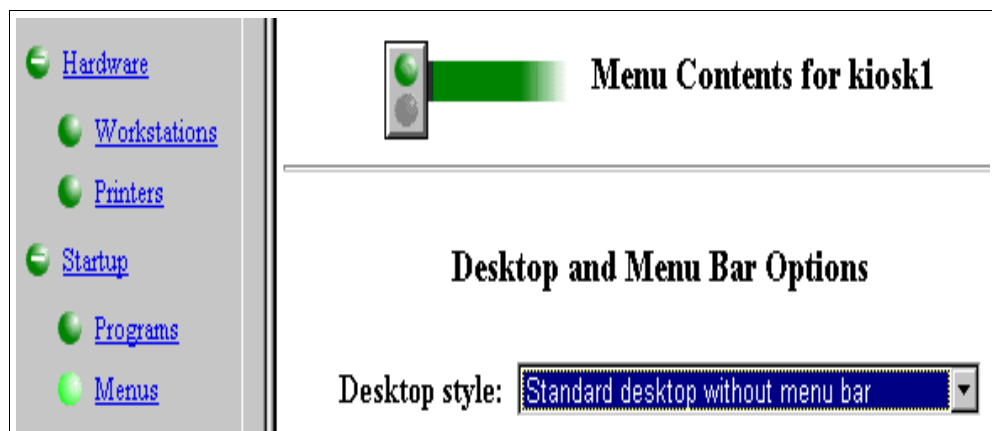


Figure 193. Removing Menu Bar

- Autostart a 3270 session.

Select **Startup=>Programs=>User Defaults=>3270 Sessions to autostart** and:

- Enter the name of the 3270 host.
- Set the width and height to match the monitor resolution of the station.
- Set the vertical and horizontal offsets to zero.

**Custom sessions**

System/390	Session title (optional)	Screen size (rows x columns)	Graphics	Telnet port (blank=default)
<input type="text" value="9.12.14.1"/>	<input type="text" value="PokieA"/>	<input type="text" value="Default"/>	<input type="text" value="Enabled"/>	<input type="text" value=""/>

**Window size and location in pixels (optional)**

Width	Height	Horizontal offset	Vertical offset	Corner to offset
<input type="text" value="1024"/>	<input type="text" value="768"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="Upper left"/>

Figure 194. Autostart a 3270 Session in Kiosk Mode

- Set the background color to black.
- Select **Hardware=>Workstation=>User defaults** and set the desktop background color to black.

**Hardware**  
**Workstations**  
**Printers**  
**Startup**

Desktop background:

☐ Use default

☒ **Black**

☐ Path for XBM file:

Figure 195. Setting Background to Black

4. Create (or add to) a kiosks.source file. You can use any name (other than kiosks.source) you wish for this file.

Edit the kiosks.source file and add the following line, where x.x.x.x is the IP address (or IP host name) of the IBM Network Station:

```
x.x.x.x kiosk1 3270full
```

**Note:** You can use wildcard characters to specify the IP address or host name. See the documentation at <http://www.im.com/nc/pubs> for examples of using wildcards.

5. Execute the nsmkiosk.exe utility in order to encode the kiosks.nsl file.

The utility is located in the ..\nstation\servbase\bin directory. For example:

```
c:\nstation\servbase\bin\nsmkiosk x:\mydir\kiosks.source
```

The nsmkiosk.exe utility encodes the kiosks.source file, names the output kiosks.nsl and stores it in ..\nstation\prodbase\configs.

You are now ready to boot the station that you want to operate in kiosk mode.

### **12.2.3 Security Considerations**

Please be conscious that the kiosks.source file contains the un-encoded passwords of the kiosk user IDs, and that it should therefore be protected adequately from access by anyone but the system administrator.

The encoding program (nsmkiosk.exe) should also be accessible only by the system administrator.

The kiosk user IDs should have limited authority, similar to guest user IDs.

The kiosks.nsl file should be writable only by the system administrator.

If the file system cannot prevent a general user from creating the kiosks.nsl, an empty file should be created and protected by the system administrator.

The unencoded file should not be kept in any subdirectory of \nstation because clients have read access to these directories.



---

## Chapter 13. Configuration Files Structure

The objective of this chapter is to provide you with the information necessary to understand the different types of configuration files, what they contain, how they are used and in what sequence they are read by the IBM Network Station during the initialization process.

This is essential in order to understand how the IBM Network Station works and how to work with the different configuration parameters.

**Note:** Most of the information provided in this chapter has been taken from a presentation and document created by the IBM Network Station Manager development team. This information is also available under Advanced User Information on the Web at:

<http://www.ibm.com/nc/pubs>

We have reproduced it here, not only for your convenience of having all the information at the same place, but also because we used examples specific to Windows NT and we also added additional comments.

Still, we suggest that you reference the Web source as well since it is likely to be more up-to-date as time goes by.

### Attention

Most of the configuration parameters that an administrator must work with in order to set up the proper environment for a network of IBM Network Stations are configurable through the IBM Network Station Manager application.

Therefore, use of the IBM Network Station Manager is the preferred and recommended method to change configuration parameters.

However, in cases where you cannot do otherwise, you can still change some parameters by manually editing some configuration files. If you have to do this, then you should use the back door configuration files that are provided for that purpose because they provide a way of overriding the parameters in the NSM controlled files in a controlled fashion.

If you modify any of the parameters in the configuration files other than the back door files (Type 3 files), you may be seriously jeopardizing your ability to do future migrations because the changes you make will not be migrated automatically.

The information provided in this chapter is intended for advanced users that understand the consequences of directly editing configuration files. Please be aware that these parameters are subject to change at any time, and that the use of the IBM Network Station Manager is intended to shield the user from these changes.

This particular chapter discusses the configuration files as they are used in Release 3 of the IBM Network Station Manager; it is assumed that the reader is already familiar with the configuration files that were available with the previous releases of the IBM Network Station Manager.

If a refresh of knowledge is required, these configuration files were discussed in the previous redbook entitled *IBM Network Station Guide for Windows NT*, SG24-2127, dated March 1998.

Because there is a fairly significant number of parameters and files, it helps to break down the parameters into categories and types, so let's first discuss the types of parameters.

---

## 13.1 Types of Configuration Parameters

As illustrated in the next figure, we can group the configuration parameters into four types or categories:

1. Hardware parameters that pertain to the characteristics of the IBM Network Station itself and attached printers.
2. Application parameters, which have to do mainly with the preferences specific to each of the native applications executing on the IBM Network Station.
3. Startup parameters, that deal with the autostarting of applications, the make up of the menu bar and the settings of environment variables.
4. User and group parameters, for those characteristics that deal with either a specific user or a group of users. The group function is new with Release 3 of the IBM Network Station Manager, but all the other categories were present with the previous releases.

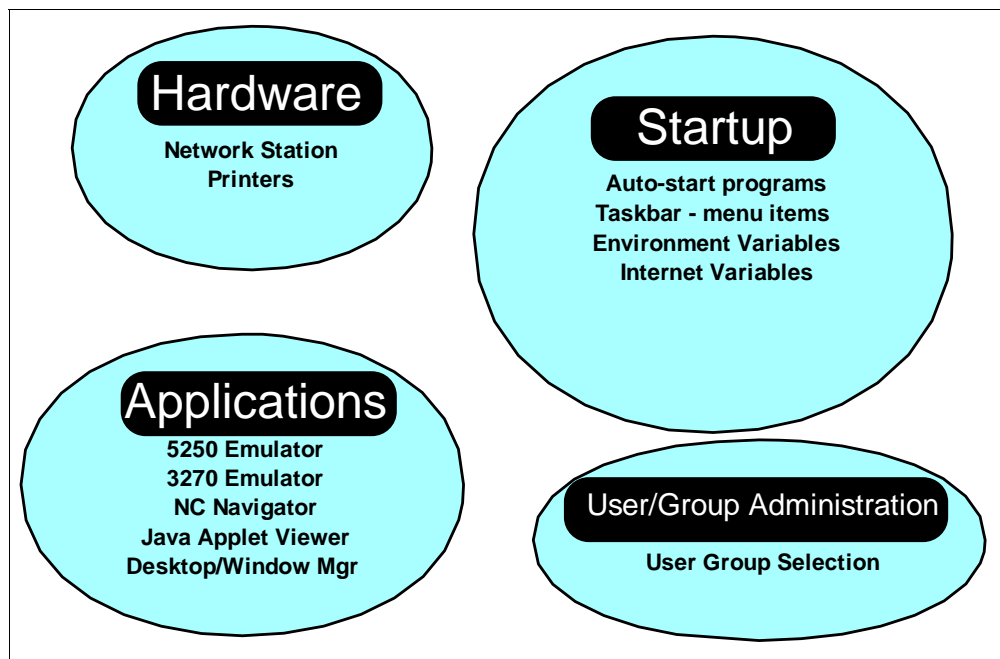


Figure 196. Types of Configuration Parameters

---

## 13.2 Types of Configuration Files

For each of the categories described above, we can now define a type of configuration file, based on whether that configuration file is one that is shipped

with the product, one that contains defaults settings that can be migrated from one release to another, or one that can be manually edited by an administrator.

The types have been arbitrarily defined as follows:

Type	Description
1	Shipped by IBM and replaced by the installation process.
2	Created by NSM and migrated by the installation process.
3	Created by a System Administrator to set parameters not available through NSM. Not replaced or migrated by the installation process.

Figure 197. Configuration File Types

In order to avoid future migration problems, it is important to understand the distinction between these different file types:

1. Type 1

These files are shipped with the product and they are replaced by the installation process every time you install. Therefore, if any modifications are made manually to these files, they will be lost during the next installation of the product.

2. Type 2

These files are created and modified by the IBM Network Station Manager application whenever the administrator or the user makes configuration changes.

Therefore, the format and content of these files is strictly controlled by the IBM Network Station Manager. This allows the product development team to be fully aware of the contents of these files and therefore to be able to automatically migrate the contents of these files for the next release of the product.

If the content of these files is altered manually, there is no guarantee that these changes can be migrated. It is therefore strongly recommended not to alter these files manually. Other files have been provided for that purpose.

3. Type 3

These files are provided as the approved method to override any of the parameters in the other file types or to specify any parameter that is currently not supported by the IBM Network Station Manager application. These files are also known as *back door files* because they provide a way to override any parameter without altering the system provided files.

When the product is re-installed, or a future release is installed, these files are not replaced by the installation process, thereby protecting custom made changes. However, they are also not migrated since the installation process is not aware of these files, but they can be manually moved to any new system by the administrator.

The next figure illustrates how these different file types work. The most important item to notice in the figure is the arrow labeled *overrides* in the top right-hand corner because it indicates which parameter actually takes precedence when it is specified multiple times in multiple files.

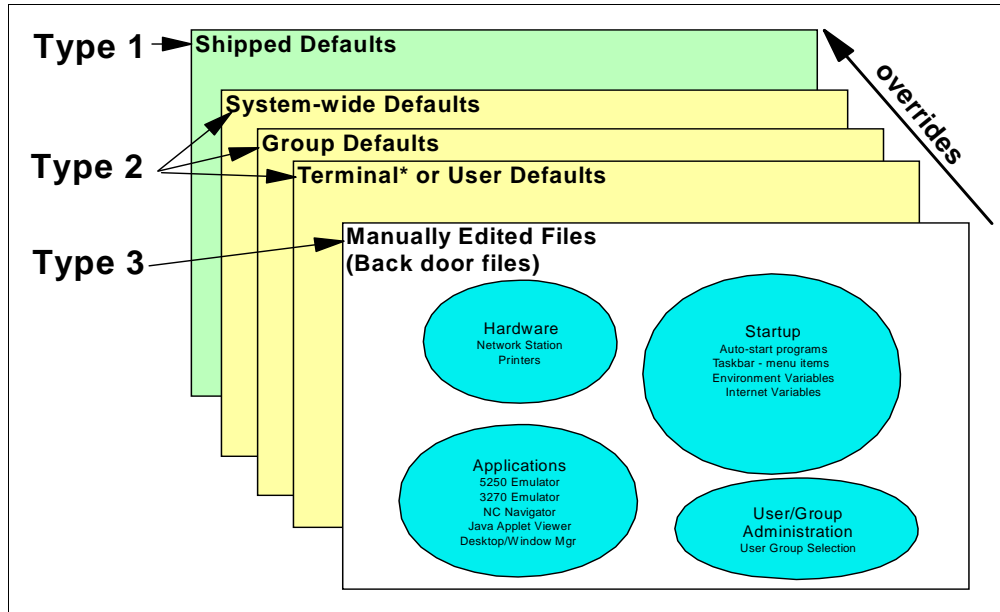


Figure 198. Configuration File Types

Let us take a simplistic example to illustrate the process and assume that we want to specify whether the mouse is set for a left-hand user or right-hand user.

- In the default files that are shipped with the product (Type 1), the mouse is set as right-hand.
- In the system defaults however, the administrator has used the IBM Network Station Manager application to change the default setting to a left-hand mouse.
- But, he or she has also configured that for any member of the group called engineers the default is right-hand.
- And finally, for user Mary, he or she has specified a left-hand mouse.

When user Mary the engineer sits down at her IBM Network Station, the files that are read during the boot, initialization and logon processes are read in a pre-determined order as follows: the shipped defaults are read (she now has a right-handed mouse), then the system defaults are read (she now has a left-handed mouse), then the group defaults are read after Mary logs on (she now has a right-handed mouse) and finally the user-specific files for Mary, which gives her a left-handed mouse.

This mouse configuration parameter has therefore been specified in four different locations but the specification in the last file read is the one that overrides all previous specifications of the same parameter.

### 13.3 Configuration Files Directories

The next important consideration, before we discuss the individual configuration files, is the general location of these files, which varies by platform.



Even though we are concerned mainly with the Windows NT platform in this document, it is useful to be aware of the location of these files on other platforms as well.

With Release 3, this has become a lot easier because there are now common reference points that are used to refer to these files. The common points are called PRODBASE and USERBASE, and the tables below indicate, for each platform, the real directories that are represented by these common points.

For example, if we are talking about a file located in prodbase on an AS/400, then its base location would be QIBM/ProdData/NetworkStation/, whereas the same file would be located at /usr/netstation on an AIX system and at ..\nstation\prodbase in Windows NT.

<b>Platform</b>	<b>PRODBASE directory</b>
<b>NT</b>	<b>/nstation/prodbase</b>
OS/390	/usr/lpp/tcpip/nstation/standard
OS/400	/QIBM/ProdData/NetworkStation/
AIX	/usr/netstation
VM/ESA	/QIBM/ProdData/NetworkStation/

Figure 199. Prodbase Directories per Platform

Notice that the Windows NT platform is particular in two ways:

1. First because it does use actual directories called prodbase and userbase, which makes it a lot easier to work with these files.
2. Second because its base point for these directories can float. That is, the customer decides where he or she wants to install these directories, and then everything becomes relative to that point.

For example, if the customer decides to install on drive F: in a directory called MYSTATIONS, then the prodbase reference point would be F:\MYSTATIONS\nstation\prodbase.

In releases prior to Release 3, the base was x:\nstation, where x: represents the drive on which the customer installed the network station software.

<b>Platform</b>	<b>USERBASE directory</b>
<b>NT</b>	<b>/nstation/userbase</b>
OS/400	/QIBM/UserData/NetworkStation/
OS/390	/etc/nstation
OS/400	/QIBM/UserData/NetworkStation/
AIX	/usr/netstation/nsm
VM/ESA	/QIBM/UserData/NetworkStation/

Figure 200. Userbase Directories per Platforms

## 13.4 Configuration Files

In this section, our intent is to list and describe all the configuration files.

First a reminder that most of these configuration files are controlled and managed by the IBM Network Station Manager application and that these files should therefore not be manipulated in any other fashion.

If there is a need to override the parameters in these configuration files, or to add parameters that cannot be configured using the NSM application, then there are special files called back door files available to the administrator for that specific purpose. By proceeding this way, the administrator is assured of retaining the maximum flexibility for the migration of his or her configuration data to future releases of the Network Station software.

In each of the tables that follow, we use the following table headings:

<b>Type</b>	This is 1, 2 or 3 as described above in "Types of Configuration Files" on page 222. Type 1s are shipped default files, Type 2s are NSM managed files and Type 3s are back door files.
<b>Edit</b>	This indicates whether it is recommended to edit the file or not. Only Type 3 files should be manually edited.
<b>File Format</b>	This is either ASCII or Unicode. Most of the files today are still ASCII. In some cases, when these are created by the administrator, he or she may have the choice of one or the other.

### 13.4.1 Hardware Configuration Files

The following groups of files are hardware-related files.

#### 13.4.1.1 Shipped Configuration Files

The following files are always shipped with the product and will therefore replace any existing files by the same name during installation of the product.

None of these files is new with Release 3; they all existed with prior releases and functioned the same way.

These files are located in `..\nstation\prodbase\configs`.

File Name	Type	Edit	File Format	Description Located in <code>..\nstation\prodbase\configs</code>
standard.nsm	1	No	ASCII	This is the master file that controls the other hardware configuration files downloaded by the IBM Network Station. It is simply a pointer file, that points to the other files.
required.nsm	1	No	ASCII	This file contains the settings for the base IBM Network Station functions. These are settings that are not configurable through the IBM Network Station Manager application.
control.nsm	1	No	ASCII	This file contains the default settings in the IBM Network Station Manager program.

Figure 201. Shipped Hardware Configuration Files

### 13.4.1.2 System-Wide Defaults Configuration Files

The first two files contain the default settings that are applicable to all stations and that are controlled and managed via the NSM.

The last two files are the back door files that can be used in order to override any of the configuration parameters specified in all the previous files or to add parameters that could not be specified via the NSM.

Note that the last file (local.nsm) is specific to AIX only and is migrated to the next installation even though it is a Type 3 file.

Again, all of these files already existed in prior releases, and they are located in `..\nstation\prodbase\configs`.

File Name	Type	Edit	File Format	Description Located in <code>..\nstation\prodbase\configs</code>
hosts.nsm	2	No	ASCII	This file contains the Domain Name Server (DNS) settings that are configured via the IBM Network Station Manager application.
defaults.nsm	2	No	ASCII	This file contains the settings configured via the IBM Network Station Manager application.
defaults.dft	3	Yes	ASCII	This file may be created and edited by administrators.
local.nsm	3	Yes	ASCII	Found on the AIX platform only. This file is created during AIX installation. This file may be edited by administrators and changes are migrated (even though it is a type 3) on the next installation.

Figure 202. System-Wide Defaults Hardware Configuration Files

### 13.4.1.3 Terminal-Specific Configuration Files

These are files that are applicable only to one specific physical terminal. That's why the names of these actual files must be made up of either the IP host name, IP address or MAC address of the terminal. We recommend using the MAC address since this is the only fixed value that you can always count on to represent a specific station.

The first of these files is in fact a pointer file, pointing first to standard.nsm so that all the previous files are processed first, and then to the next two terminal-specific files listed here.

Note that these are optional files, meaning that they do not have to be used. If there are no configuration parameters that are different from the default parameters, then these files actually do not exist. They only get created by the NSM if the administrator configures terminal-specific parameters.

These files also existed with prior releases of the IBM Network Station software; they are located in `..\nstation\prodbase\configs`.

File Name	Type	Edit	File Format	Description Located in <b>..\nstation\prodbase\configs</b>
name	2	No	ASCII	This is the master file that controls the other configuration files called name.nst and name.trm, where <i>name</i> is the TCP/IP host name, IP address (in dotted decimal notation), or MAC address (lower case, no colons) of the IBM Network Station.
name.nst	2	No	ASCII	This file contains the settings that are configured via the IBM Network Station Manager program for the IBM Network Station called <i>name</i> .
name.trm	3	Yes	ASCII	This file is created (empty) by NSM when the two other files above are created and it may be edited by the administrator.

Figure 203. Individual Terminal Hardware Configuration File

#### 13.4.1.4 Group Configuration File

These files are used to specify parameter values that are applicable to a particular group.

These files are new in Release 3. They are located in **..\nstation\userbase\groups\"groupname\"**.

File Name	Type	Edit	File Format	Description Located in <b>..\nstation\userbase\groups\"groupname\"</b>
groupname.nsg	2	No	ASCII	This file contains the settings that are configured via the IBM Network Station Manager program for the IBM Network Station group of users called <i>groupname</i> where <i>groupname</i> is the name of the group of users. New with Release 3.
groupname.grp	3	Yes	ASCII	This file may be edited by administrators. New with Release 3.

Figure 204. Group Hardware Configuration File

#### 13.4.1.5 User Configuration File

Finally, these files are used to specify parameter values that are specific to a particular user.

These files also existed with prior releases. They are located in **..\nstation\userbase\users\"username\"**.

File Name	Type	Edit	File Format	Description Located in <b>..\nstation\userbase\users\"username\"</b>
username.nsu	2	No	ASCII	This file contains the settings that are set through the IBM Network Station Manager program for the IBM Network Station user called <i>username</i> where <i>username</i> is the name of the user.
username.usr	3	Yes	ASCII	This file may be edited by the customer.

Figure 205. User Hardware Configuration File

## 13.4.2 Application Configuration Files

There are quite a few configuration files that are related to the four native applications available on the IBM Network Station.

These application configuration files contain the default settings and preferences for each of the applications. Similar to the hardware configuration files, there are files for the shipped settings, for system-wide settings, group and user settings.

### 13.4.2.1 Product-Owned Configuration Files

These files contain the settings are shipped with the applications. These settings are not configurable through the IBM Network Station Manager.

File Name	Type	Edit	File Format	Description
pref	1	No	ASCII	This file contains the settings for the base NC Navigator browser functions. Location is <code>..\nstation\prodbase\mods\NAV</code> .
resources.nsl	1	No	ASCII	This file contains the settings for the base IBM Network Station Login functions. Location is <code>..\nstation\prodbase\configs</code> .
Login	1	No	Unicode	This file contains the base translated settings for the IBM Network Station Login program. Location is <code>..\nstation\prodbase\nls\locale\MRI</code> .
boot.nsl	1	No	ASCII	This file is used by IBM Network Station Login to indicate the file service protocol to use when communicating with the boot server. Location is <code>..\nstation\prodbase</code> .
nsl.dft	3	Yes	ASCII or Unicode	This file may be created and edited by the administrator. The settings in this file allow the IBM Network Station Login process to be customized. Location is <code>..\nstation\prodbase\configs</code> .
kiosks.nsl	3	Yes	Encoded	This file contains the settings used to suppress the Network Station Login screen. Location is <code>..\nstation\prodbase\configs</code> .

Figure 206. Product-Owned Application Configuration Files

### 13.4.2.2 Shipped Configuration Files

These are the files that contain the settings for the application, as they are shipped. They are located in `..\nstation\prodbase\SysDef\application` where application is either NAV for the NC Navigator, NCDwm for the Window Manager, NS3270 for the 3270 Emulator or NS5250 for the 5250 Emulator.

File Name	Type	Edit	File Format	Description Located in <code>..\nstation\prodbase\SysDef\application</code>
pref (Nav)	1	No	Unicode	This file contains the default settings for the NC Navigator Web browser and it overrides the NC Navigator pref product file.
pref (NCDwm)	1	No	Unicode	This file contains the default settings for the X-window manager.
pref (NS3270)	1	No	Unicode	This file contains the default settings for the 3270 emulator.
pref (NS5250)	1	No	Unicode	This file contains the default settings for the 5250 emulator.

Figure 207. Shipped Application Configuration Files

### 13.4.2.3 System-Wide Configuration Files

These files contain the values, set by the administrator using the IBM Network Station Manager application, which are applicable and the defaults for all stations. These values override the values specified in the shipped configuration files.

Notice that most of these files now are Unicode, and that even the files that can be created and manually edited by the administrator can be Unicode-based.

These files are all located in `..\nstation\userbase\SysDef\"application"` except for the `pref.dft` file, which is located in `..\nstation\userbase\SysDef`.

File Name	Type	Edit	File Format	Description Located in <code>..\nstation\userbase\SysDef</code>
pref (Nav)	2	No	Unicode	This file contains the system-wide settings for the NC Navigator Web browser as configured via the NSM.
pref (NCDwm)	2	No	Unicode	This file contains the system-wide settings for the X-window manager as configured via the NSM. Note that as of Release 3, the Motif Window manager (mwm) is used. Although the directory is NCDwm, it actually contains mwm resources.
pref (NS3270)	2	No	Unicode	This file contains the system-wide settings for the 3270 emulator as configured via the NSM.
pref (NS5250)	2	No	Unicode	This file contains the system-wide settings for the 5250 emulator as configured via the NSM.
pref.dft	3	Yes	ASCII or Unicode	This file may be created and edited by administrators. Settings (X resources) can be added to this file to customize any application except NC Navigator. NOTE: Settings in this file take precedence over NCDwm, NS320, NS5250, NCDterm, and Login pref files at any levels.
pref.dft (Nav)	3	Yes	ASCII or Unicode	This file may be created and edited by administrators. The settings (X resources) in this file allow the NC Navigator browser to be customized.

Figure 208. System-Wide Application Configuration Files

### 13.4.2.4 Group Configuration Files

Similar to the hardware files, these files are used to specify settings that are applicable to users belonging to a specific group, and these settings take precedence over the system-wide settings.

These files are all new with Release 3 of the IBM Network Station software and they are located in `..\nstation\userbase\groups\"groupname\"application"`.

Note that in this case, there is no back door file that can be used by an administrator for the group settings.

File Name	Type	Edit	File Format	Description Located in ..\nstation\userbase\groups\"groupname\"\"application"
pref (Nav)	2	No	Unicode	This file contains the group settings for the NC Navigator browser as configured via the NSM.
pref (NCDwm)	2	No	Unicode	This file contains the group settings for the X-window manager as configured via the NSM. For Release 3, the Motif Window Manager (mwm) is used.
pref (NS3270)	2	No	Unicode	This file contains the group settings for the 3270 emulator as configured via the NSM.
pref (NS5250)	2	No	Unicode	This file contains the group settings for the 5250 emulator as configured via the NSM.

Figure 209. Group Application Configuration Files

#### 13.4.2.5 Individual User Configuration Files

Finally, we discuss the user configuration files to specify settings applicable to a particular user, and these settings take precedence over the group configuration settings.

The files are located in ..\nstation\userbase\users\"username\"\"application".

Again, notice that there is also no back door file for user settings.

File Name	Type	Edit	File Format	Description Located in ..\nstation\userbase\users\"username\"\"application"
pref (Nav)	2	No	Unicode	This file contains the user settings for the NC Navigator browser as configured via the NSM.
pref (NCDwm)	2	No	Unicode	This file contains the user settings for the X-window manager as configured via the NSM. The Motif Window Manager is used in Release 3.
pref (NS3270)	2	No	Unicode	This file contains the user settings for the 3270 emulator as configured via the NSM.
pref (NS5250)	2	No	Unicode	This file contains the user settings for the 5250 emulator as configured via the NSM.
pref (NCDterm)	2	No	ASCII	This file contains changes made to the VTxxx terminal emulator settings by the user on the Network Station. This file is not currently managed by NSM.
pref (Login)	2	No	ASCII	This file contains the Network Station user's last selection on the menu bar for Hide, Top/Bottom, and Lock. This file is not managed by NSM.

Figure 210. Individual User Application Configuration Files

#### 13.4.3 Startup Configuration Files

Startup files are processed after the user has logged on and has been authenticated. They perform three main functions:

1. They build the buttons that appear on the menu bar on the desktop.
2. They automatically start applications that have been configured to autostart.
3. They set environment variables.

Just like all the other configuration files we have seen up to now, there are multiple levels of startup files: a shipped default, files that are applicable to all users, group files and finally user-specific files.

Note that there is a back door startup file available only for the system-wide defaults. There are no back door files for the group and user levels. All these files are Type 2 (managed and controlled by the NSM) except for the first file which is the shipped default.

#### 13.4.3.1 Shipped Startup File

This startup file, as the name implies, is shipped with the product and contains the base default settings for the menu bar buttons, the launching of the X-Window Manager and mandatory environment variables.

These settings apply to all users. This file is located in `..\instation\prodbase\SysDef`.

File Name	Type	Edit	File Format	Description Located in <code>..\instation\prodbase\SysDef</code>
startup.nsm	1	No	Unicode	This file contains the settings for the initial environment variables, which programs are automatically run at login, and what menu bar buttons are displayed.

Figure 211. Shipped Startup Configuration Files

#### 13.4.3.2 System-Wide Startup Files

These startup files contain the parameters that are applicable to all users.

These files are located in `..\instation\userbase\SysDef`.

File Name	Type	Edit	File Format	Description Located in <code>..\instation\userbase\SysDef</code>
startup.nsm	2	No	Unicode	This file contains the settings for system-wide environment variables, indicating which programs are to be automatically started at login, and what buttons are to be displayed on the menu bar.
envvars.nsm	2	No	Unicode	This file contains environment variables substitutions for Language and Select User's Group.
startup.dft	3	Yes	ASCII or Unicode	<b>Note: If this file exists, it is the only startup file that is read; in other words, the other startup files are ignored if this one exists.</b> This file may be created and edited by administrators. It can be used to set environment variables, launch applications, and add menu bar buttons. This file must contain the following five mandatory environment variable statements: SET NSM_NAV_PREF_VERSION R3M0 SET NSM_MWM_PREF_VERSION R3M0 SET NSM_NCDWM_PREF_VERSION R3M0 SET NSM_NS5250_PREF_VERSION R3M0 SET NSM_NS3270_PREF_VERSION R3M0

Figure 212. System-Wide Startup Configuration Files



#### 13.4.3.3 Group Startup Files

These files contain the parameter values that are applicable to a particular group of users. They are located in `..\nstation\userbase\groups\"groupname\"`.

File Name	Type	Edit	File Format	Description Located in <code>..\nstation\userbase\groups\"groupname\"</code>
startup.nsm	2	No	Unicode	This file contains the settings for the group environment variables, indicating which programs are to be automatically started at login, and which buttons are to be displayed on the menu bar.
envvars.nsm	2	No	Unicode	This file contains environment variable substitutions for Language and Select User's Group.

Figure 213. Group Startup Configuration Files

#### 13.4.3.4 Individual User Startup Files

These files are specific to a particular user. They are located in `..\nstation\userbase\users\"username\"`.

File Name	Type	Edit	File Format	Description Located in <code>..\nstation\userbase\users\"username\"</code>
startup.nsm	2	No	Unicode	This file contains the settings for the user environment variables, indicating which programs are to be automatically started at login, and which buttons are to be displayed on the menu bar.
envvars.nsm	2	No	Unicode	This file contains environment variables substitutions for Language and Select User's Group.

Figure 214. Individual User Startup Configuration Files

### 13.5 Configuration Files Download Sequence

A good knowledge of the file download sequence is vital to understand how the IBM Network Station gets configured and ultimately how it behaves.

The sequence in which the files are read is important because when a parameter is set in more than one file, the last setting read by the IBM Network Station determines the final value of the parameter.

In general, the download sequence is designed so that:

- A parameter set in an individual user configuration file overrides (replaces) the same parameter in a group configuration file.
- A parameter set in a group configuration file overrides (replaces) the same parameter in a system-wide configuration file.
- A parameter set in an individual IBM Network Station configuration file overrides (replaces) the same parameter in a system-wide configuration file.
- A parameter set in a system-wide configuration file overrides (replaces) the same parameter in a shipped configuration file.

There are exceptions for parameters that are additive. If the same additive parameter is present in more than one file, all instances of these parameters are aggregated. Examples of additive parameters are:

- Remote printers
- Menu bad buttons
- Programs to autostart

Note that some files may contain statements that cause other files to be read. This is called *sourcing*. Generally, the first statement that causes other files to be read is the first statement in the file.

The major download steps are as described in the following paragraphs. We show here all the files that could exist on a server, but all these files do not necessarily have to exist all the time, as some are optional. For example, the individual network station files, or individual user files, or group files and system-wide files are not mandatory.

1. The login client initializes and performs the pre-authentication tasks.
2. The login client authenticates the user, and then downloads the preference files.
3. The login client then asks the kernel to download the group and user level hardware preference files.
4. The login client processes the startup files.
5. If and when started, the NC Navigator browser downloads its own preference files.

### 13.5.1 Hardware Files Download

After the IBM Network Station is powered on, the following hardware files are downloaded. This is the *pre-login* period. In the list of files below, we only indicate the prodbase or userbase root, understanding that the path is `x:{float}\nstation\prodbase` or `x:{float}\nstation\userbase`, where {float} is any other directory that the user has chosen as the install base.

1. The individual network station `prodbase/configs/"name"` file is downloaded. This is also called the initial file.

This is the master file that contains READ statements for the `standard.nsm`, `"name".nst` and `"name".trm` files. This name can be either the IP host name, the MAC address, the IP address in hex format or the IP address in decimal notation, so the logic is as follows:

1. If name exists where name is the hostname, read it.

**Note 1:** It appears, according to our tests, that the above step only happens if the parameter `set unit-query-for-name-at-boot = tcpip` has been previously set in NVRAM. This causes the station's unit name to be set to a value, which is acquired by using the IP address and doing a reverse DNS lookup to find out the IP host name. The host name is then used as the unit name for the station and the station then uses this name as the name of the first configuration file to look for. If it does find that file, it stops looking.

**Note 2:** If there is more than one configuration server configured, each of these file lookups is attempted on the first server, then the second server, and if none are configured, the boot server is attempted.

2. If name exists where name is the MAC address, read it.
3. If name exists where name is the IP address in hex form, read it.
4. If name exists where name is the IP address, read it.
5. Or else read standard.nsm.
2. The system-wide hardware files are downloaded (apply to all network stations):
  1. prodbase/configs/standard.nsm (This is the master file. It sources the next six files.)
  2. prodbase/configs/required.nsm
  3. prodbase/configs/control.nsm
  4. prodbase/configs/hosts.nsm
  5. prodbase/configs/defaults.nsm
  6. prodbase/configs/defaults.dft (editable)
3. The hardware files associated with an individual Network Station are downloaded.
  1. prodbase/configs/"name".nst
  2. prodbase/configs/"name".trm (editable)

### 13.5.2 Client Initialization (Pre-Authentication)

After the hardware files have been read, the kernel starts the Network Station Login program, which in turn downloads the pre-authentication login configuration files.

The following files are downloaded:

1. prodbase/nls/"locale"/MRI/Login
2. prodbase/boot.nsl
3. prodbase/configs/resources.nsl
4. prodbase/configs/kiosks.nsl (editable/encoded)

This file exists if the administrator has created it to specify that there are terminals that operate in full-screen mode. See Chapter 12, "Full-Screen Solutions" on page 215 for more details.

5. prodbase/configs/nsl.dft (editable)

### 13.5.3 Preference Files (Post-Login)

At this time, the Network Station Login program shows the login screen (or suppresses the display of the login screen if kiosks.nsl indicates that this station is operating in kiosk mode).

After the user has entered a user name and a password (or the user name and password has been taken from the kiosks.nsl file), the system is now able to download preference files for that particular user, so the login program does the following:

1. Downloads the envvars.nsm files:

- Downloads `userbase/users/"username"/envvars.nsm`. The first line of this file causes the next file to be read.
  - Downloads `userbase/groups/"groupname"/envvars.nsm`. The first line of this file causes the next file to be read.
  - Downloads `userbase/SysDef/envvars.nsm`.
2. Then the application (X-resource) files are downloaded for the window manager for all four levels:
    - `prodbase/SysDef/NCDwm/pref`
    - `userbase/SysDef/NCDwm/pref`
    - `userbase/groups/"groupname"/NCDwm/pref`
    - `userbase/users/"username"/NCDwm/pref`
  3. Then the application (X-resource) files are downloaded for the NS5250 emulator for all four levels:
    - `prodbase/SysDef/NS5250/pref`
    - `userbase/SysDef/NS5250/pref`
    - `userbase/groups/"groupname"/NS5250/pref`
    - `userbase/users/"username"/NS5250/pref`
  4. Then the application (X-resource) files are downloaded for the NS3270 emulator for all four levels:
    - `prodbase/SysDef/NS3270/pref`
    - `userbase/SysDef/NS3270/pref`
    - `userbase/groups/"groupname"/NS3270/pref`
    - `userbase/users/"username"/NS3270/pref`
  5. Then the application (X-resource) files are downloaded for the NCDterm emulator for all four levels:
    - `prodbase/SysDef/NCDterm/Pref`
    - `userbase/SysDef/NCDterm/pref`
    - `userbase/groups/"groupname"/NCDterm/Pref`
    - `userbase/users/"username"/NCDterm/pref`
  6. Then `userbase/SysDef/pref.dft` (editable) is downloaded.
  7. Then `userbase/home/"username"/Login/Pref` is downloaded.
  8. The login program asks the kernel to download the remaining hardware files, that is those that are specific to a group or user (now that the system knows the name of the user and the group it belongs to).
    - `userbase/groups/"groupname"/"groupname".nsg`
    - `userbase/groups/"groupname"/"groupname".grp` (editable)
    - `userbase/users/"username"/"username".nsu`
    - `userbase/users/"username"/"username".usr` (editable)

### 13.5.4 Startup Files

The only remaining files to process are the startup files, which determine which programs are to be autostarted and which menu bar buttons are to appear.

If `userbase/SysDef/startup.dft` (editable) exists, it is downloaded, and the other startup files (listed below) are ignored, otherwise, the following files are downloaded:

1. `userbase/users/"username"/startup.nsm`. The first line of this file causes the next file to be read.
2. `userbase/groups/"groupname"/startup.nsm`. The first line of this file causes the next file to be read.
3. `userbase/SysDef/startup.nsm`. The first line of this file causes the next file to be read.
4. `prodbase/SysDef/startup.nsm`.

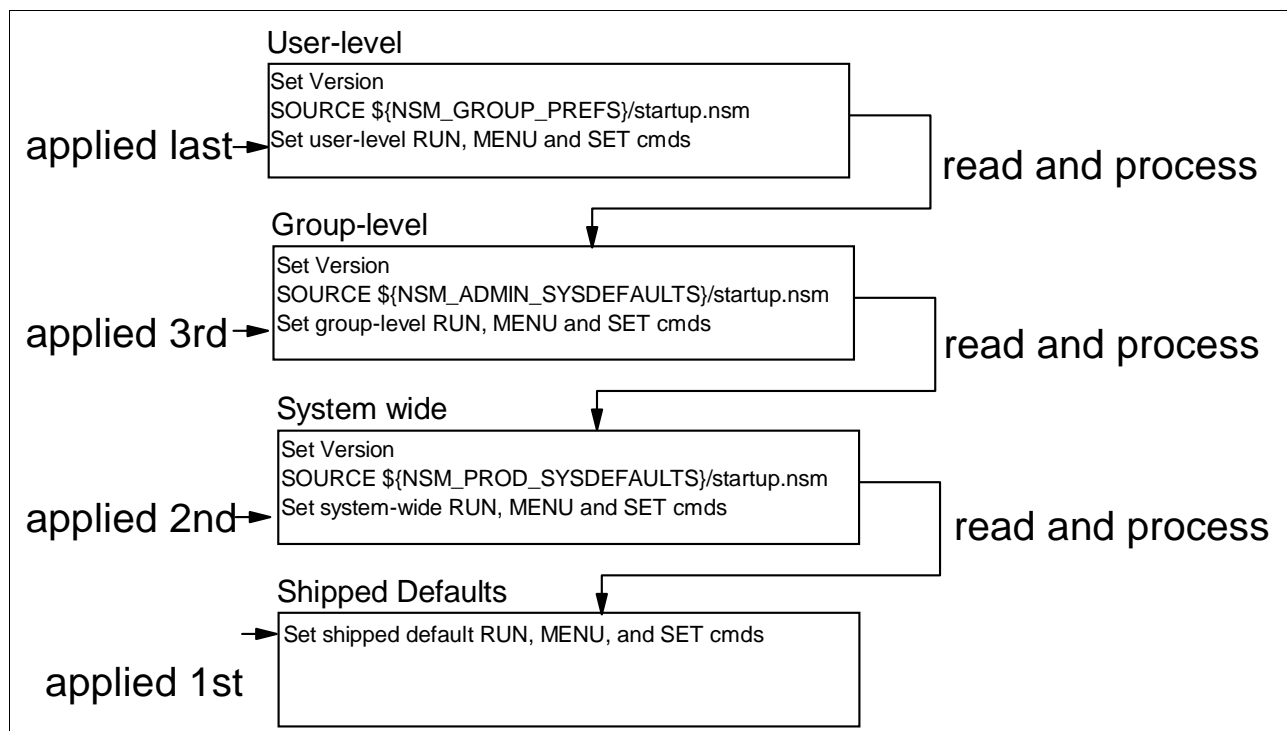


Figure 215. Startup File Sourcing

In the figure above, the `SOURCE` statement causes the named file to be read. The `RUN` and `MENU` commands are added whereas the `SET` commands override the previously set values.

Since all these files are sourced, even though the user-level file is read first, actually, its settings are processed last, as illustrated in the figure above.

In the hardware configuration files such as `standard.nsm`, a `READ` statement is used to provide the same function. In other words, a `SOURCE` statement in a startup file is similar to a `READ` statement in a hardware configuration file and produces the same effect, which is to read the file named on the `READ` or `SOURCE` statement.

Notice here that variables, such as `${NSM_GROUP_PREFS}`, are used on the `SOURCE` statement to point to the appropriate file.

### 13.5.5 NC Navigator Start

When the NC Navigator is started by the user, the following application files are downloaded:

1. `prodbase/mods/NAV/pref`
2. `prodbase/SysDef/NAV/pref`
3. `userbase/SysDef/NAV/pref`
4. `userbase/SysDef/NAV/pref.dft` (editable)
5. `userbase/groups/"groupname"/NAV/pref`
6. `userbase/users/"username"/NAV/pref`

---

## 13.6 User Editable Files - Summary

So which files, out of all the files above, is the user supposed to edit if he or she has a need to customize certain parameters?

These are all the files of Type 3, which we summarize here for your benefit:

Path/File Name	Purpose
<code>prodbase\configs\defaults.dft</code>	For system-wide overrides
<code>prodbase\configs\"name\".trm</code>	For terminal overrides
<code>userbase\groups\'groupname\'.grp</code>	For group overrides
<code>userbase\users\"username\"\"username\".usr</code>	For user overrides
<code>prodbase\configs\nsl.dft</code>	To customize the login process
<code>prodbase\configs\kiosks.nsl</code>	For full-screen solutions
<code>userbase\SysDef\pref.dft</code>	To customize applications
<code>userbase\SysDef\pref.dft(Nav)</code>	To customize NC Navigator
<code>userbase\SysDef\startup.dft</code>	To replace all other startup.nsm files

*Table 8. Summary of Type 3 (User Editable) Files*

---

## Chapter 14. Printing

Our objective in this chapter is to provide you with a brief summary of the information you need to understand the printing facilities that are available on the IBM Network Station.

Only a summary is provided here because we have dedicated a separate redbook on this topic, called *IBM Network Station Printing Guide*, SG24-5212.

The summary we provide here is actually the overview chapter of this separate publication and it should be sufficient to give you an understanding of the printing facilities available, and how to use them. If a more in-depth look is required, please refer to the above publication.

---

### 14.1 History

The IBM Network Station history only goes back to the end of 1996, at which time the IBM Network Station only had what could be called rudimentary print support.

At that time, only the IBM Network Station browser and the local ASCII terminal emulator were able to print to a locally attached printer. Some remote systems, such as a WinCenter server, had the ability to send a print job to the local printer as well by directly accessing the local daemon controlling the serial and parallel ports.

In a second release of the support software at the end of 1997, these capabilities were only marginally improved by the addition of a 5250 emulator which could print to the local printer.

However, it is with the advent of the Release 3 of the software in the summer of 1998 that the printing capabilities of the IBM Network Station were significantly enhanced with the addition of LPR/LPD capabilities.

---

### 14.2 Release 3 Print Support

Release 3 of the IBM Network Station software provides support for the TCP/IP LPR/LPD protocol (RFC 1179), which allows the IBM Network Station to act as either a print client or print server. This includes also LPR/LPD streaming support, which is a draft extension to RFC 1179.

This is summarized in the following diagram:

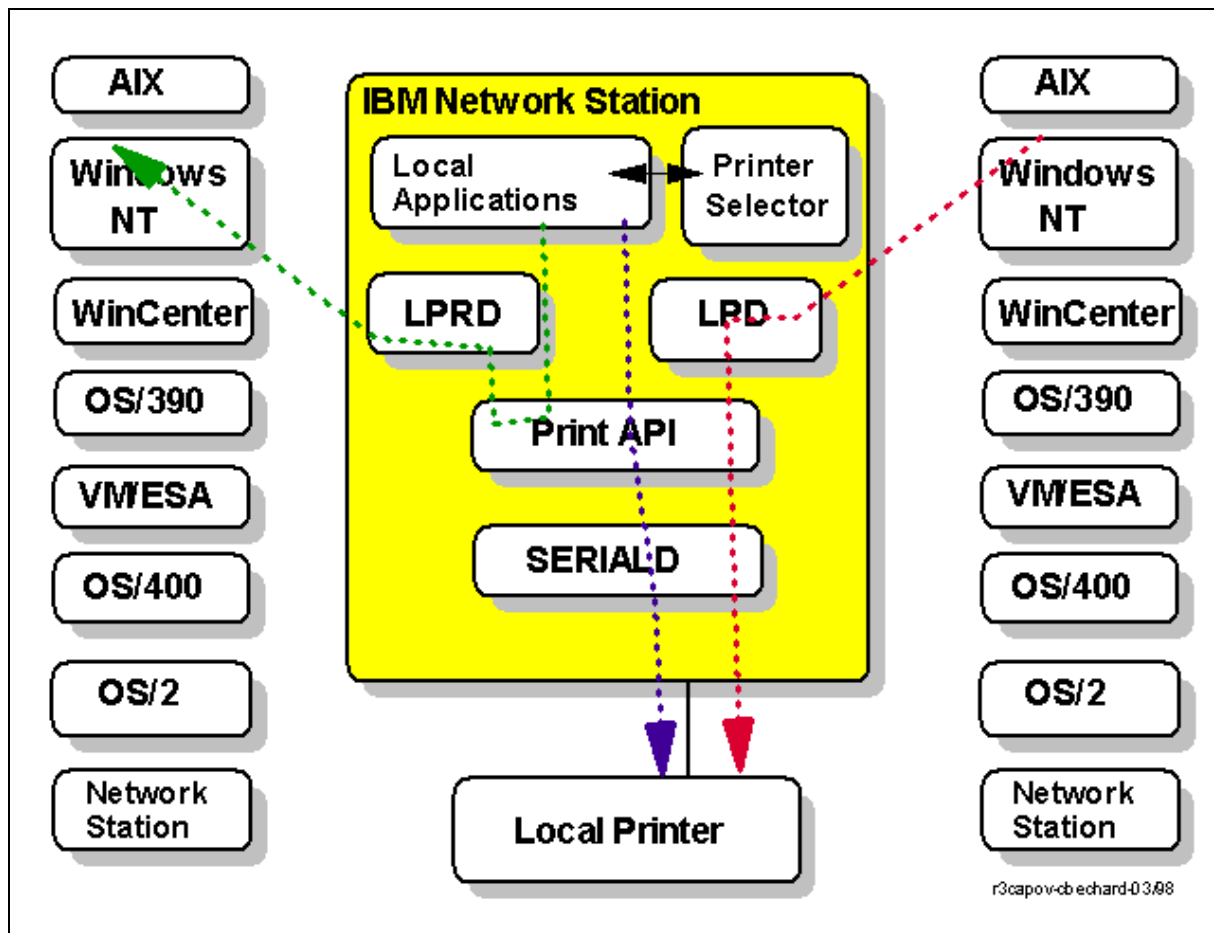


Figure 216. Print Capabilities Overview

The printing capabilities of the IBM Network Station are as follows:

1. LPD capabilities

On the right-hand side of the diagram, we show typical host systems that implement LPR/LPD functionality and that therefore have the ability to send print requests to an LPD server.

The LPD server on the IBM Network Station can receive print requests from any remote system that implements the LPR functionality as described in RFC 1179.

On receipt of these requests, the LPD server routes the print job through the local API and to the module controlling access to the local serial or parallel port where local printers are attached.

Note that the LPD server can reject print requests based on an access control list of hosts with the required authority to use the printing facility on the IBM Network Station.

2. LPR capabilities

On the left-hand side of the diagram, we show typical host systems that implement LPR/LPD functionality and that therefore have the ability to receive print requests from an LPR requester.



The LPRD requester on the IBM Network Station can send print requests to any remote system that implements the LPR functionality as described in RFC 1179.

Note that this LPR requester is labeled LPRD to indicate that it is a daemon. This daemon runs in the background, handling requests from local applications to route print jobs to remote hosts instead of to the local printer(s).

Note that print requests can only come from local applications. Print requests originating on remote hosts, and received by the LPD on the IBM Network Station cannot be routed back to another remote host through the use of the LPRD daemon.

### 3. Printer Selector

In the top right-hand corner of the IBM Network Station, notice the Printer Selector component. This component is called by local applications when the user elects to print data, in order to provide the user with a choice of printers to select from.

The printers listed in the Selector can be either the printers attached locally to the network station or can be printers on remote hosts. Since all print requests from local applications go through the print API, the API routes the request to either the SERIALD component, which handles local printers, or to the LPRD component if the requested printer is a remote printer.

Here are examples of the panels displayed to the user, on the IBM Network Station, when he or she elects to print. The user first gets a Print Dialog panel, such as the one illustrated below, on which he or she gets to choose a few characteristics of the print job such as the number of copies, or paper size. The entries available on this particular dialog panel varies dependent on the application used.

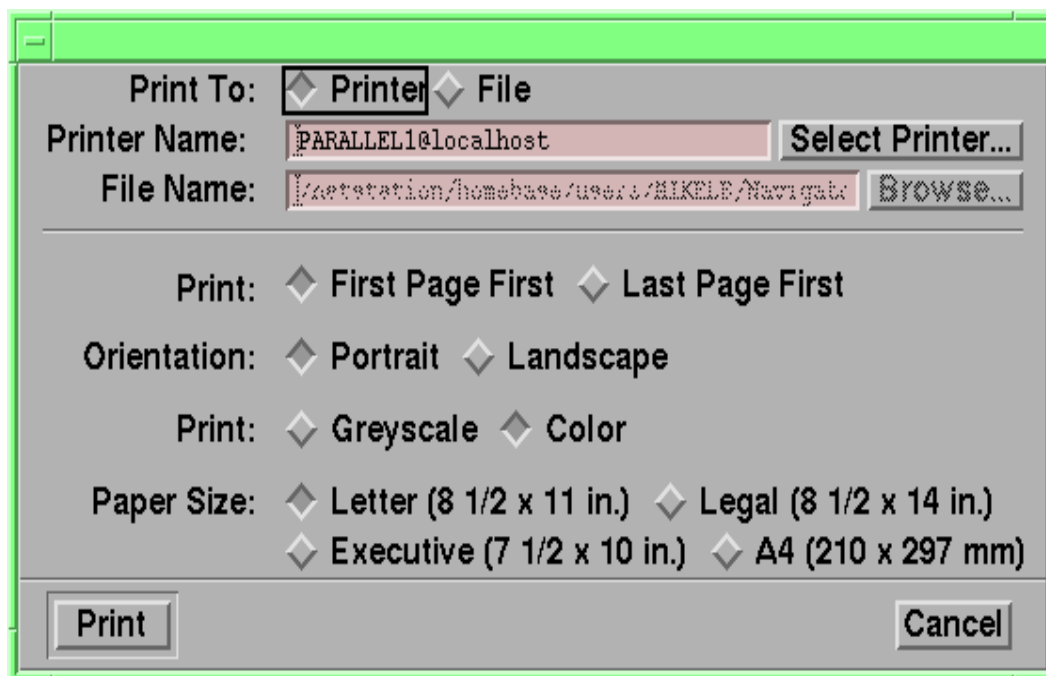


Figure 217. A Sample Print Dialog

If the printer selected by default is not appropriate, and the user wants to make another choice, a click on the **Browse** button or **Select Printer** button brings up the Printer Selector panel, a sample of which appears in the figure below.

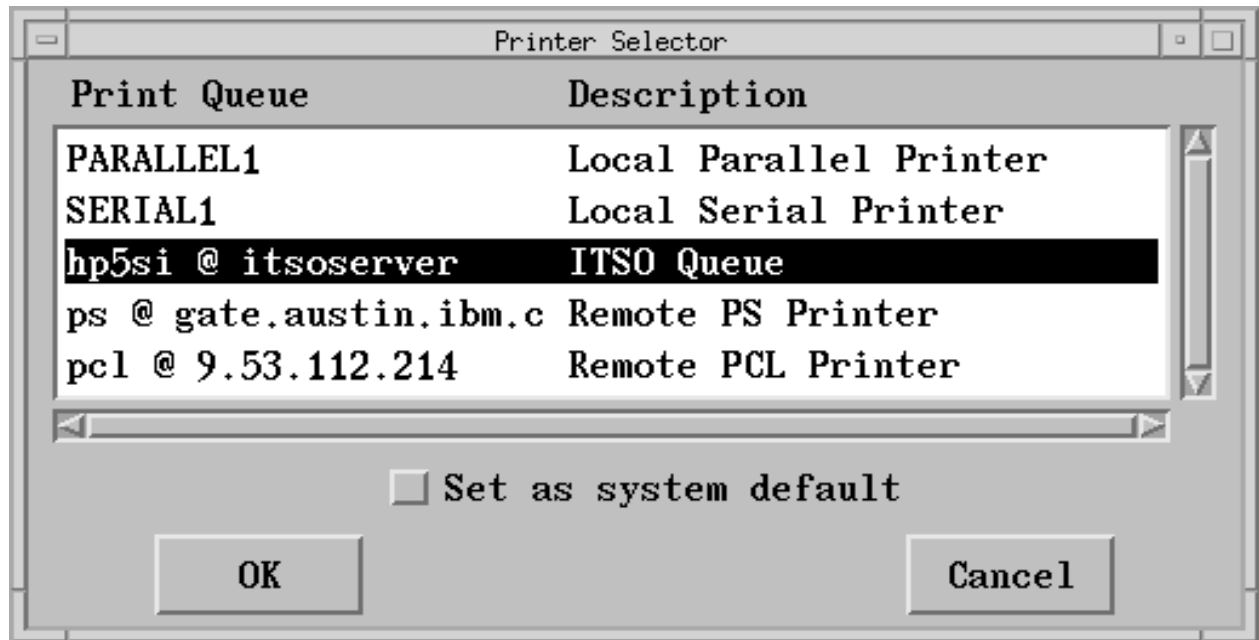


Figure 218. The Printer Selector

This panel looks the same for all applications. Notice that this one shows a local parallel printer, a local serial printer as well as some remote printers, some being PostScript-capable, some being PCL-capable.

The list of printers appearing in this panel is configured by the administrator using the IBM Network Station Manager and are loaded by the IBM Network Station at boot time. Since the administrator has the ability to configure printers for all users, or for certain specific workstations, or for certain groups of users and finally for specific users, this list of printers can be different for every user dependent on who he or she is, on the group he or she belongs to and on the specific IBM Network Station that he or she is using.

4. Local parallel and serial port

Although not shown in the summary diagram of the Release 3 capabilities, the print APIs now allow applications to print to either the local serial port or to the local parallel port, as demonstrated by the entries available in the Print Selector panel.

5. DBCS conversion

Also not shown in the diagram is the ability for local applications to invoke a data conversion program to convert ASCII data streams containing DBCS characters into bitmap images that can be sent to printers that do not have DBCS fonts loaded.

---

### 14.3 Particularities of the IBM Network Station

When considering the use of the printing capabilities of the IBM Network Station, it is important to remember that as opposed to traditional systems, the IBM Network Station does not have local disk storage and that it has a limited amount of memory for applications and data.

These limitations negate the need for a traditional spooling system or for a print management system. However, it still has the capability to handle large print jobs, whether received from a remote host or generated by a local application, by implementing a streaming mode version of LPR/LPD support.

This provides the IBM Network Station with the ability to stream print output to a local printer without having yet received the whole job, or to stream output to a remote host without having generated the whole print job yet, assuming that the remote print server also implements streaming mode.

---

### 14.4 Configuration Using the IBM Network Station Manager

Most of the important parameters that relate to printing are available for configuration using the IBM Network Station Manager.

All these parameters are accessible through the Printers task of the IBM Network Station Manager Setup tasks menu. Below is an illustration of one section of the main configuration panel, to specify the print buffer sizes for the LPR and LPD daemons, and the access control list identifying the hosts that are authorized to send print jobs to the IBM Network Station. These parameters can be specified at the system default level and at the workstation default level.



## Printer Settings - System Defaults

### Printer Services

#### Print client (LPR)

Use Default

Maximum LPR buffer size :

☒ (10%)

(0-95% of available memory)

#### Print server (LPD)

Maximum LPD buffer size:

☒ (10%)

(0-95% of available memory)

Bypass print buffer when file exceeds buffer size:

Default (Yes) ▼

Remote systems allowed to print on this IBM Network Station:

☒ Default (All systems)

☐ All systems

☐ Selected systems

Separate system names with commas.

☐ No systems

Figure 219. The IBM Network Station Manager Printer Settings Configuration

The second part of that same panel is shown below, where remote printers can be added to the list of available printers, and where the local printers can be specified as available or not.

Printer List						
Default printer	Printers	Queue name	Stream type	Description (optional)	Banner page	
<b>Local parallel printer</b>						
<input type="radio"/>	None attached	PARALLEL1	Postscript	Local Parallel P	None	ASCII Options...
<b>Local serial printer</b>						
<input type="radio"/>	None attached	SERIAL1	PCL	Local Serial Pri	None	ASCII Options...
<b>Remote printer server</b>						
<input type="radio"/>			Postscript		None	ASCII Options...
Add a Remote Printer						

Figure 220. Printer List Parameters - System Defaults

Remote printers can be configured not only at the system default level but also at the workstation, group and user default levels.

## 14.5 Additional Details

Here is a very brief overview of the contents of each of the chapters in the *IBM Network Station Printing Guide, SG24-5212* in case you need more details:

- A Few Concepts

A brief review of concepts such as spooling, printer queues, data streams, printer drivers, and LPR/LPD for those who may be new or rusty.

- How Printing Works on the IBM Network Station

Diagrams and tables summarizing all the printing capabilities since Release 1 of the product, and an explanation of the main components involved in providing the print support as well as the particularities of the IBM Network Station, especially the streaming mode support for LPR/LPD.

- Configuration Using the IBM Network Station Manager

How to use the IBM Network Station Manager tool to configure all the main printing-related parameters of the IBM Network Station.

- Host Applications Printing to an IBM Network Station Local Printer

For each major platform, a look at how to define printers, or queues, or ports allowing applications on these hosts to print on printers attached to the IBM Network Station. These platforms include AIX, Windows NT, WinCenter, OS/400, VM and OS/390.

- IBM Network Station Application Printing Examples

This provides details on some of the particularities of each of the local applications on the IBM Network Station when needed to use the printing capabilities. They include the 3270 and 5250 emulators, the NC Navigator browser, Java applications and Lotus eSuite.

- Printing from the IBM Network Station to Remote Hosts

Here we take a look at the preparations required on remote hosts to receive print requests generated by applications on the IBM Network Station, such as ensuring that the LPD daemon is functional, and that there are printer queues defined corresponding to the printers configured in the IBM Network Station Printer Selector table.

- Problem Determination Tools, Tips and Techniques

A collection of miscellaneous considerations that might prove helpful in attempting to solve some of the problems that might arise initially. Also some additional details on some of the more detailed and involved facilities, such as direct access to some of the SERIALD daemon's ports.

- Application Programming Interfaces

A very brief overview of the print APIs available. Since these APIs are not available to the user, this information is provided mainly for the sake of completeness and because it may help in understanding how some of the functions work.

- DBCS Considerations

A very brief look at some of the parameters pertaining to using the DBCS conversion facility.

---

## Chapter 15. The Lotus eSuite Workplace

Lotus eSuite WorkPlace is a suite of applications that include popular Windows-based applications such as a word processor, a Web browser, a spreadsheet application, calendar, mail, etc. but these applications are a subset of their Windows counterpart and they are coded in Java, which means that they can execute locally on the IBM Network Station.

---

### 15.1 Prerequisites

The minimum recommended IBM Network Station hardware for Lotus eSuite WorkPlace is a model 1000 with 64M of RAM because this is what the product has been designed for.

On the Windows NT Server, the JDK 1.1.5 is required, in addition to all the other prerequisite products for the IBM Network Station Manager.

---

### 15.2 Installation

Insert the Lotus eSuite WorkPlace CD in the CD-ROM drive on the server and the InstallShield should be launched automatically. If not, type `x:\pc\setup.exe`, where x: is the CD-ROM drive.

There is a readme.txt file in the root directory of the CD, but it is only a short pointer to the contents of the CD.

The real readme.txt file that we recommend you should always read before proceeding with the installation is in the PC subdirectory on the CD. The description here is a repeat of that information with a few comments and illustrations added.

The install process is fairly uncomplicated. You get the usual InstallShield panels, one of which is the destination directory as shown in the next figure.

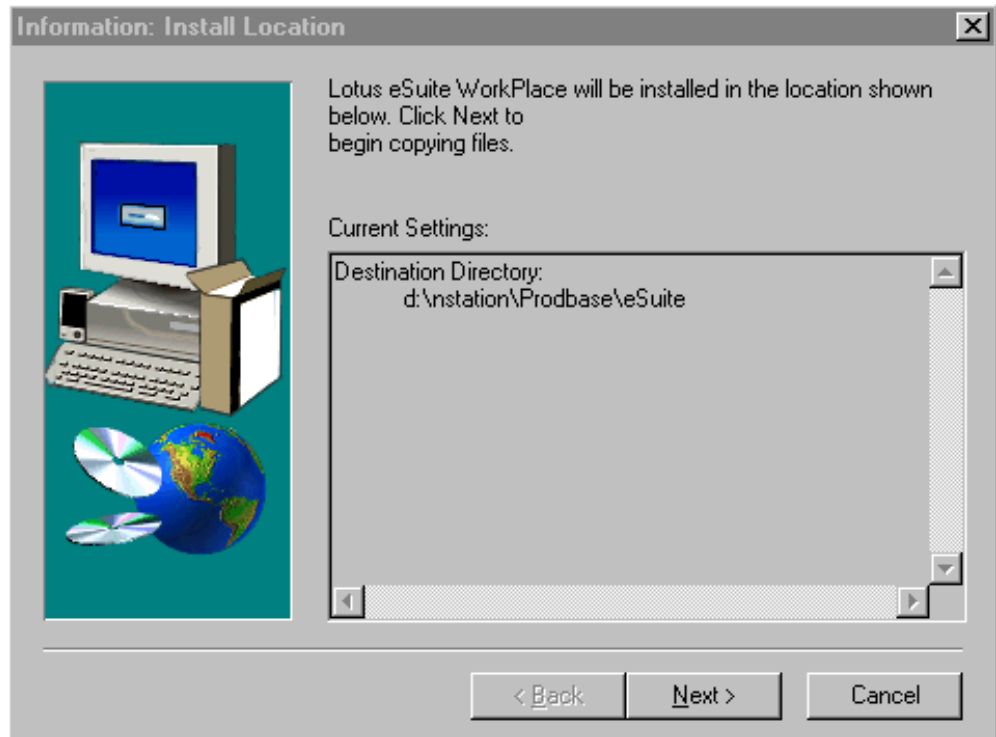


Figure 221. Destination Directory - Lotus eSuite WorkPlace Installation

If you attempt to install and you do not have the JDK 1.1.5 installed, the installation process issues a warning and terminates.

After the installation process ends, reboot the server to complete the installation, because there were NT services that were installed and need to be started.

After a reboot, you should see two command prompt entries on the task bar:

- One labeled x:\jdk1.1.5\bin\rmiregistry.exe
- One labeled x:\jdk1.1.5\bin\java.exe

They remain on the task bar all the time.

The following three environment variables are added to your system variables:

- DESKTOP\_HOME
- JAVA\_HOME
- HOSTNAME

Examining the NT services, you should also see two new entries labeled Java RMI Registry and Lotus eSuite Workplace Registry, as illustrated in the next figure:



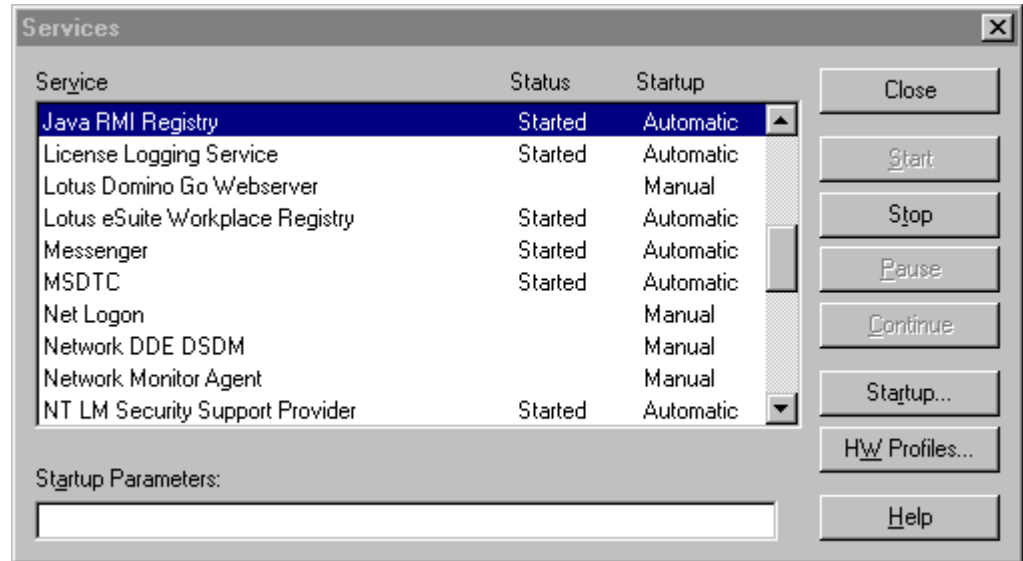


Figure 222. NT Services for Lotus eSuite WorkPlace

## 15.3 Configuration/Administration

Before an IBM Network Station user can use the Lotus eSuite WorkPlace, there are a few configuration tasks that need to be performed.

### 15.3.1 Configure the DNS in IBM Network Station Manager

Use the IBM Network Station Manager to ensure that your domain name server (DNS) information is properly configured.

Select **Hardware=>Workstations=>System Defaults**, scroll down to Domain Name Server, and select the entries as illustrated below:

**Domain Name Server:**

Domain name server to use:

☐ DNS Configuration from BOOTP or DHCP server  
☒ DNS Configuration created by Network Station Manager  
☒ Update Network Station Manager DNS file

Figure 223. DNS Configuration in IBM Network Station Manager

What this entry specifies is that the domain name server configuration can be obtained either from the DHCP options if the IBM Network Station is booted from DHCP or from the boot server configuration files when they are loaded. In this later case, the DNS information is generated from the DNS information on the boot server.

If you are using a DHCP server, the first entry is the one that should be selected.

## 15.3.2 Configure the Desktop in IBM Network Station Manager

This activity lets you specify which IBM Network Station users will have the Lotus eSuite WorkPlace desktop configured as their default desktop when they log on to their IBM Network Station.

As with all other IBM Network Station Manager parameters, you can configure at the system level, to make changes applicable to all users, or you can use the group level or the individual user level. In order to simplify these examples, we decided to define a group called esuite that we use to configure the eSuite characteristics.

### 15.3.2.1 Create a New Group

Before we can enter this group name in any of the IBM Network Station Manager configuration panels, we need to define it to Windows NT using the User Manager for Domains, so we create this group first.

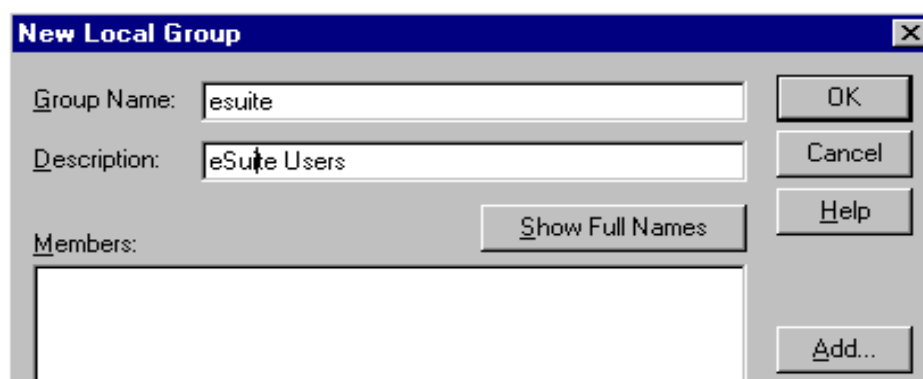


Figure 224. Creating a New NT Group

### 15.3.2.2 Define Desktop Settings

Now that we have a group, use the IBM Network Station Manager to define the default desktop settings for members of this group. In NSM, select **Startup=>Menus=>Group Defaults**, with the name esuite entered in the group name, as illustrated below:

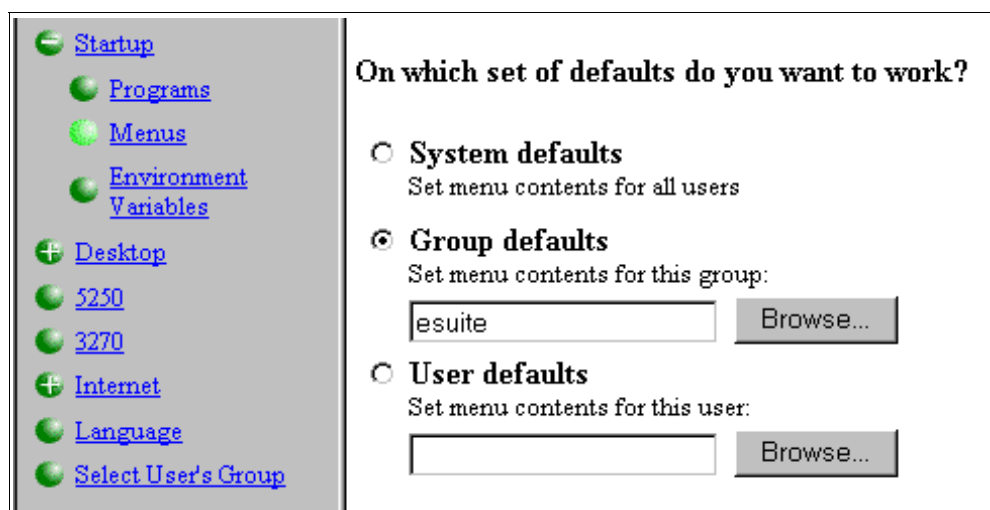


Figure 225. Setting Group Defaults

In the Desktop and Menu Bar Options, the choices are as illustrated below:

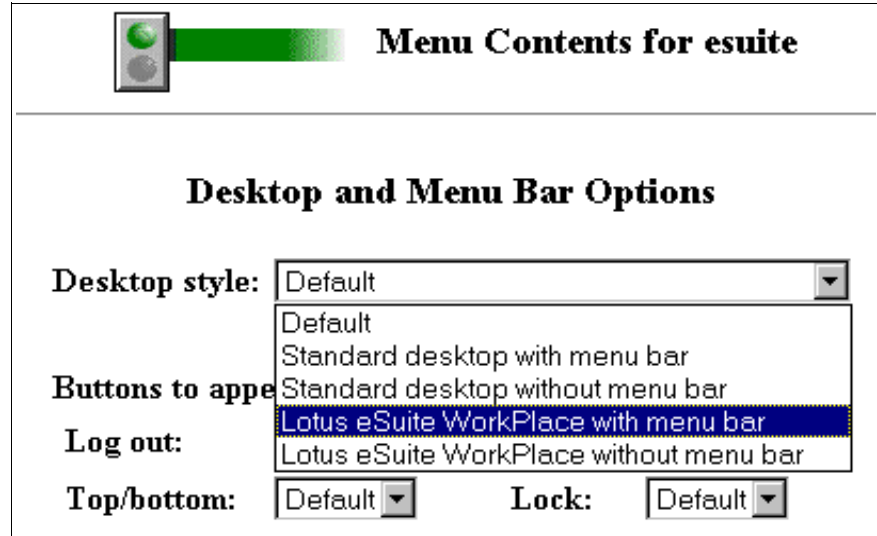


Figure 226. Desktop and Menu Bar Options

We select the **Lotus eSuite WorkPlace with menu bar** option. This means that any user that is a member of the esuite group will get by default, at logon, the eSuite desktop started.

### 15.3.2.3 Define a Time Zone Environment Variable

We also need to define an environment variable for the time zone so we select **Startup=>Environment Variables=>User Defaults** for the esuite group.

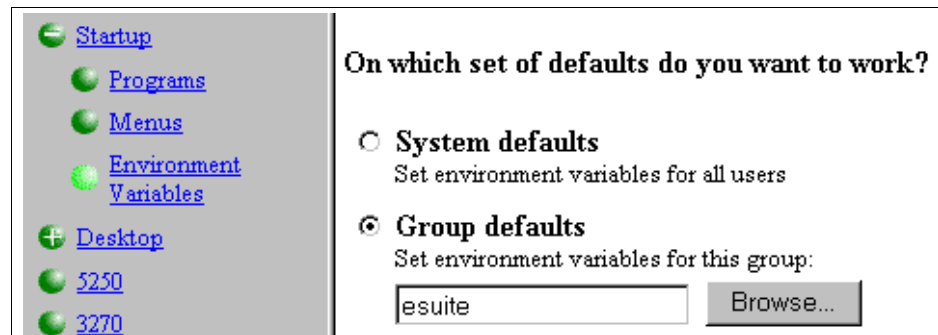
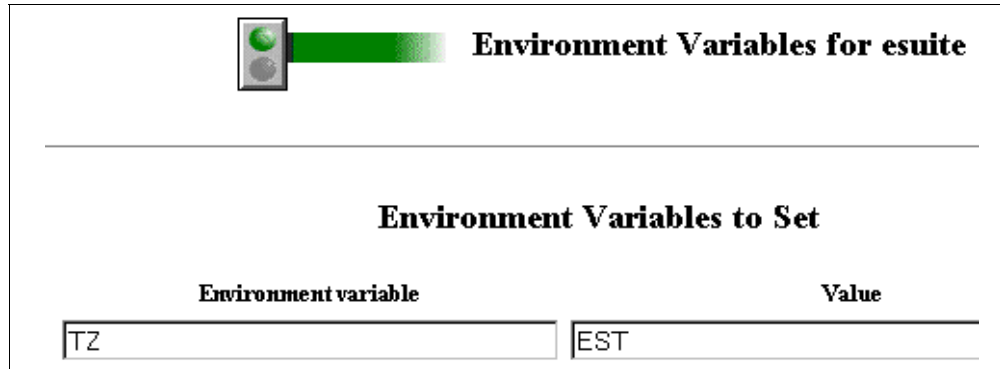


Figure 227. Setting an Environment Variable

In the next panel, enter the variable name TZ (for time zone) and enter the value appropriate to your location.

In our example here, we use the Eastern Standard Time (EST) zone.



**Environment Variables for esuite**

---

**Environment Variables to Set**

Environment variable	Value
TZ	EST

Figure 228. Setting the TZ Environment Variable

#### 15.3.2.4 Adding Users to a Group

While we are still in the IBM Network Station Manager application, we might as well do one more task, which is to add users to the group we just defined.

If we had decided to make all the configuration changes above applicable only to a specific group, but applicable to all users, then we would have made the changes in the system defaults and there would be no need for this additional step.

However, it is possible that all IBM Network Station users might not also be Lotus eSuite WorkPlace users, which is why we decided to make an esuite users group only for the esuite users.

In this example, let's assume that we have two users, Ariane and Thomas, that are already defined as Windows NT users, and members of the NSMUser group so that they can log in from an IBM Network Station, and also members of the esuite group, as shown below:

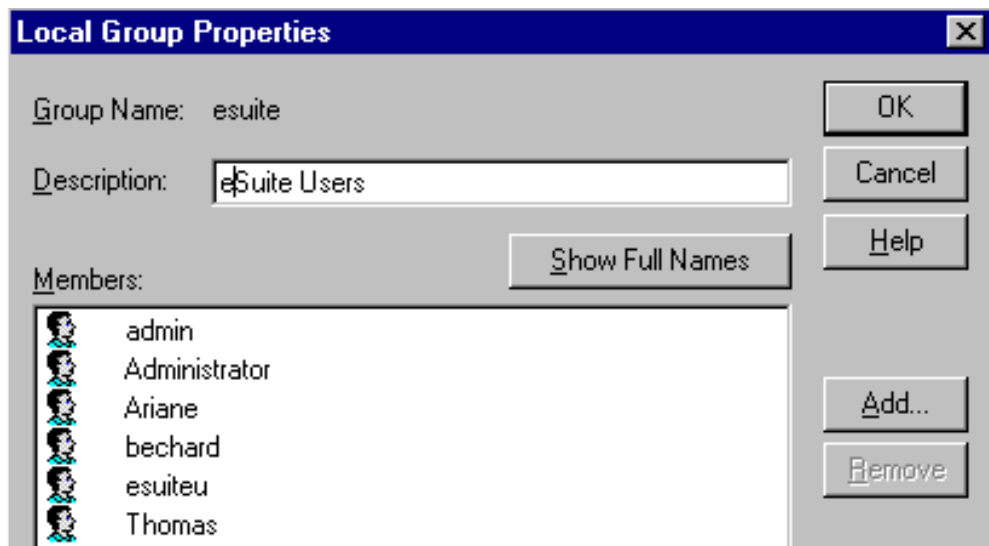


Figure 229. Members of the esuite Group

However, that is *not* sufficient. Ariane and Thomas are part of the esuite group in Windows NT, but they must also be made part of that group in IBM Network Station Manager.

In other words, we must also tell IBM Network Station Manager that these two users should use the defaults that have been defined in NSM for the esuite group.

To do this, select the **Select User's Group** task in the NSM Setup Tasks list, and use the **Browse** button to display all the user names in the Windows NT User Manager for Domain definitions.

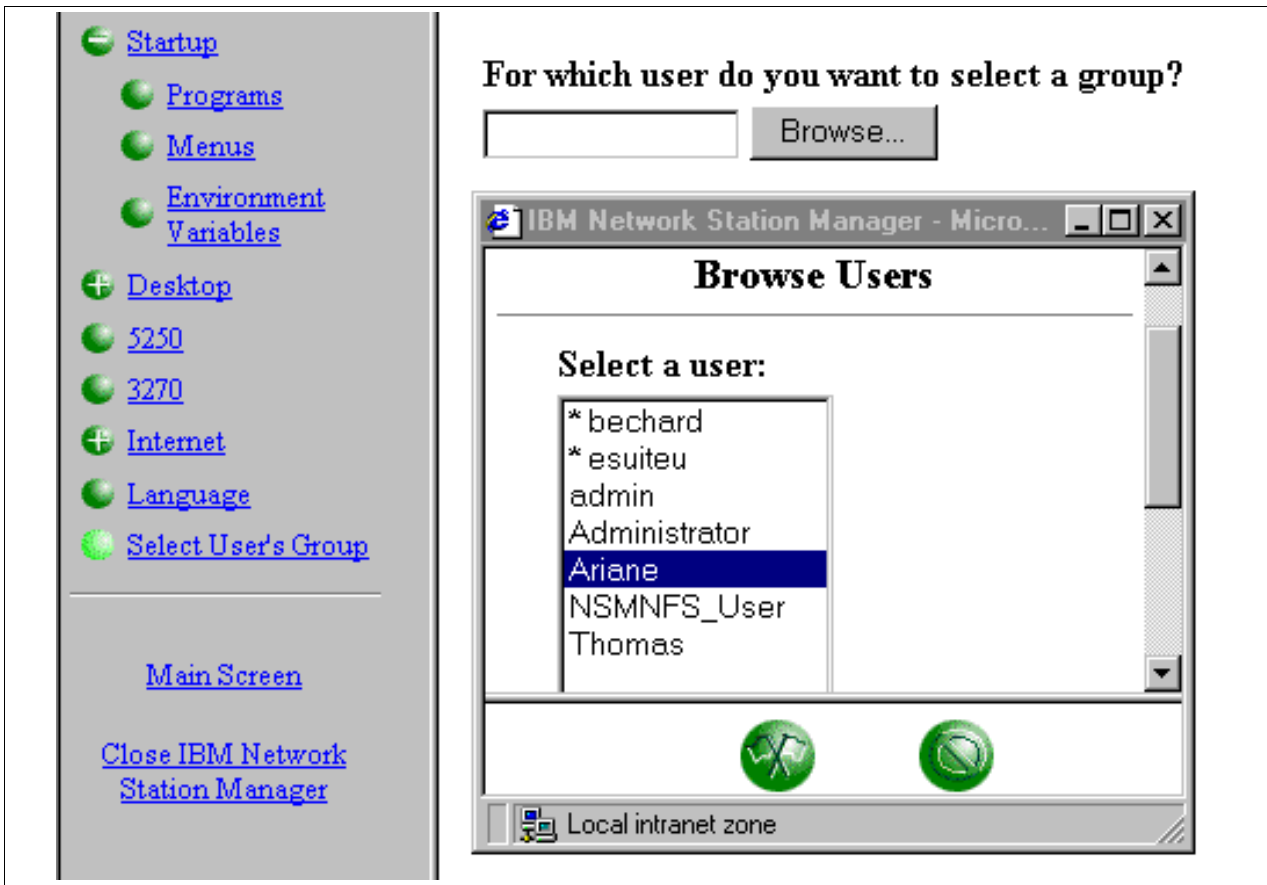


Figure 230. Selecting a Users Group

In the Select a user list, we choose Ariane for example, and choose **Select** and **Return**, and then **Next**, which brings up the next panel, as shown in Figure 231 on page 254.

Remember that what we are doing here is indicating to IBM Network Station Manager that when choosing defaults for this user, the settings in the group selected here should be applied to this user.

Even though a user can belong to more than one group at the Windows NT level, that user can only choose one group in NSM from which to inherit the default settings.

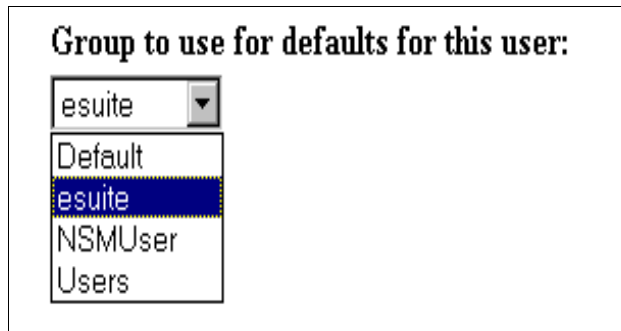


Figure 231. Choosing a Group for a User

In the panel above, choose one group (in our case the esuite group). User Ariane inherits the default settings specified in that group, which in our case means that the user will get a Lotus eSuite WorkPlace desktop at login.

Repeat the procedure for user Thomas, and any other users that you want to include in that group.

### 15.3.3 Starting the eSuite WorkPlace Administrator

We are not quite finished yet, but nearly there. The last set of tasks to be accomplished is to use the eSuite WorkPlace Administrator to define users and to set some application settings.

Unfortunately, this requires an additional administrator interface which is different from the IBM Network Station Manager.

Because the eSuite WorkPlace Administrator has been designed to be run by a user named admin, you must first create such a user ID on the Windows NT server and make it a member of the NSMAdmin and NSMUser groups. Then log off and log back on as user admin.

To start the eSuite WorkPlace Administrator, bring up a command prompt, change the directory to \nstation\prodbase\esuite and type `ewadmin`, as shown below:

```

Command Prompt - ewadmin

D:\>cd \nstation\prodbase\esuite

D:\nstation\PRODBASE\esuite>ewadmin
ECHO is off.
d:\jdk1.1.5\bin\java -classpath .;d:\jdk1.1.5\lib\classes.zip;d:\nstation\Prodba
se\esuite;d:\nstation\Prodbase\esuite\com\lotus\jars\hotjava.jar;d:\nstation\Pro
dbase\esuite\com\lotus\jars\swing.jar;d:\nstation\Prodbase\esuite\com\lotus\jars
\organic.jar;d:\nstation\Prodbase\esuite\com\lotus\jars\motif.jar;d:\nstation\Pr
odbase\esuite\com\lotus\jars\windows.jar -Duser.base=d:\nstation\Prodbase\esuite
/ -Duser.home.server=itsowts -Dhotjava.home=d:\nstation\Prodbase\esuite\lib\hotj
ava -Dhelp.files.home=file://localhost/d:\nstation\Prodbase\esuite\com\lotus\ser
ver\help/en/ -DStartup.Root=file:/d:\nstation\Prodbase\esuite\com\lotus\server\ad
min com.lotus.server.admin.NCAdmin
[Loading: C:\WTSRU\Profiles\admin\hotjava\urlpool]

```

Figure 232. Starting the eSuite Workplace Administrator

A small logo appears indicating that the application is starting:



*Figure 233. Lotus eSuite WorkPlace Administrator Starting*

Then the main configuration panel is displayed, as shown below:

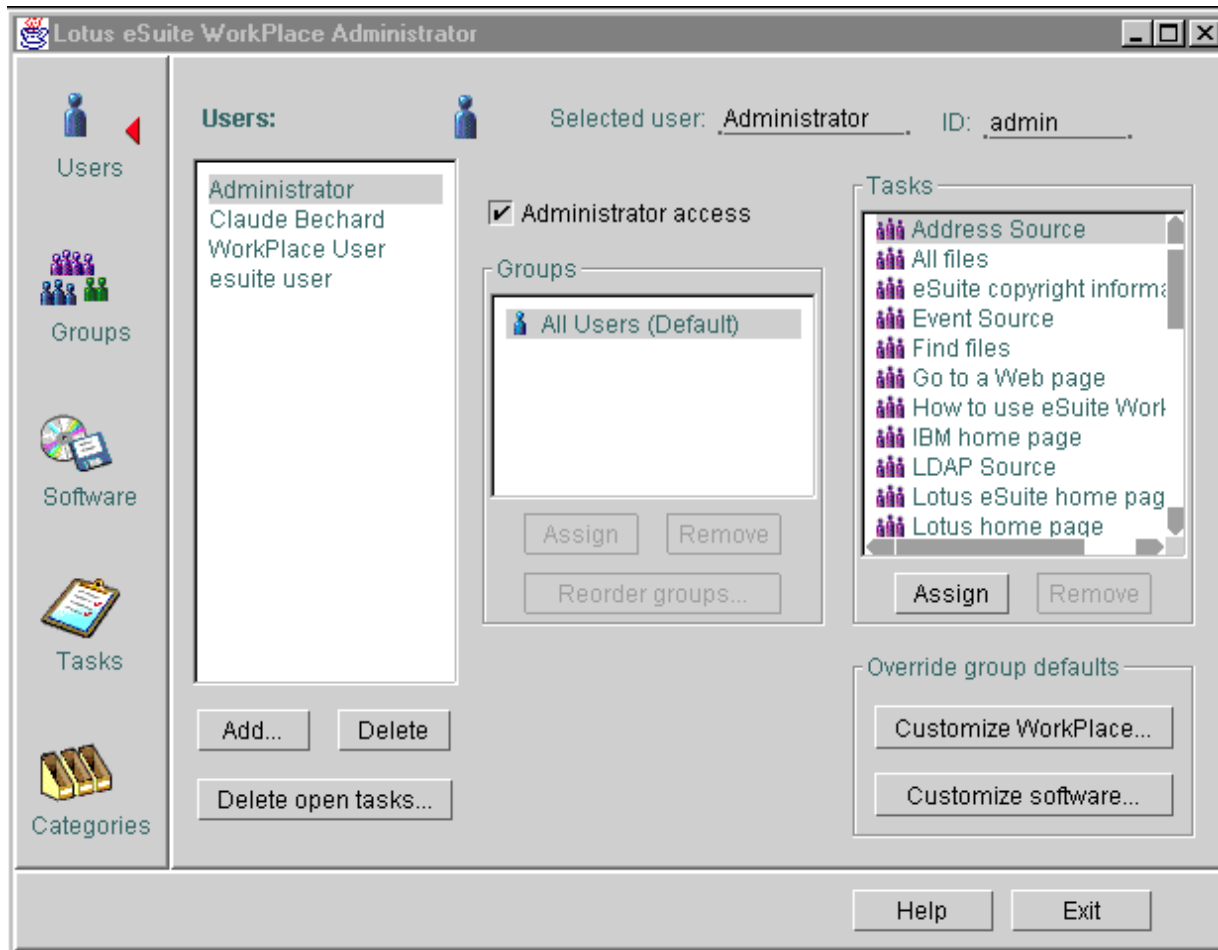


Figure 234. Lotus eSuite WorkPlace Administrator Main Configuration Panel

### 15.3.4 Configuring eSuite WorkPlace Applications

We have two more tasks left to do using this interface in order to provide our IBM Network Station users with the Lotus eSuite WorkPlace desktop.

#### 15.3.4.1 Add Users to the Lotus eSuite WorkPlace Administrator

This step seems to have been omitted in the readme file that we had on our version of the CD, but it is required.

Any user of the Lotus eSuite WorkPlace Desktop must first be added using the eSuite WorkPlace Administrator. This is required because the desktop can be customized for each user in terms of the groups and application tasks that appear on the user's desktop, and each user must therefore be identified. This cannot be done in the IBM Network Station Manager application because it is unaware of the eSuite application settings.

To add our Ariane and Thomas eSuite users, click on the **Add** button at the bottom of the Users list on the left-hand side of the panel. This brings up a small panel, such as the one below where you can enter the user ID that was defined in the Windows NT server, and you can use any user name if you want to identify this user by a name different than the user ID. Be aware that the name that



appears in the Users list however is the user name, not the user ID, unless you leave the user name blank, in which case the user ID is used also as user name.

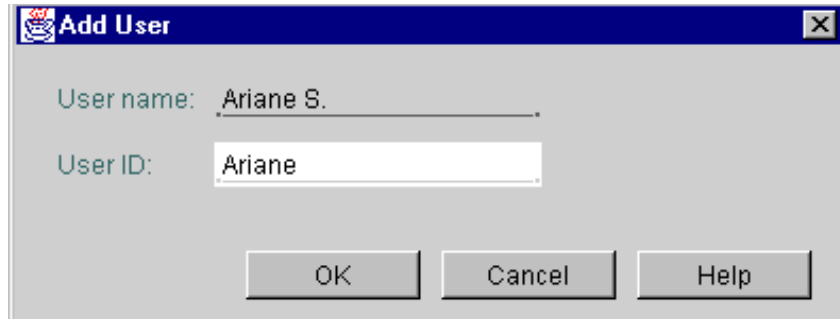


Figure 235. Adding a User to eSuite WorkPlace Administrator

#### 15.3.4.2 Customizing eSuite WorkPlace Applications

Some applications may require some customization before users can use them. Such is the case of the Web browser for example, which requires a proxy configuration if users are to access the Web.

Let us assume that in our example, we want to set the proxy settings for all users.

**Note:** We do not intend to describe here how to use the eSuite WorkPlace Administrator for all functions but only to show how to accomplish the first few tasks required to be operational. Please consult the online documentation and the online Help facilities to learn how to use this interface.

To set a proxy for all users, select, on the left-hand side, the icon labeled **Groups**, which displays a panel such as the one illustrated below:

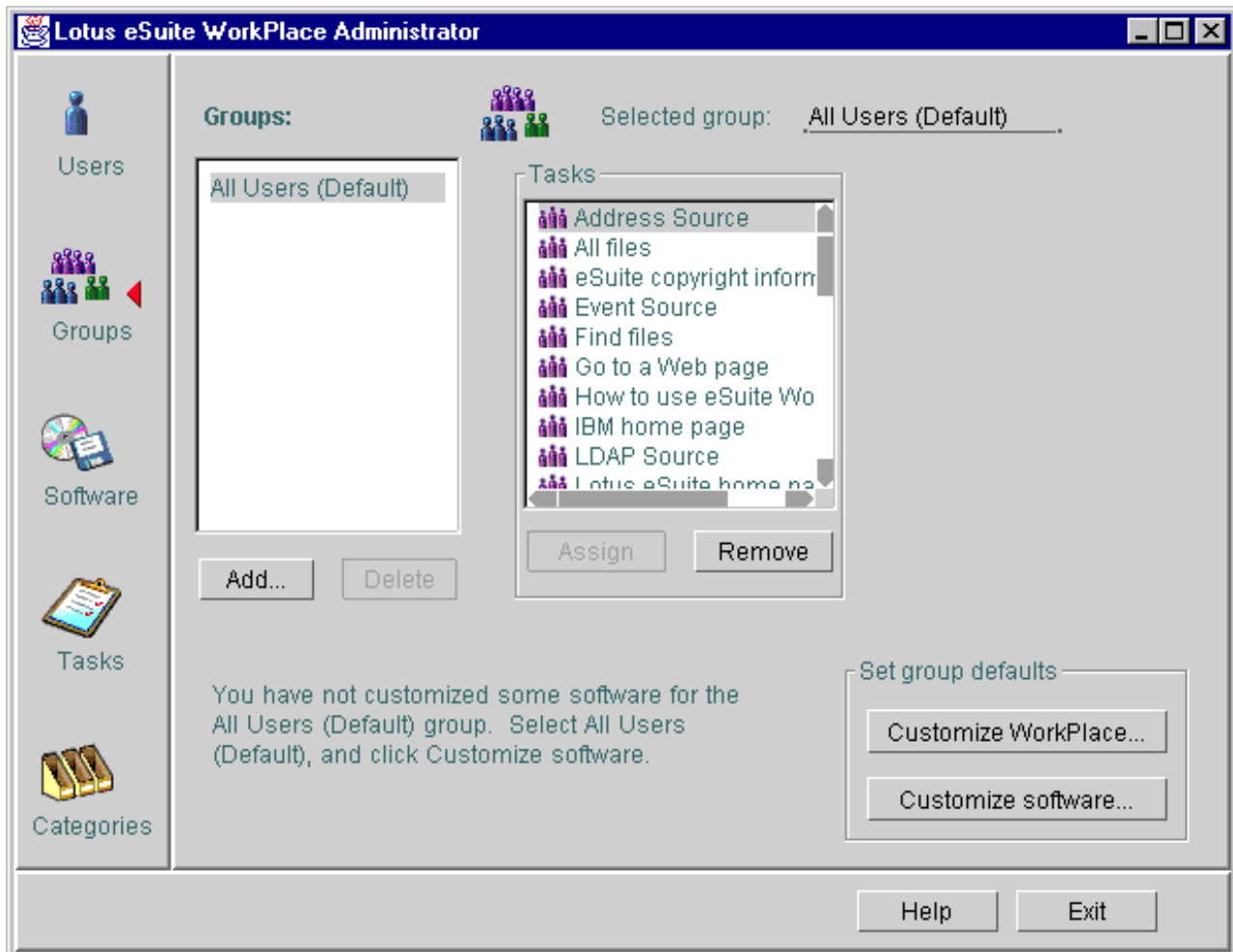


Figure 236. The All Users Group in eSuite WorkPlace Administrator

On this panel, in the bottom right-hand corner, click on the **Customize WorkPlace** button to bring up the next panel:

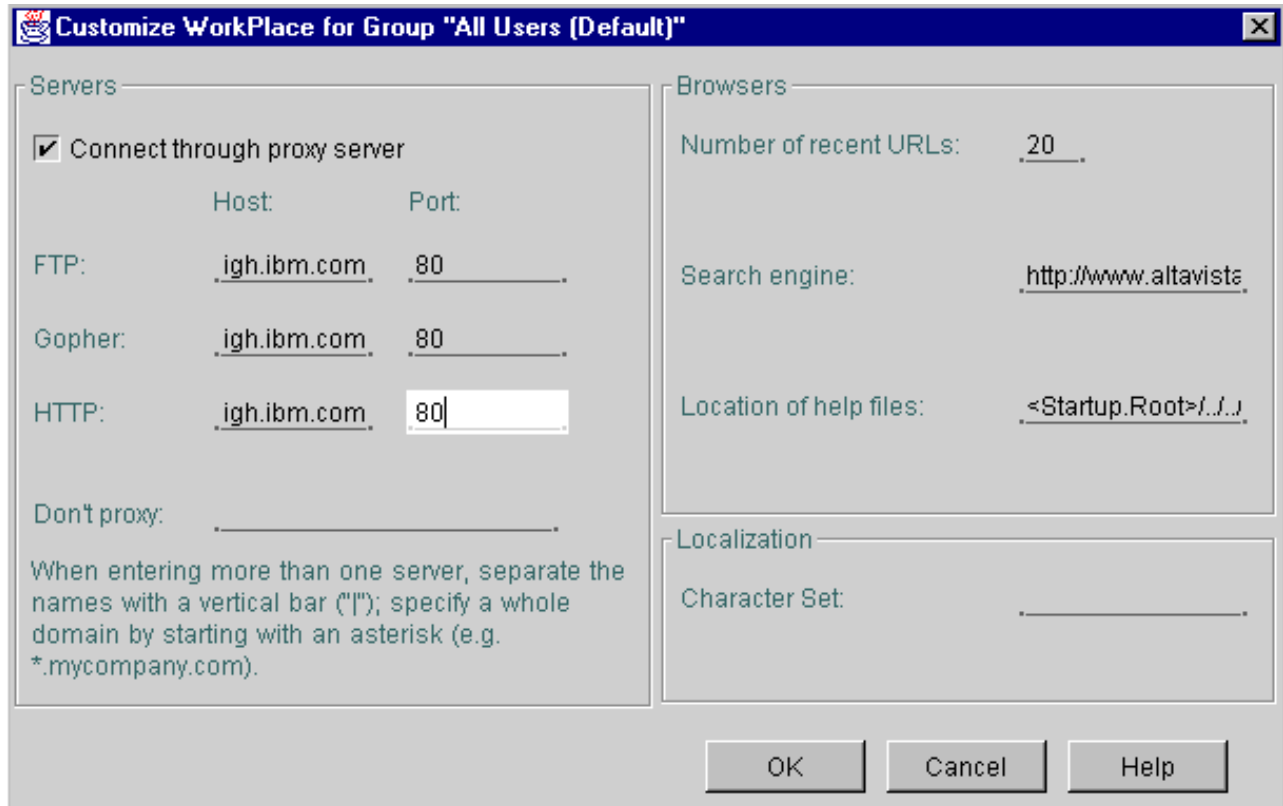


Figure 237. The Customize Workplace Panel in eSuite Workplace Administrator

On this panel, put a check mark in the Connect through proxy server check box.

This opens up the FTP, Gopher and HTTP fields in which you can enter the name of a proxy host and the port used.

In our example, we used proxy.raleigh.ibm.com and port 80 which are the valid values for our site. This application is not socksified which is why it does not have an entry field for a socks host instead of using proxies.

Notice on the panel above that there is an entry on the right-hand side labeled Search Engine, where <http://www.altavista.digital.com/> is specified. This specifies the default search engine to use on the Web and it can be changed to another if preferred. This can be done for all users, for groups or for specific users.

### 15.3.5 Starting the eSuite Workplace Desktop

That concludes the installation and configuration required to activate the Lotus eSuite Workplace desktop on an IBM Network Station.

Boot the IBM Network Station from the server where the Lotus eSuite Workplace is installed, and log on with one of the users that was defined as an eSuite user.

After the user is authenticated, the Lotus eSuite Workplace desktop should be automatically started and there should be a menu bar item labeled eSuite for restarting the eSuite desktop if necessary.

The default standard desktop that gets displayed is illustrated in the next figure:

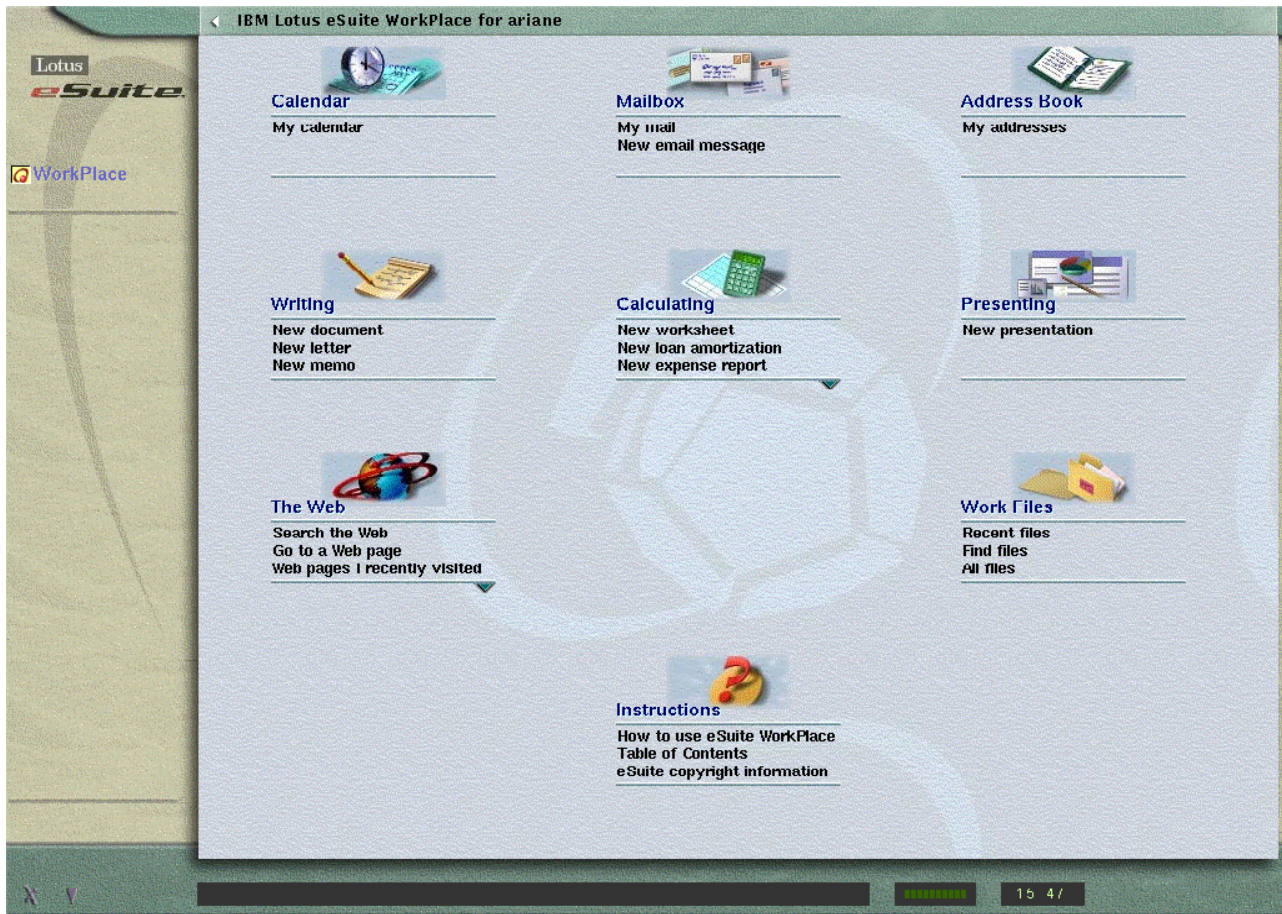


Figure 238. The Lotus eSuite WorkPlace Standard Desktop

On the panel above, tasks that the user can perform are grouped into categories of tasks. These categories are configurable through the WorkPlace Administrator.

Multiple tasks can be started and these tasks then appear on the left-hand side of the panel where the user can switch from one to the other by selecting each task.

If we click on the **Search the Web** task, located in the The Web category (bottom left-hand corner of the main panel), we get the panel displayed in the next figure:

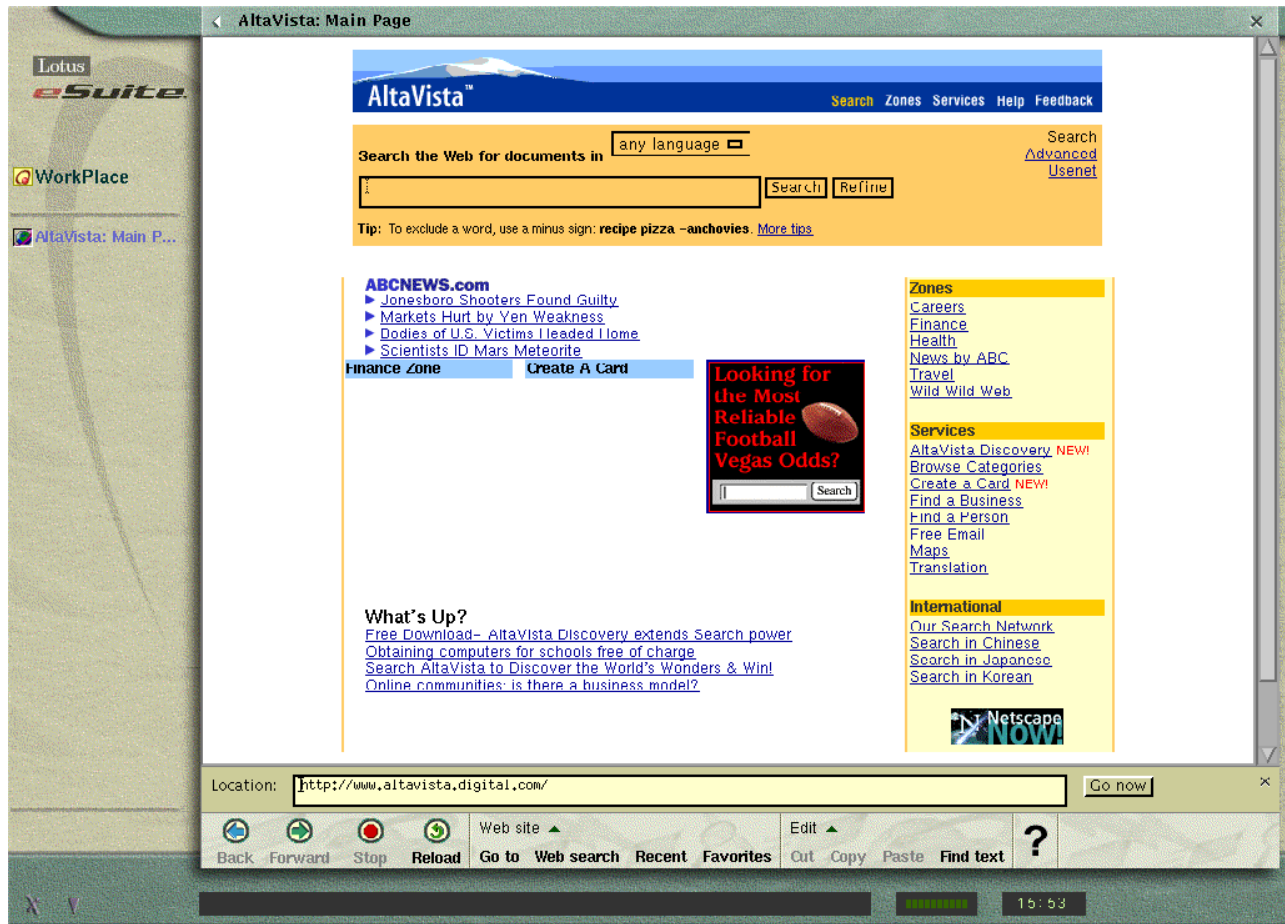


Figure 239. The Lotus eSuite WorkPlace Browser Application

This is the browser interface, which has accessed the default URL of the AltaVista search engine.

Notice that a small icon has appeared on the left-hand side of the panel representing this task.

The best way to get familiar with the application is to explore and try all the tasks and to use the online help.





---

## Chapter 16. National Language Support (NLS)

This chapter focuses on the National Language Support functions provided by Release 3 of the IBM Network Station Manager.

The objective is to provide an overview of the supported functions and a brief description of how to use them.

The most important aspect is probably to understand which functions are available in which language and what exactly is the effect of a particular function.

The main functions we discuss are:

- The installation language
  - A brief summary and rules of thumb
  - The installation dialog's language
  - The application language
  - The Windows NT regional settings
  - The Windows NT input locales
- The startup (or boot monitor) language
- The keyboard language
- The login panel language
- The kernel environment language

---

### 16.1 Installation Language

When discussing installation language, there is a need to distinguish between whether we are talking about the language used during the installation or the language used by the application once installed.

There is also a need to distinguish between the additional products and the IBM Network Station Manager because they behave differently when it concerns installation in a language other than English.

---

### 16.2 Summary - Rule of Thumb

It is likely that if you are installing in a language other than English you will want all components to be in that language, in which case the choices are pretty simple and straightforward.

The discussion only gets complicated when you want to start mixing different languages, which is why we give a bit more details in the section that follows.

Assume that you are a French user and that you want every product to be in French. Your installation procedure would then be as follows:

1. Install the Windows NT base system, where you would choose to install in French, and your Windows NT Regional Settings and Input locales would be specified as French.
2. Insert the NSM CD and on the first panel and choose **French** as the installation language.

3. Install the Additional Products first, which would be installed in French because of your language selection on the first panel. The installation dialogs, Install Shield dialogs and installed shortcuts are all in French.
4. Start the NSM installation and choose **French** as the installation language. That choice causes the installation dialog to be in French, and the installed icon labels and shortcuts to be in French, but the installation process also checks the language specified in your Windows NT Regional Settings and installs the French version of NSM (even if you had chosen another installation language on the Language Selection panel) because the determining factor for the installation language is the Windows NT Regional Settings.

So, this is pretty simple, but it can get a bit more complicated if you start talking about mixed language environments. Therefore, before this discussion gets a bit more complicated, there are two simple rules to remember:

1. When you install additional products such as the Netscape browser or the Lotus Domino Go Webserver, the language selection you make on the first installation panel determines *both* the language that will be used for the dialogs used during the installation process *and* the language of the installed application.
2. When you install the IBM Network Station Manager (which includes the eNetwork On-Demand Server), the language selection you make on the first installation panel, or on the specific NSM Language Selection panel affects *only* the language used for the dialogs during installation.

The language of the installed application is actually determined by your choice of the Windows NT Regional Settings. In other words, you choose the language of the application by choosing a regional setting in Windows NT and *not* by selecting an installation language during the installation dialogs.

Now that we have summarized it, let's establish a few terms that we can use to describe in a bit more detail what we discussed above.

### 16.2.1 The Installation Dialog Language

The installation dialog language is the language used for communicating with the user during the installation by the IBM Network Station Manager application process and by the InstallShield installation interfaces.

The effect of choosing a language to be used during the installation affects the language used on any of the installation panels and dialogs, including the InstallShield panels.

**Note:** This also affects the language used on labels for icons or shortcuts that are created by the installation process. In other words, be aware that if you are actually installing an application for an English user for example, and you use French because you happen to understand that language, then your English user will end up with shortcuts that are labeled in French.

A simple rule should then be that you should use the same language for the installation as the language that you intend to use for the application.

There are two places where the user chooses the installation dialog language:



1. On the first IBM Network Station Manager Release 3 Installation panel, as illustrated in the next figure:



Figure 240. The First Installation Panel

The choice you make here determines the language used when installing the additional products or the NSM.

**Note:** In the case of the additional products (Netscape and Lotus Go), this also determines the language of the installed application.

2. On the IBM Network Station Manager Release 3 Setup Language selection panel, which is the first panel that appears after the user chooses Run Installation.

This panel applies *only* to the installation dialog language for NSM and cannot be used to select the language for the installed application. The *only* way to select the installed application language is by setting the Windows NT regional settings *before* starting the application process.

The selection list on this panel contains about 22 entries.

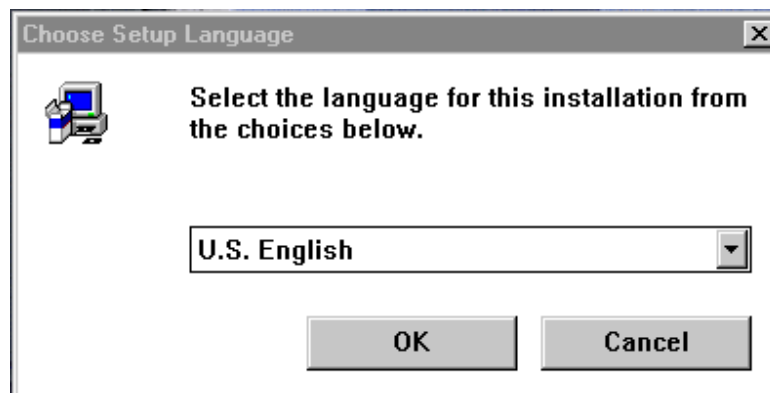


Figure 241. The NSM Release 3 Setup Language Selection Panel

### 16.2.2 The Application Language

The application language is the language that the product being installed uses after installation when communicating with the user, in other words, the language

used when displaying panels and messages to the user when he or she starts the application.

For the NetScape and the Lotus Go products, this is chosen by selecting a language on the first installation panel. If the language selected is not one of the primary six languages, choose **Other Languages**, which directs you to how to install using the other available languages. In those cases, you are presented with a readme file that displays the directories where the setup.exe is located for other languages, and the setup.exe can be launched from those directories directly.

For the IBM Network Station Manager, the only way to choose the application language is to set the Windows NT regional settings to the desired language *before* you start the installation. In other words, the application process automatically determines the language of the application based on the Windows NT regional settings, no matter what you selected as the installation dialog language.

### 16.2.3 The Windows NT Regional Settings

This is the setting of the Windows NT system indicating the primary language or default system locale that the system is set for. This is defined by selecting **Start=>Settings=>Control Panel=>Regional Settings**, which displays a panel as illustrated in the next figure:

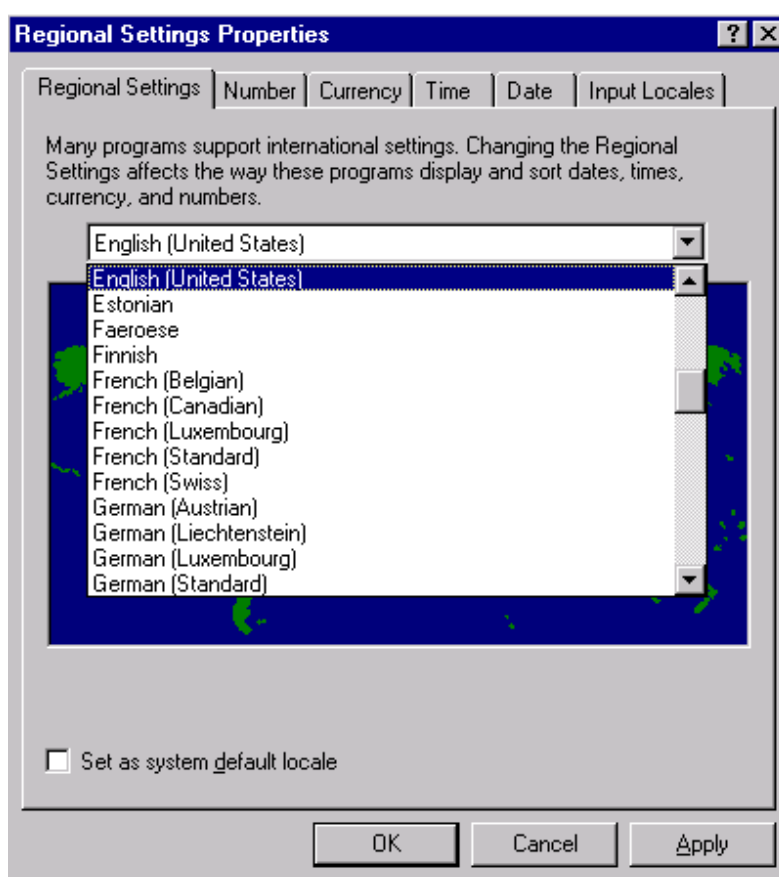


Figure 242. The Windows NT Regional Settings

The procedure for setting a language is to choose one of the over 75 choices available on this panel. Click on the **Set as system default locale** at the bottom of the panel, and click on **OK**.

This may require access to the Windows NT CD if this is the first time that this locale is installed, and it requires a reboot to take effect.

It is this language setting that determines the language that the IBM Network Station Manager application will use, and only one language can be selected. In other words, on the Windows NT platform NSM can only be installed in one language, and all users using the application must use the installed language.

Other platforms, such as AS/400, do have the ability to have multiple versions of NSM in different languages on the same platform, in which case, a user can select the language of his or her choice for operating the IBM Network Station Manager.

#### 16.2.4 The Windows NT Input Locales

On the same panel as shown in the previous figure, selecting the **Input Locales** tab on the right-hand side allows the user to select effectively a keyboard layout corresponding to a language.

More than one language can be installed, as illustrated in the next figure, and the user can switch between layouts at any time either by using this panel, or by using one of the key combinations selected on this panel (Left Alt + Shift in this example) or even more simply, by checking **Enable indicator on task bar**, which puts a small selectable on the task bar, EN or FR. Switching from one to the other is only one click away.

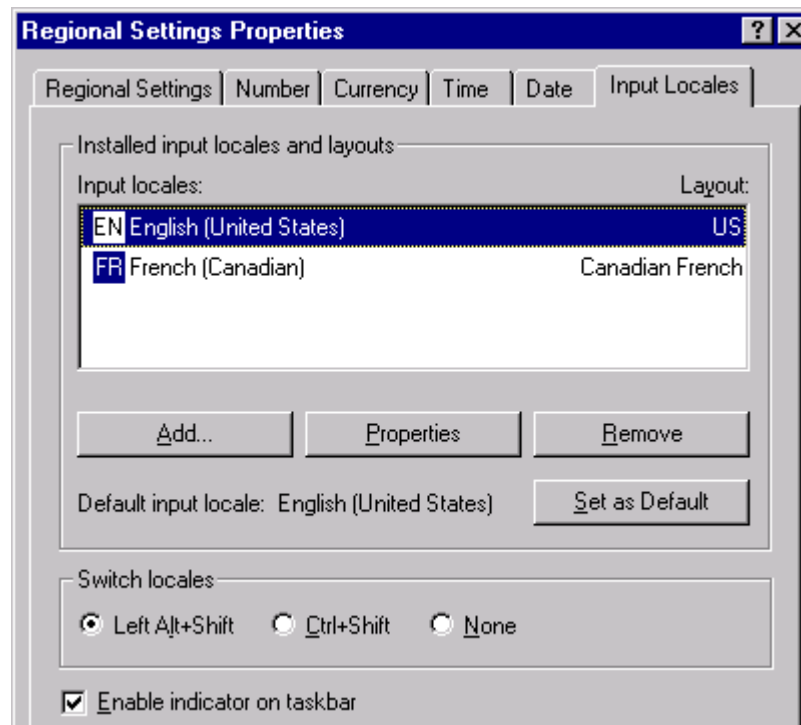


Figure 243. The Windows NT Input Locales

This setting has no effect on the language that the installation process uses for any product.

Next, let us take a look at the other elements of language on the IBM Network Station itself.

---

## 16.3 The Startup Language

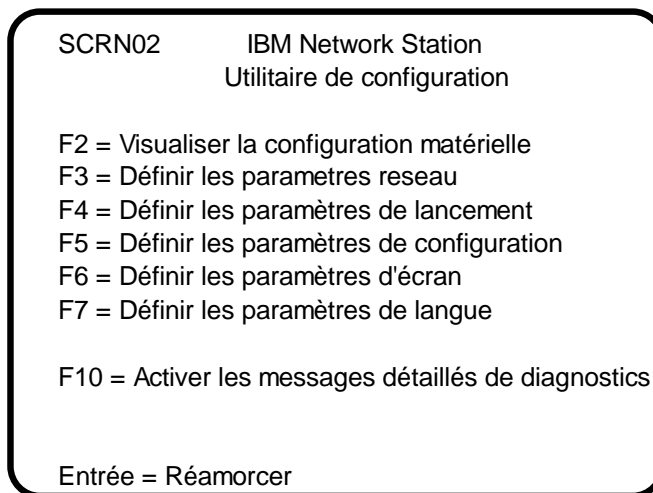
This concerns the language used on the IBM Network Station itself when using the Setup Utility configuration panels.

This is also sometimes referred to as the boot monitor language or the boot sequence language.

### 16.3.1 What Does It Affect?

The setting of the startup language affects:

1. The language of the Setup Utility panels, such as the main Setup Panel, which we show below in the French version:



2. The messages that are displayed on the IBM Network Station monitor when the station is booted, are all the messages between the time that the LOGO appears until you see the progress bar at the bottom of the screen showing that the kernel is being downloaded.

The messages that appear afterwards during loading of the configuration files if the verbose option is turned on, remain in English as these should really not concern the user.

### 16.3.2 How Is It Configured?

There are two ways to configure the startup language:

1. By using the F7 function on the main Setup Utility panel at the IBM Network Station, as shown below:

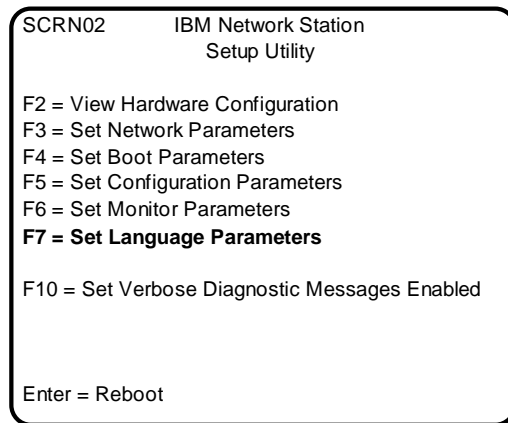


Figure 244. The Main Setup Utility Panel

This brings up the next panel, where F2 allows the selection of the keyboard language, and F3 allows the selection of the one of six languages for the startup language.

A selection of any of the six languages is effective immediately.

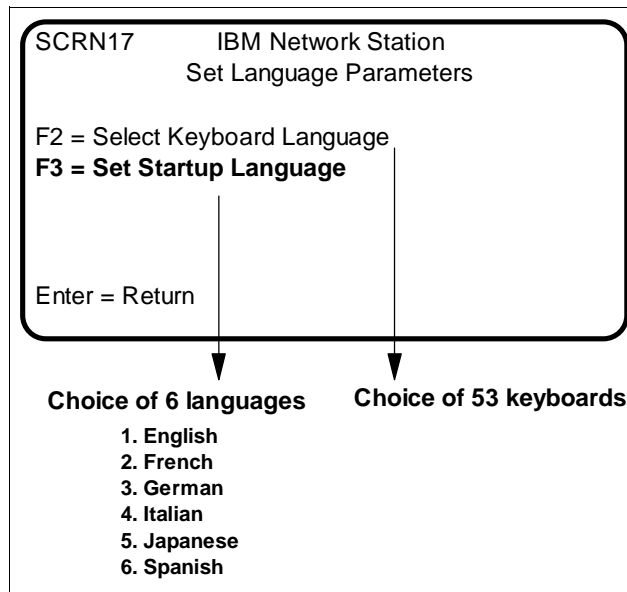


Figure 245. Setup Utility - Set Language Parameters

## 2. By using the IBM Network Station Manager

Select **Hardware=>Workstation=>System Defaults or Workstation Defaults**, and then **Boot Parameters**, as illustrated below:

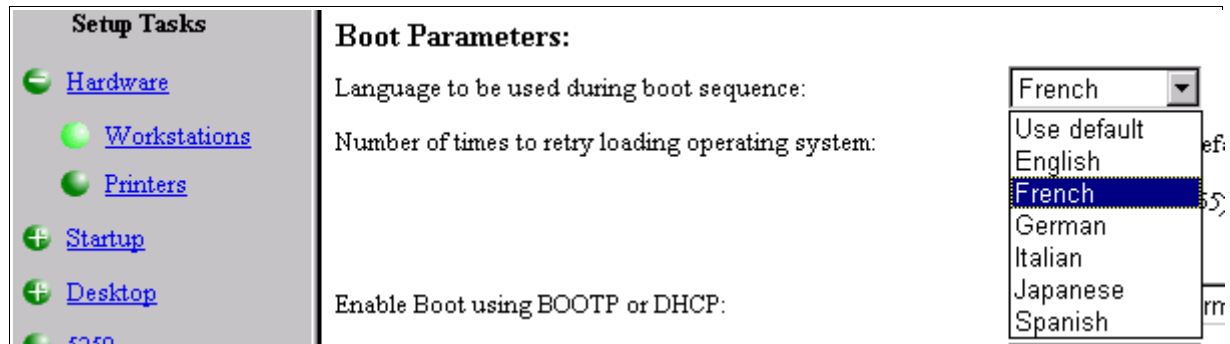


Figure 246. Setting the Startup Language

The language value selected in the IBM Network Station Manager configuration overrides the value selected through the Setup Utility.

## 16.4 The Keyboard Language

The keyboard language concerns the keyboard mappings that are used by the IBM Network Station.

### 16.4.1 What Does It Affect?

The keyboard language affects the characters that are displayed on the IBM Network Station monitor as keys on the keyboard are pressed.

Each key on the keyboard has a character associated with it, which depends on the keyboard map used.

If you specify a keyboard mapping of French (Canada) for example, the key with the forward slash (/) on an English keyboard (key above the right Alt key) displays an e with an accent (é).

Ideally, the keyboard language selected should match the physical configuration of the keyboard used.

### 16.4.2 How Is It Configured?

There are two ways to configure keyboard mapping:

1. Using the Setup Utility on the IBM Network Station.

This is done using the F7 function on the main Setup Utility panel and then F2 for selecting the keyboard language, as illustrated in Figure 244 and Figure 245 above.

2. Using the IBM Network Station Manager.

Select **Hardware=>Workstation=>System Defaults or Workstation Defaults**, and then **Keyboard Settings**, as illustrated below, where the selection list has over 50 entries:

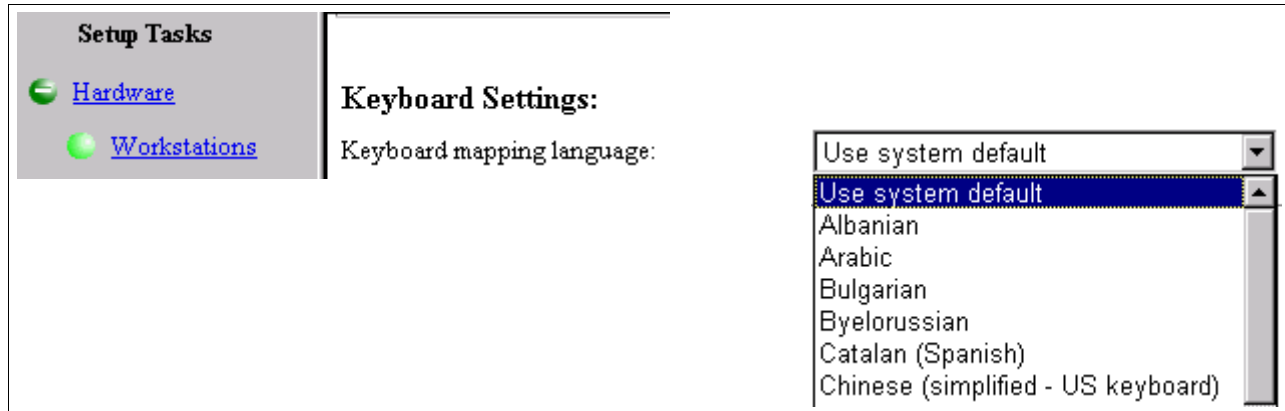


Figure 247. Setting the Keyboard Language

- If you select **Use system default**, the value used is the value specified in the Setup Utility panel, the default of which is English.
- If you select a specific value, then the value selected here overrides the value selected in the Setup Utility panel.

## 16.5 The Login Panel Language

The next area to look at is the IBM Network Station Login panel, where the user is asked to enter a user name and a password.

### 16.5.1 What Does It Affect?

The Login language only affects the field names displayed on the Login panel as well as the informational and error messages issued while using the Login panel, such as wrong user or wrong password.

Below is an illustration of a Login panel in French where a wrong name has been entered:

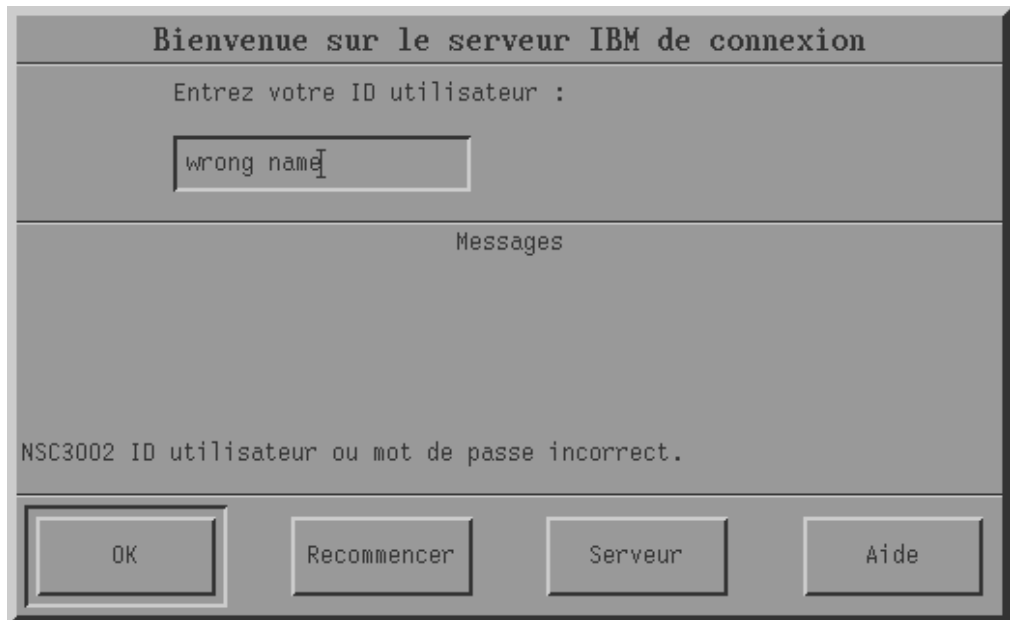


Figure 248. Login Panel, in French, for Wrong Password

### 16.5.2 How Is It Configured?

The login panel language cannot be configured using the IBM Network Station Manager; it can only be configured by adding a configuration statement to your configuration files.

For example, the statement to add in order to get a login screen in French is:

```
set unit-initial-locale = FR_FR
```

The locale is expressed as FR\_FR. See *IBM Network Station Manager Installation and Use, SC41-0664*, Appendix C, for a list of the locales supported by IBM Network Station Manager, or see the Language Setup Task of the IBM Network Station Manager.

If you wish to change this Login panel language for all stations, then you can add this statement to your defaults.dft configuration file. Otherwise, to change it on a per station basis, add it to your "name".trm file where name is the name chosen for the station.

---

## 16.6 The Kernel Environment Language

The kernel environment language concerns the locale used on the IBM Network Station itself, after the operating system (kernel) is in operation, and after the user login has completed.

### 16.6.1 What Does It Affect?

The kernel environment language affects such language-related settings as the format for dates, currency, numbers and the language of menus and messages.



Specifically, this applies to the menu bar on the IBM Network Station and the panels, prompts and error messages for the emulators. Some examples are illustrated below in French:



Figure 249. Sample Menu Bar, Prompt Panels and Error Messages in French


**Note:** The console and console messages, which a user should normally not see, remain in English.

### 16.6.2 How Is It Configured?

The kernel environment language is configured using the IBM Network Station Manager.

On the Setup Tasks list, select **Language** and then either **System Defaults**, **Group Defaults** or **User Defaults**. The panel illustrated below shows the language settings for a user called claudius, where French in Canada is the selected language.

- [Hardware](#)
- [Workstations](#)
- [Printers](#)
- [Startup](#)
- [Desktop](#)
- [5250](#)
- [3270](#)
- [Internet](#)
- [Language](#)
- [Select User's Group](#)
- [Main Screen](#)
- [Close IBM Network Station Manager](#)


**Language Settings for claudius**

---

**Format to use for dates, currency, numbers, and messages:**

FR\_CA--French in Canada

▼

(LANG)

**You can specify a different format for the items below:**

Date and time format:	<div style="border: 1px solid black; padding: 2px;">Default</div> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">▼</div>
Currency related format:	<div style="border: 1px solid black; padding: 2px;">Default</div> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">▼</div>
Numeric format:	<div style="border: 1px solid black; padding: 2px;">Default</div> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">▼</div>
Character handling rules:	<div style="border: 1px solid black; padding: 2px;">Default</div> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">▼</div>
Language for messages and menus:	<div style="border: 1px solid black; padding: 2px;">Default</div> <div style="border: 1px solid black; width: 20px; height: 20px; text-align: center; line-height: 20px;">▼</div>

Figure 250. The Language Settings for a User

In the panel above, you can select default settings for all formats, and then leave the value Default for the other five individual fields labeled Date and time format, etc., or you can override one or more specific entries by selecting an individual specification. For example, you might want all to be in French, but leave the messages in English, in which case you would override the last entry labeled Language for messages and menus with the value English.

### 16.6.3 Japanese Language Input Method

Notice that on the same IBM Network Station Manager Language settings screen, there are parameters that can be specified for Japanese language users in order to select an input method, as illustrated in the figure below:

**Input method information (for Japanese language users only)**

**Input method:**

Default

**Wnn6 input method options:**

Use default

**Jserver host name:**

☒

**Jserver port:**

☒

(1 - 65535)

**Wnn6 input manager port:**

☒

(1 - 65535)

Figure 251. Japanese Language Input Method

Please refer to *IBM Network Station - RS/6000 Notebook, SG24-2016*, Chapter 7 "National Language Support", for a description on how to use this input method.

#### 16.6.4 The NC Navigator

The NC Navigator is supported only in English, Japanese, Korean and German.



---

## Chapter 17. Connecting to Windows Applications Servers

It seems that you cannot discuss a network computer topic today without mentioning WinFrame, WinCenter or Windows Terminal Server Edition (previously known as Hydra), which are Windows application servers.

The reason for this is that it is rare to see a personal computer on a typical user's desk without some sort of Windows application such as a spreadsheet or word processor application.

An IBM Network Station therefore likely needs to have access to Windows applications, and since the IBM Network Station is not an Intel-based processor, it cannot run Windows applications natively. However, it can function as an X-terminal for example and have access to these Windows applications running and executing on a remote server.

The intent of this chapter is to provide the reader who is not already familiar with these products with a quick overview in order to understand what these Windows application servers are, and how they work, but more importantly how an IBM Network Station can connect to these application servers.

---

### 17.1 Windows Applications Servers

So, what is a Windows application server? A Windows application server is a machine that executes Windows applications on behalf of clients that cannot run these same applications on their own processor.

The client does not have to be a network computer, or an X-station, but it can be any machine, even one capable of executing Windows applications itself.

A typical case for example might be an old PC, with a slow processor and limited local storage capacity. This PC might be adequate to run a 3270 emulator for example, which requires little local storage and processing power but once in a while it needs to execute an application that requires a fast processor and large files.

In that case, the PC can take advantage of a Windows application server and connect to the server when this application needs to be executed.

This is also a good way of reducing the maintenance associated with these applications by making them available on a server; therefore, when it is time to upgrade these applications, it can more easily be done by upgrading a few servers rather than a much larger number of PCs.

However, in our specific discussion here we are more concerned with an IBM Network Station user, who does not have local storage and limited processor capability, or the ability to even execute Windows applications locally.

The diagram in the next figure illustrates this environment.

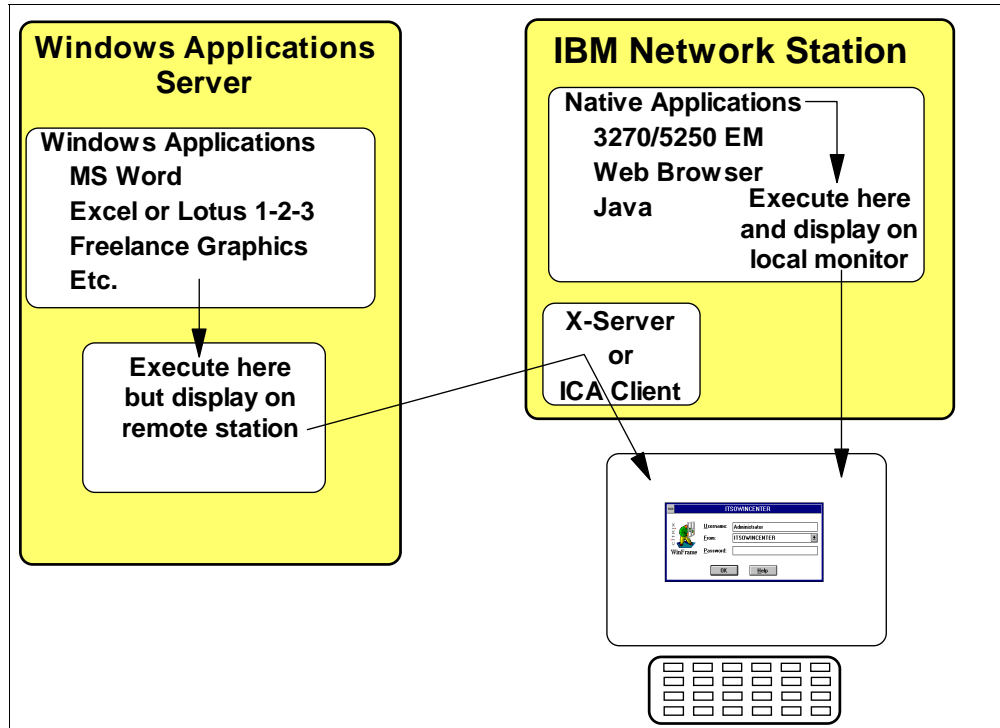


Figure 252. Local vs. Remote Application Execution

In the figure above, the IBM Network Station has some native applications that can execute locally on the IBM Network Station's processor. These are a 3270 and 5250 emulator, a Web browser and any Java application.

When these native applications are executed, they process on the local engine and display on the local IBM Network Station-attached monitor.

However, when the need comes to execute an Excel spreadsheet application for example, the IBM Network Station can use a local client called an X-server or an IICA client to connect into a Windows applications server and trigger the execution of the spreadsheet application on the remote server.

This client, together with its counterpart running on the server, has the ability to redirect input and output to the display, mouse and keyboard attached to the IBM Network Station.

In effect therefore, the user at the station sees on his or her display a normal Windows desktop, and runs applications just as if his or her mouse, keyboard and display were attached to the server itself.

This brings up an interesting point, which is the fact that a Windows machine is normally a single-user machine, from the point of view of executing an application. An NT server for example can certainly have many network users connecting in to share file and printer resources, but actually executing applications requires a multi-user environment, which is not typical of a Windows machine.

Therefore, these Windows application servers are in fact multi-user versions of a Windows NT operating system.

There are many flavors of the Windows application servers and a few types of protocols and clients that can be used to connect to these servers, so we now briefly review and explain these different flavors.

## 17.2 What Is WinFrame?

WinFrame is a product from Citrix, which consists of a Microsoft's Windows NT 3.51 base operating system that has been modified to function as a multi-user version.

In other words, when a server runs the WinFrame operating system, multiple users can connect into this server and all appear to be using the Windows NT desktop as if they were the only user.

To connect into WinFrame, users (clients) use a proprietary protocol called the Independent Computing Architecture (ICA) to connect their PCs into the WinFrame server.

The figure below illustrates the multi-user capability provided by WinFrame.

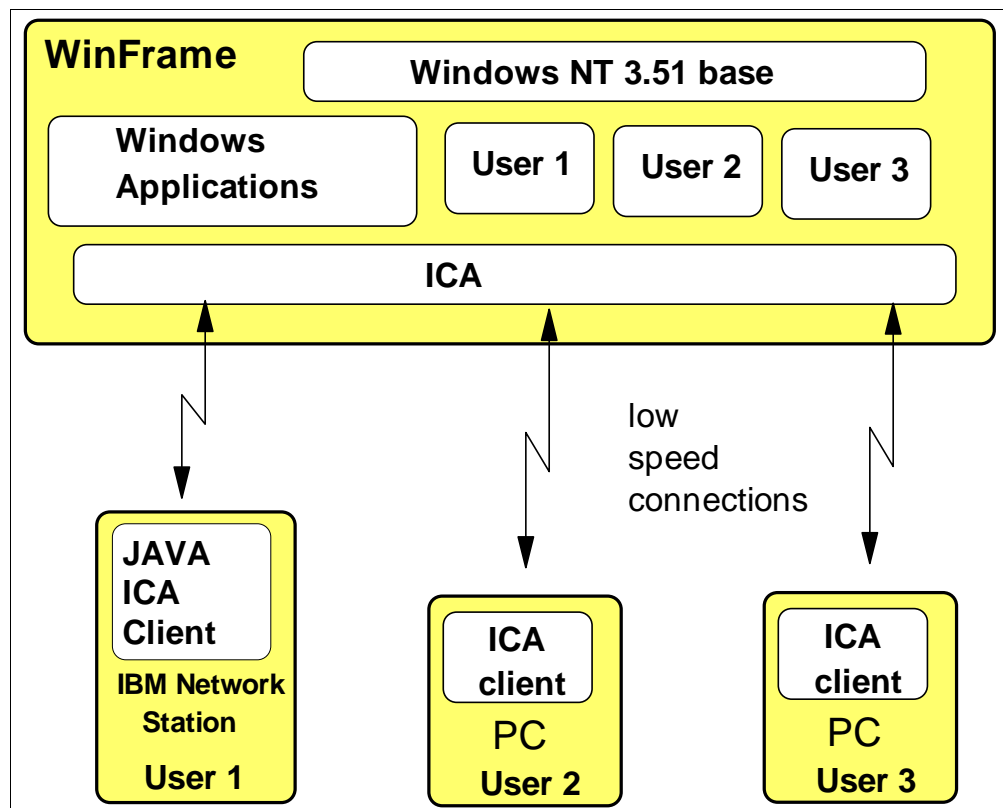


Figure 253. The WinFrame Product

Prior to IBM Network Station Manager Release 3, the IBM Network Station did not have a native ICA client that could be used to connect to a WinFrame server. As we see in the next diagram, the IBM Network Station was using an X-server function to connect such a server. However, Citrix does have a Java-based ICA client available that can run on the IBM Network Station since the station can run Java applications.

### 17.3 What Is WinCenter Connect?

The ICA protocol used by clients to connect into the WinFrame server was designed primarily for use over low-speed connections. If one wants to connect clients over high-speed LAN connections then another product, called WinCenter Connect, from NCD Inc., is needed in addition to WinFrame.

This is illustrated in the next figure:

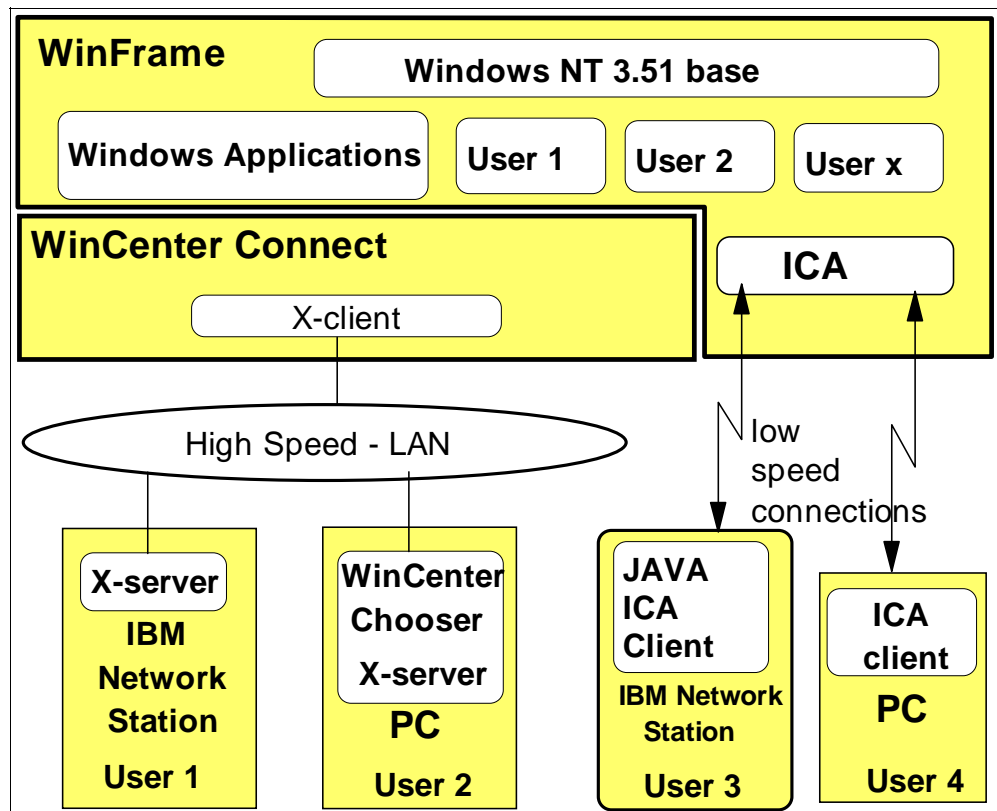


Figure 254. WinCenter Connect

In the figure above, a product called WinCenter Connect is added to the WinFrame product in order to provide clients the ability to use the X.11 protocol to connect into the WinFrame server. This provides any machine that can function as an X-station with the way to connect into WinFrame.

In the figure above, we show that the IBM Network Station's X-server capability provides the way to connect to WinFrame. A WinCenter Chooser application can also be installed on PCs to provide an X-server capability.

#### 17.3.1 What Is WinCenter?

If a user wants to get all the products above (Windows NT 3.51 from Microsoft, WinFrame from Citrix and WinCenter Connect from NCD) as one product, this is available as WinCenter, which is a product from NCD Inc.

In summary, what the WinCenter product really provides is the support of the X.11 protocol for X-stations to interface into the WinFrame multi-user Windows NT system.



## 17.4 Windows NT 4.0 - Terminal Server Edition (WTSE)

The Citrix WinFrame product was based on Windows NT 3.51. For Windows NT 4.0, the same multi-user functionality is now provided by Microsoft in a special version of Windows NT 4.0 Server called the Terminal Server Edition.

This has been known for some time now, while in development, under the code name of Hydra, and is commonly referred to as Windows Terminal Server (WTS or Windows Terminal Server Edition (WTSE). We often use the WTS or WTSE acronyms in this document to refer to Windows NT Server 4.0, Terminal Server Edition.

What Windows Terminal Server brings is the same multi-user functionality that was provided by WinFrame, but at the Windows NT 4.0 level and an additional protocol to connect into the server called the Remote Desktop Protocol (RDP), which is the protocol used by Windows terminals.

The ICA functionality provided by Citrix's ICA protocol is still available but requires the addition of Citrix's MetaFrame product to WTS.

In addition, if the X.11 functionality is desired, then NCD's UNIX Integration Services is required in addition to MetaFrame.

This structure is illustrated in the next figure:

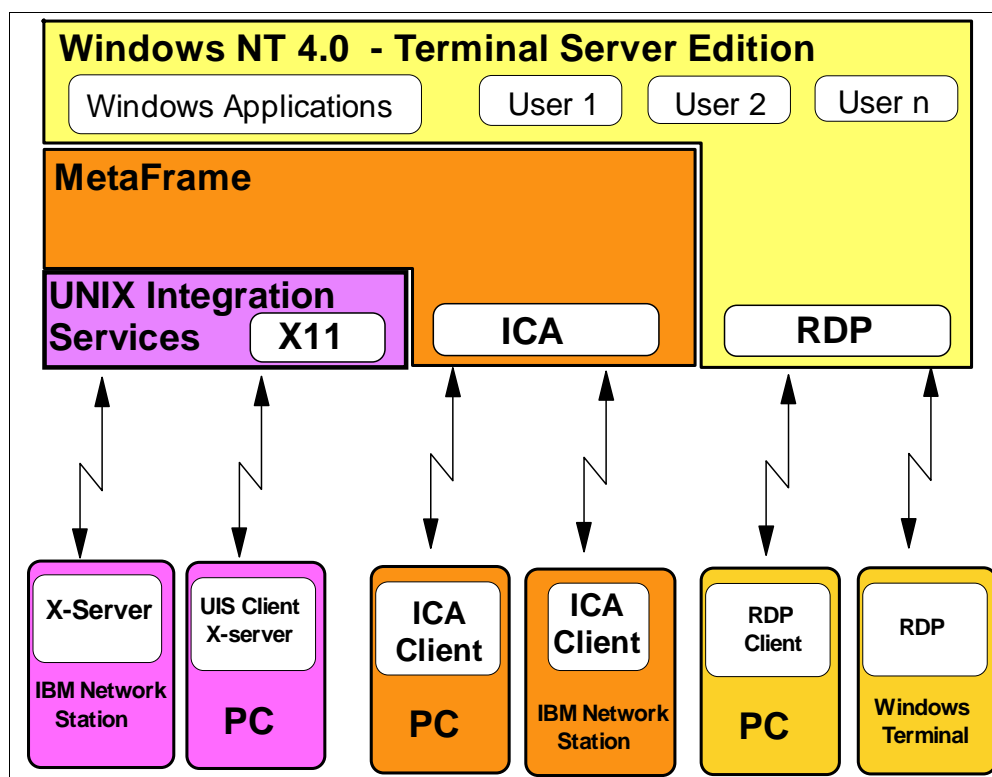


Figure 255. Windows NT 4.0 - Terminal Server Edition

In summary:

- Any terminal that supports the RDP protocol can connect directly into the Windows Terminal Server.
- Any terminal using the ICA protocol requires that the Citrix MetaFrame product be also installed on the Windows Terminal Server.
- Any terminal using the X.11 protocol requires that both Citrix's MetaFrame and NCD's UNIX Integration Services products be installed on the Windows Terminal Server.

---

## 17.5 Connecting an IBM Network Station to Windows Terminal Server

As summarized above, there are three protocols available to connect into a Windows Terminal Server:

- RDP
- ICA
- X.11

The IBM Network Station supports only the last two of these protocols: either the ICA protocol, using a native ICA client executing on the IBM Network Station, which is new with Release 3, or the X.11 protocol using the native X-server functionality as in previous releases.

### 17.5.1 Using Microsoft's Remote Desktop Protocol (RDP)

Even though the IBM Network Station does not support the RDP protocol, if you have the administration responsibility of a Windows Terminal Server, it is likely that you want to connect using any of your other available machines, so here we give a brief description of the RDP client on a PC.

The RDP client can be installed on PCs running Windows 95, Windows NT and Windows for workgroup.

It can be installed:

- From the network, by the client connecting into a shared drive on the WTS server at \\wtsrv\System32\Clients\Tsclients\Net and executing the proper setup.exe.
- From a diskette. This diskette is created on the WTS server using the Terminal Server Client Creator Utility, illustrated below, which is started by selecting **Start=>Programs=>Administrative Tools=>Terminal Server Client Creator**.

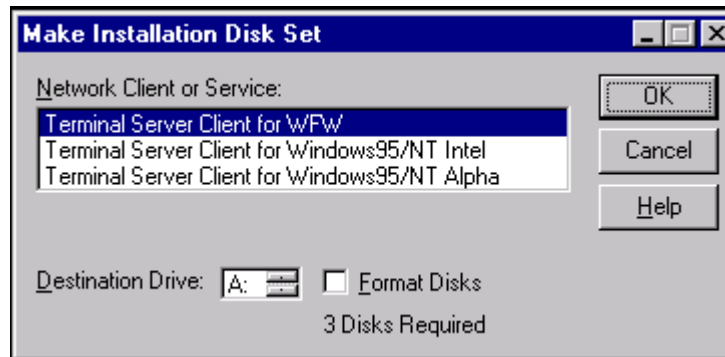


Figure 256. Terminal Server Client Creator

After installation of the client, select **Start=>Programs=>MS Terminal Server Client** as illustrated below:

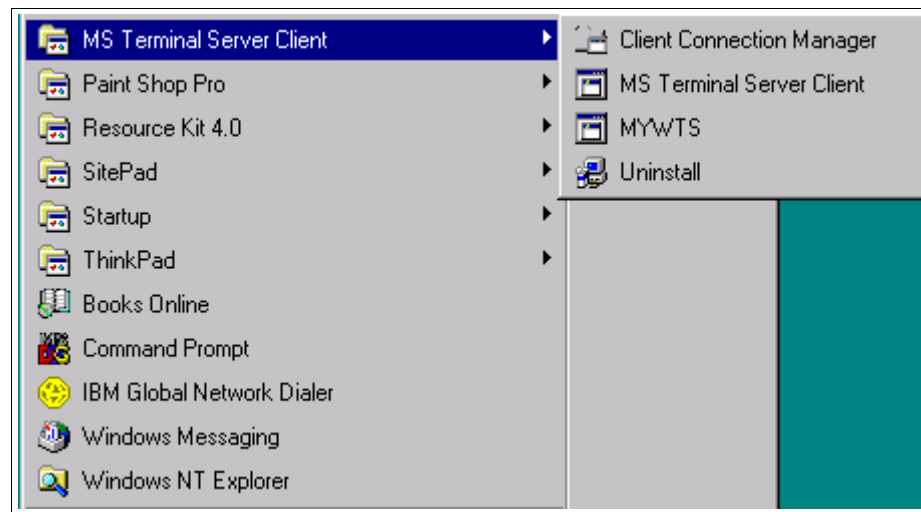


Figure 257. Installed Terminal Server Client Shortcuts

If you just want to start a connection to a WTS server, you can click on **MS Terminal Server Client**, which brings up the panel shown below, where you enter the IP address or name of the target server, the resolution that you want to use for the display session, and click on **Connect**.

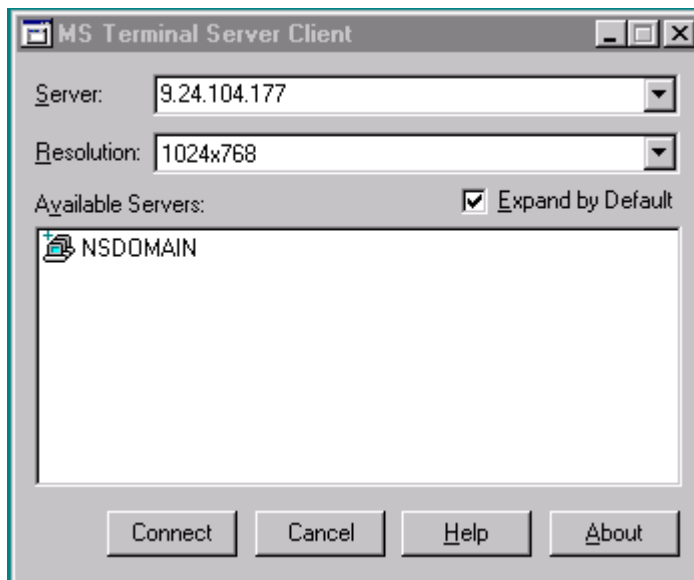


Figure 258. MS Terminal Server Client Panel

If you want to pre-define some connections in order not to have to specify a server and resolution every time you need a connection, especially to different servers, then use the Client Connection Manager.

In the next figure is shown the Client Connection Manager where we have already defined a connection called MYWTS.



Figure 259. Client Connection Manager

In addition to being shown as an icon here, MYWTS is also added to the Start=>Programs shortcuts, as can be seen in Figure 257 on page 283. You can also create a shortcut on the desktop for this connection by clicking with the right mouse button after selecting the connection icon.

If you select the MYWTS connection, right click and select **Properties**, the following three panels show the characteristics of this connection definition.

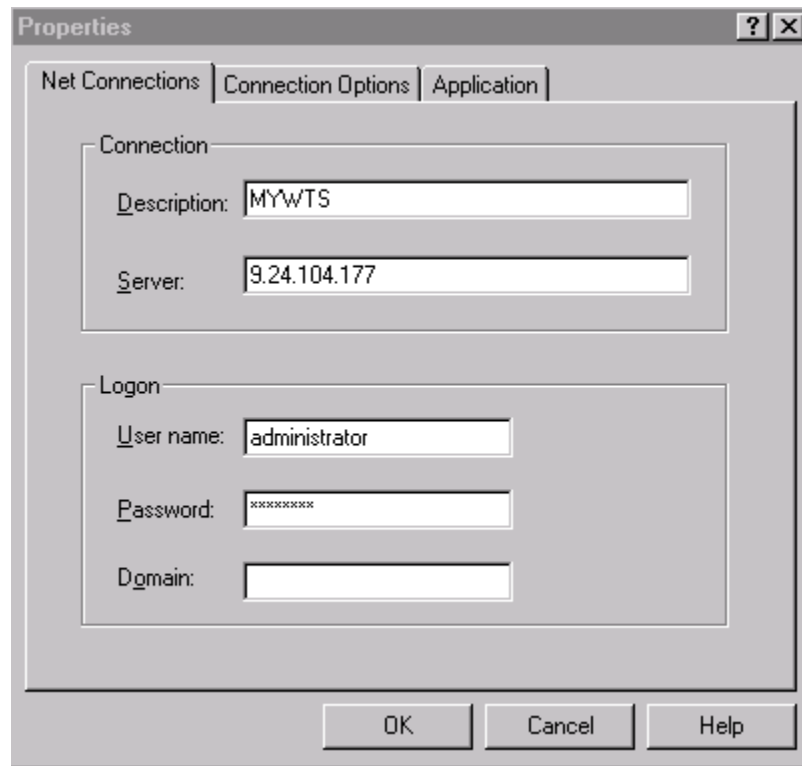


Figure 260. Connection Details

In the panel above, you can specify the name and password to be used when connecting so that you are not presented with a logon panel.

In the next panel, you can specify the resolution for the display session, and whether you want the session full screen or in a window.

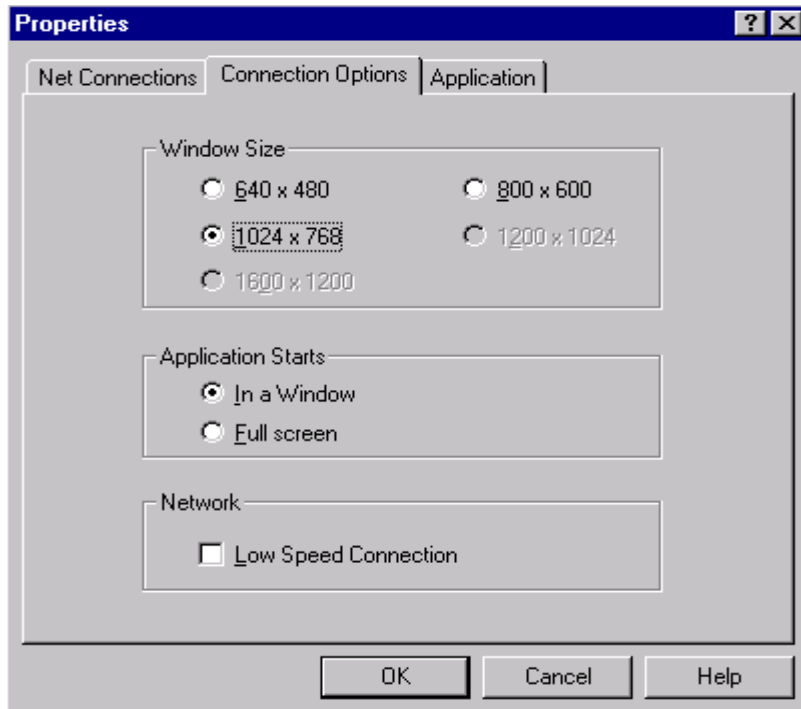


Figure 261. Connection Options

If you use the same resolution as you have on your display, the session window has scroll bars, which can be annoying; however, at any time, you can use the Ctl+Alt+Break key sequence to toggle between full-screen mode and window mode.

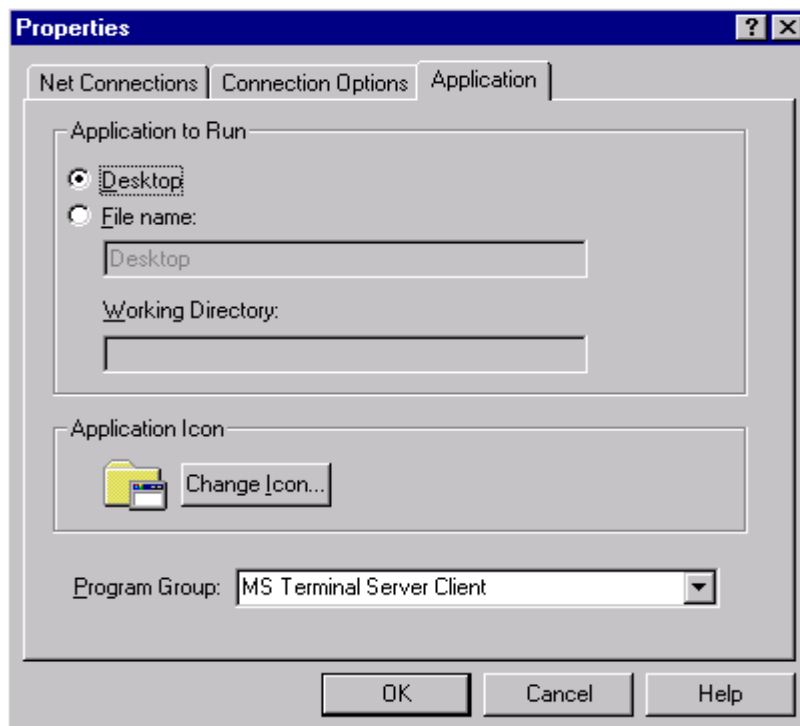


Figure 262. Application Selection

By default, after the logon to WTS, the user gets the normal Windows NT desktop. You can change this to execute a specific application by using the tab labeled Application and specifying a path and executable to be started.

Here you can also change the icon associated with that connection and put the connection (in this case MYWTS) into a folder other than the default Program Group called MS Terminal Server Client.

---

## 17.6 Connect Using ICA

Release 3 now includes a local client called ICACLNT that can be used to connect to a MetaFrame (or WinFrame) server using Citrix's Independent Computing Architecture (ICA) protocol.

This includes connecting to MetaFrame Enterprise Edition, MetaFrame for workgroups and MetaFrame Terminal Edition.

Prior to Release 3, there was a Java-based ICA client that could be used as well to connect to a WinFrame server.

Today, with R3, there are a few methods to use the ICA protocol to establish a session with a MetaFrame or WinFrame server, for example:

1. Define a button on the menu bar that the user can use to trigger the establishment of a session to a specific host.

Of course, you can set up multiple buttons if there are multiple hosts that can be chosen by a user, but a better solution then would be to use the ICA Chooser application, which we describe further on.

If there are multiple hosts as potential targets, and they are set up as load balanced servers, you can set it up with only one host target and use the load balanced option to let the system decide which server to connect the session to.

2. Autostart a session to a specific host.

If you want a session to appear automatically, you can then autostart it, but it is also preferable to have a menu bar button to restart it in case the user terminates the session. Here again, the ICA Chooser may be the best way to set this up.

3. Use an ICA Chooser application that displays a list of hosts that the user can choose from. The ICA Chooser application itself can be autostarted if you want the list to appear automatically.

4. Define the station in kiosk mode in order to automatically bring up a session to a particular host.

Even in this case, you can set it up so that the ICA Chooser also appears on the desktop allowing the user to restart a session or to choose different hosts.

Let us examine each of these methods.

### 17.6.1 Define a Menu Bar Item for an ICA Connection

Use IBM Network Station Manager, in the Startup tasks, and define a local program menu item as illustrated in the next figure.



### Local Program Menu Items

Menu item label	Program to run	Parameters
ICA-ITSOWTS	ICACLNT	-host itsowts -colors 16

Figure 263. Configuring an ICA Client

The program to run is called ICACLNT and here we specify the -host parameter to indicate the target host and the -colors 16 to ensure no color flashing.

The usage of the icacInt command is:

```
icacInt [-host hostname] [-options ...] [-- command args]
-help          <print out this message>
-ca[che]       <large cache size in KB>
-c[olor]       <16 | 256 color>
-g[eometry]    <WidthxHeight>
-ti[tle]       <window name>
-na[me]        <client name>
-lb           <request load balancing>
- -           <application to be started>

-username     <user name>  ** Undocumented **
-password     <password>   ** Undocumented **
-domain       <domain name> ** Undocumented **
```

Figure 264. The icacInt Command Usage

In the above command, notice the following:

- The -geometry parameter is used to specify the size of the window for the session. See 17.7.1.3, “The Geometry and Resolution Parameters” on page 296 for more details.
- The -title parameter allows you to specify the name that appears in the window’s title bar when the WTS session is displayed on the desktop.
- The -name parameter allows you to set the CLIENTNAME variable on the host. For example, if you specify -name \${IP}, the IP variable on the IBM Network Station is replaced by the IP address of the station, for example 9.24.104.189.

This is transmitted to the MetaFrame host at session establishment, causing the CLIENTNAME variable, on the MetaFrame host, to be set to the value 9.24.104.189. You can then issue a command from your MetaFrame session, such as RSH %clientname% show version for example, which will cause the Version screen to appear on your station’s display.

This is used as a way to have generic commands issued in a MetaFrame session to apply to any client. This is similar to using the WCPRSH command from a WinCenter host as described in 17.8, “Issuing IBM Network Station Commands from a Windows Desktop” on page 299.



- The `-lb` parameter indicates that load balancing is required for that session.

The client contacts the host to find out which host is acting as the *master*, it then connects to the master host to find out which host it should use to run the application and finally connects to the designated host. This particular function was added in version 3.02 of NSM.

- The `--` parameter allows you to specify the application that should be started when connecting to the Windows Application Server. For example, if we want to start the PFE editor located in `d:\tools`, we specify `-- d:\\tools\\pfe32.exe`, a backslash (and a few other special characters like `$`, `*`, `#` and `?`) must be preceded by another backslash to indicate that it is a special character.

On the X11 command, the equivalent parameter is the `-exec` parameter, although `--` also seems to be accepted by X.11.

**Note:** Notice that there are also three undocumented parameters. These undocumented parameters are not supported at this time (at the NSM Release 3.02 level) and you should therefore not expect them to work. However, the `username` and `password` parameters do work (Release 3.02 level); the `-password` does not. This will need to be fixed by the next update.

- The `-username` parameter is undocumented. It is not listed when doing a `-help` on the `icacnt` command but it is accepted and it works. To pass the same user name that was used to log in to the IBM Network Station, use the `-username ${USER}` form, since the `USER` environment variable name contains the user name that was used on the IBM Network Station login panel.
- The `-domain` parameter is undocumented. It is not listed when doing a `-help` on the `icacnt` command but it is accepted by the command.
- The `-password` parameter is undocumented. It is not listed when doing a `-help` on the `icacnt` command but it is accepted by the command; however, this parameter does not work at the moment (Release 3.02), with the `icacnt` command.

However, this parameter does work properly with both the `wincenter` and the X11 command. (See 17.7, “Using NCD’s UNIX Integration Services (UIS) for X.11 Connections” on page 293 for use of the `wincenter` and X.11 commands.)

**Note:** At this time, you can no longer specify the `${PASSWORD}` variable on the `-password` parameter because this environment variable is no longer available in NSM Release 3. We were unable to find out if this variable will be reinstated or if a workaround will be available to provide a similar functionality.

## 17.6.2 Using an Autostarted Session

This is similar to creating a menu bar item except that you use the Programs Setup task in NSM rather than the Menu task.

## 17.6.3 Using the ICA Chooser Application

If you have more than one host that users can choose, the best way to set it up is to use the ICA Chooser application.

Here again, you can have the ICA Chooser application started from a menu bar item or simply autostarted.

The next figure illustrates the ICA Chooser panel as it is displayed to the user. In this example, we have three hosts that the user can choose from, which we named itsowts, itsowts2 and itswincenter.

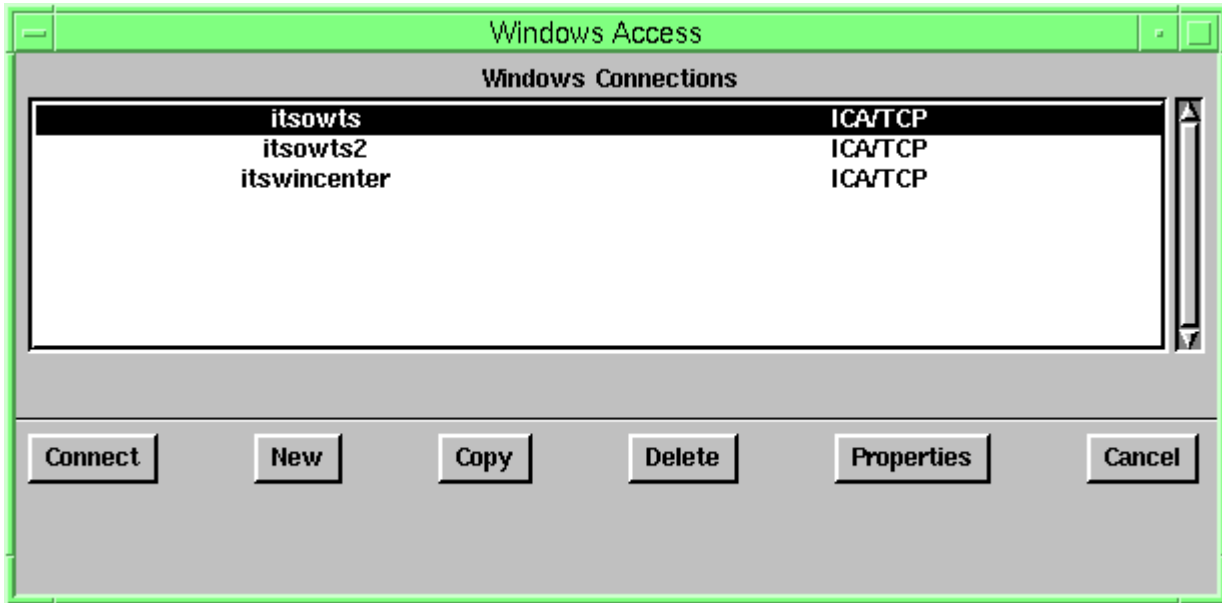


Figure 265. ICA Chooser Panel

To start this chooser application, you use the ICAUI command without any parameters, as illustrated below:

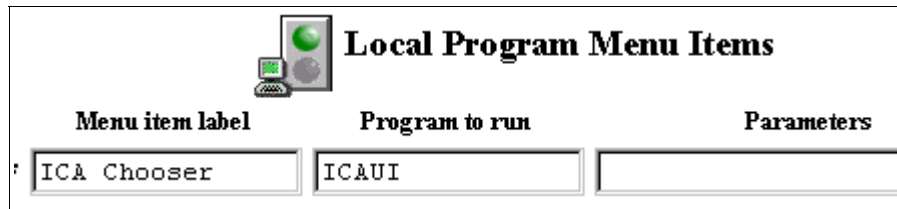


Figure 266. Defining an ICA Chooser Menu Item

The entries that appear in the ICA Chooser window however cannot be set in NSM. You must use the `ica-chooser-entries` parameter in the `defaults.dft` file. The next figure illustrates the parameters that were used to display the entries shown in the ICA Chooser panel above.

```
set ica-chooser-entries = {
  { "-ti itsowts -h 9.24.104.240 -c 16 -ty tcp -g 1024x768 -ca 2048" }
  { "-ti itsowts2 -h 9.24.104.177 -c 16 -ty tcp -g 1024x768 -ca 2048" }
  { "-ti itswincenter -h 9.24.104.178 -c 16 -ty tcp -g 1024x768 -ca 2048" }
}
set ica-enable-chooser-editing = true
```

Figure 267. `ica-chooser-entries` Parameter in `defaults.dft`

If you select an entry on the ICA Chooser panel, and click on **Properties**, the panel illustrated in the next figure is displayed, showing the characteristics that were specified in the set ica-chooser-entries parameter.

If you want the user to be able to modify these specifications from this panel, you must set the set ica-enable-chooser-editing parameter to true, as we did in this example. To prevent users from altering these entries, set this parameter to false.

Note that any changes made by the user are only temporary until the next time they log out or reboot.

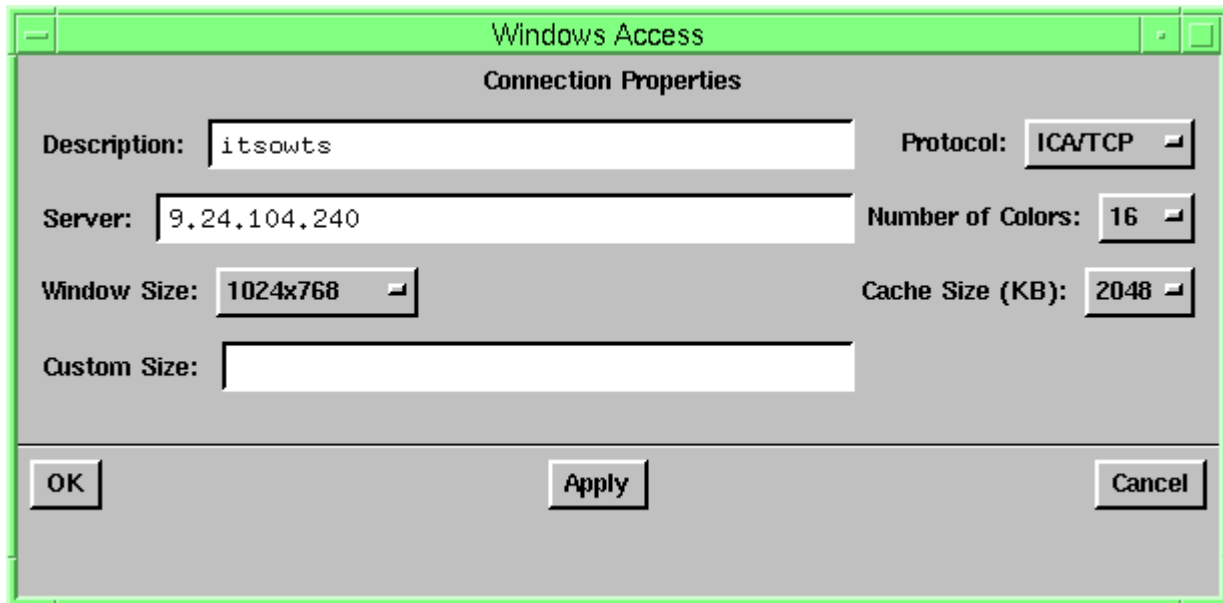


Figure 268. ICA Chooser - Properties

If you disconnect from a session, instead of logging off, and reconnect to a session using a different resolution than you had before (as the same user ID), you get a message indicating that the video mode is different, and asking if you want another session to be started.

The panel shown in the next figure is displayed at the time that you are trying to log back on, and you are offered a choice between the disconnected sessions.

If these sessions are no longer valid, the administrator can get rid of these by using the MetaFrame Administration application or the Terminal Server Administration applications.

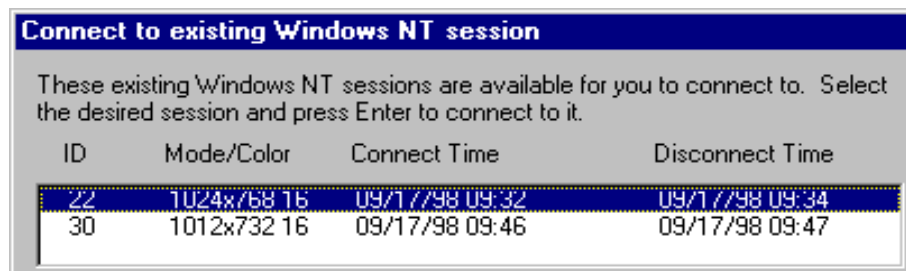


Figure 269. Existing Disconnected Sessions

#### 17.6.4 Using the Kiosk Mode

See the Chapter 12, "Full-Screen Solutions" on page 215 for more details on how to set up for kiosk mode, but here is a summary of the steps required:

1. Create your kiosk user ID on the server and add it to the NSM user group.
2. Using NSM, for this kiosk user ID, disable the window manager, remove the menu bar, and optionally set the desktop background to black.
3. Using NSM, for this kiosk user ID, autostart the ICAUI and an ICACLNT session as well if desired.
4. Add this kiosk user ID and password to the kiosks.source file and run the nsmkiosk utility to encoded it into the kiosks.nsl file.

When the station is rebooted, the ICA Chooser appears and also the ICA Session if you autostarted a specific one.

The proper way to terminate the ICA session is to log off, which clears the desktop and only the ICA chooser remains. From the chooser, you can then start the same session or another session (assuming of course that these sessions are displayed in the chooser panel).

You can use the Alt+F4 key combination to close the session that is currently in focus also. If you do this before you log on to the MetaFrame server, the session disappears and you get the ICA chooser back. If you use Alt+F4 before you log off, you are reminded to log off the session with the typical NT panel that you get when you hit Ctl+Alt+Delete in your NT session.

##### Note

If you use Alt+F4 on the ICA Chooser itself, it has no effect, but if you use the Cancel button on the ICA Chooser, the application terminates and you must then reboot in order to get it back.

By default, the kiosk user ID appears in the username field on the WinCenter logon panel. If you do not want this name to appear, use the -username parameter to specify any other name such as -username Name.

#### 17.6.5 Keyboard Support - ICA

The following keyboards are supported when using ICA:

- Belgian French
- Danish
- English UK
- English US
- French
- German
- Norwegian
- Swedish/Finnish
- Swiss French
- Swiss German
- Belgian Dutch

- Czech
- Dutch
- Hungarian
- Italian
- Polish (214)
- Polish Pmgr (457)
- Portuguese (not Brazilian Portuguese)
- Russian
- Russian Cyrillic
- Spanish (not LA Spanish)
- Swiss Italian
- Turkish (F & Q)

## 17.7 Using NCD's UNIX Integration Services (UIS) for X.11 Connections

The prerequisite to use X.11 as a protocol is that NCD's UNIX Integration Services (UIS) be installed, in addition to MetaFrame, on the WTSE system.

Once UIS is installed, there are a couple of ways to establish a connection to Windows NT Server 4.0, Terminal Server Edition using the X.11 protocol. We discuss these ways in the following sections.


### 17.7.1 Using a Remote Program Menu Item (RSH Command)

The first method is to use NSM to configure a Remote Program Menu item, which in fact generates an RSH command to be issued from the IBM Network Station when the menu bar item is clicked. The RSH command causes the execution of the X11 command on the remote MetaFrame server.

Instead of a menu bar item, this can be done also by autostarting a session.

In the example illustrated in the next figure we define two menu bar buttons, one that uses the X11 command and the other that uses the wincenter command, which was the command used in the case of a WinCenter server.

The wincenter command is accepted by UIS on WTS as well as by a WinCenter Server and the parameters on both are fairly similar.


**Remote Program Menu Items**

Menu item label	Remote host	Program to run	Optional parameters
ITSOWTS-wincente	itsowts	wincenter	-geometry 1012x732 -colors
ITSOWTS-RSH	itsowts	x11	-resolution 1012x732 -disp

Figure 270. Defining an X.11 Connection

In the example above, the first menu item labeled ITSOWTS goes to the remote host itsowts, which is our MetaFrame server, and uses the wincenter command and the -geometry parameter to get a full-screen session and the -colors 16 parameter.

### 17.7.1.1 Using the X11 Command

The X11 command has the following options that can be specified. The output below is generated by issuing X11 -help. Please consult the online documentation for additional details.

```
rsh output = Usage for connecting to Unix Integration Services is:
```

[-colors <num>]	Number of colors
[-depth <bitdepth>]	Pixel color bit depth
[-display <displayname>]	Display to use
[-domain <name>]	Domain name to logon to
[-exec <pathname>]	Pathname of application to run
[-execwd <directory>]	Working directory for application
[-geometry <geometry>]	Frame geometry (size and/or offset)
[-help or -?]	Display this message
[-icorsh output = nic]	Iconify session initially
[-keybd <mapfile>]	Keyboard mapping file
[-lang <keyboard language>]	Keyboard language
[-new_session]	Always create a new session
[-mcookie <magic cookie>]	Magic Cookie authentication code
[-password <password>]	Password
[-resolution <resolution>]	Screen resolution
[-same_session]	Always use existing session
[-user <name>]	User name to logon with
[-shadow <session>]	rsh output=Shadow an X11 WinStation

If -exec is specified, it must be the last parameter.

Examples:

```
rsh server x11 -display my_xserver -res 640x480 -depth 8
```

Figure 271. The X11 Command Options

In the example above, we defined a menu item called ITSOWTS-RSH where we used the X11 command with the following parameters:

```
-resolution 1012x732 -display ${IP}:0
```

### 17.7.1.2 Using the wincenter Command for an X Session

The wincenter command has the following format and parameters:

```
wincenter -display displayname [optional arguments][-- initial program]
```

Optional arguments include:

```
-geometry geometry_spec
-depth depth
-bw border_width
-colors num_colors
-resolution frame_resolution
-username username
-password password
-domain domain
-auth host name data
-working_directory working_directory
-noaudio
-keymapfile keyboard_file
-wan
-version
-image {none(off), minimal, good, better(on), best}
-bs {none(off), mapped(on), always, default}
-fs
-nofs
-wincursor
-cache DIB cache size
-balance
-encryption {off, login(on), always}
-netsaver {on, off, (low,high)}
-serial serial_daemon_port
```

Figure 272. The wincenter Command

For example, we can use the following command:

```
Wincenter -display ${IP}:0 -colors 16 -geometry 1012x732
```



Figure 273. A WinCenter Menu Item

Here is a brief explanation of some of these parameters:

- The -display \${IP}:0 parameter indicates where the WinCenter server should send the display output. At the time that the command is issued, the variable IP is replaced with the IP address of the station that issues the command.
- The -colors 16 parameter avoids some of the color flashing, which causes the menu bar to turn black.

**Note:** There are still some potential color problems if the NC Navigator browser is started before the WinCenter session.

- The `-geometry 10125x732` (`-geometry width x height`) parameter specifies the size and location of the window in which the WinCenter desktop is to be displayed. Even though the resolution used in this example is 1024x768, a specification of widthxheight slightly less than this must be used. This is discovered by trial and error.

What this will do is ensure that the WinCenter desktop covers the entire screen without any scroll bars. If you specify 1024x768, or the word full-screen, you still get scroll bars to appear in the window.

### 17.7.1.3 The Geometry and Resolution Parameters

To provide a better explanation of how the geometry and resolution parameters work, here are a few illustrations of their use.

In the figure below, the geometry parameter indicates the size and location of the window in which the WinCenter desktop is displayed. In the first case, when `-geometry 800x600-100-100` (`-geometry width x height -xoffset -yoffset`) is specified, the window is in the top left-hand corner. If `-geometry 800x600-300-300` is specified instead, the window is located in the bottom right-hand corner. One has to play with the values, on a trial and error basis in order to find out exactly where the window will be positioned dependent on the value of the x and y offset specifications.

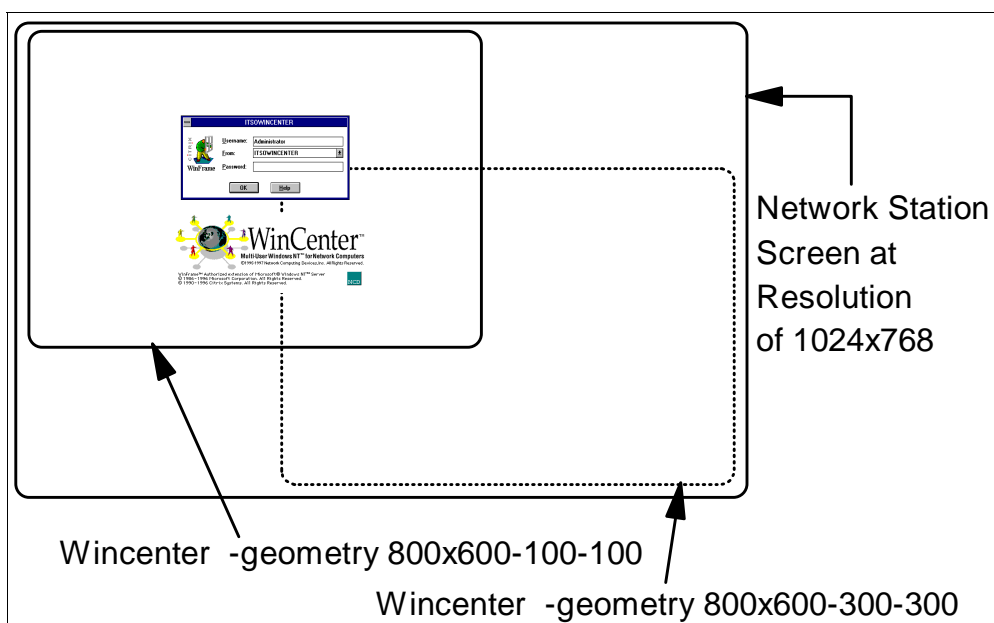


Figure 274. Geometry Parameter Example

In the next figure we use the resolution parameter (`-resolution width x height -xoffset -yoffset`), in addition to the geometry parameter, to specify the size and location of the WinCenter display. The x and y offsets are the number of pixels from the top left-hand corner of the screen.

Given that our IBM Network Station screen is set at a resolution of 1024x768, we use `-geometry 800x600 -resolution 1024x768`. Since the resolution we ask for is greater than the size of the window, we get scroll bars.



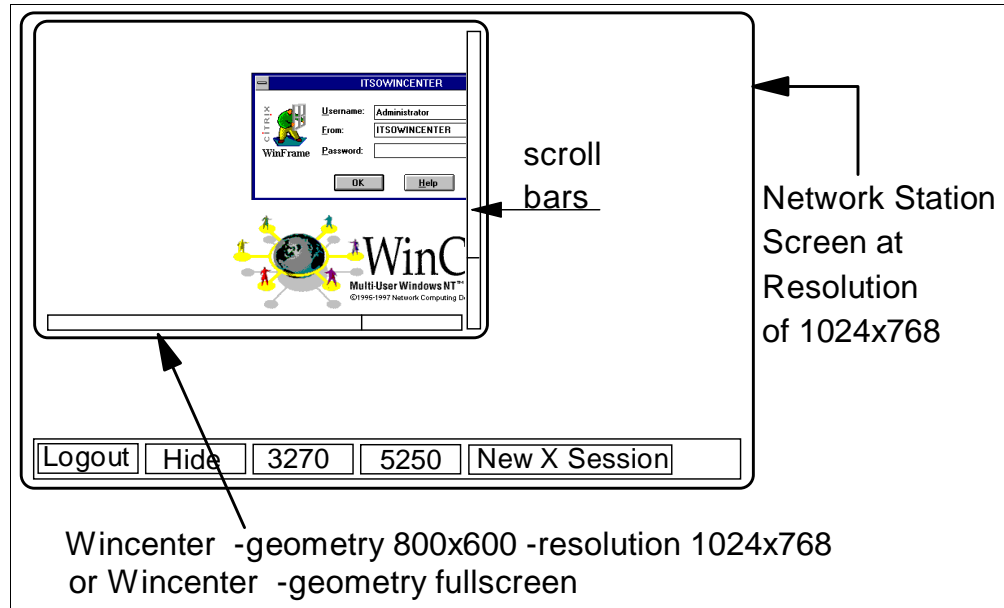


Figure 275. Resolution Parameter Example

In the next figure, with the IBM Network Station screen resolution still at 1024x768, we now specify -geometry 1005x725, (in fact somewhere between 1005x725 and 1012x732 on our test system) the result of which is a full-screen display without any scroll bars, which is typically the effect that we desire, especially when working only with a WinCenter desktop. The resolution parameter not being specified, it assumes the same defaults as the geometry parameter.

**Note:** If the WinCenter window manager is used instead of the local window manager, a specification of 1024x768 (or full-screen) is required to cover the entire display area. In this case, the menu bar is still available, and when shown, overlays the bottom (or top) portion of the display.

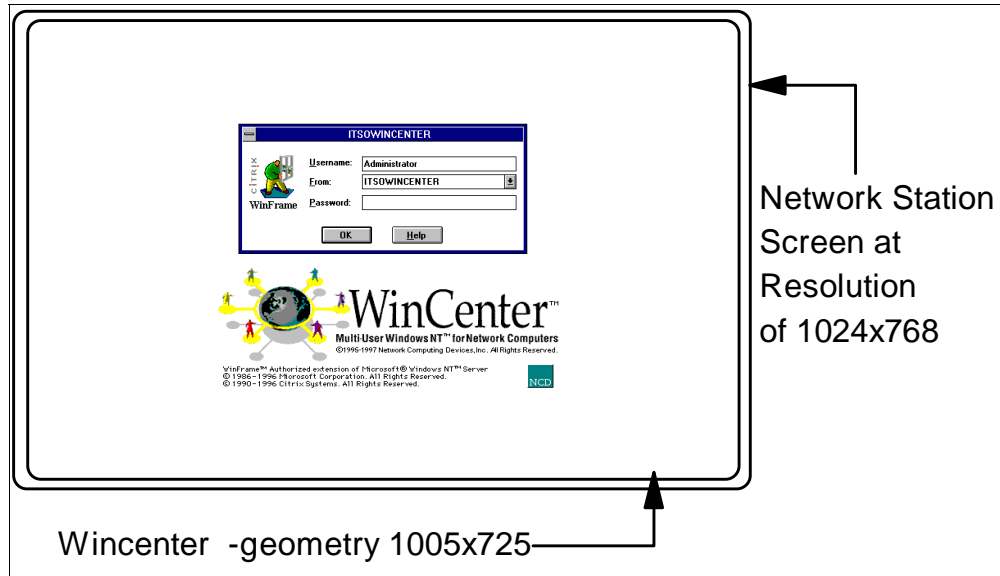


Figure 276. Resolution Parameter Example 2

#### 17.7.1.4 Using the Login Chooser

The second method is the IBM Network Station Login Chooser application.

The Login Chooser application can be started using the console, and selecting **Login New X Session...** on the Login pull-down, assuming that this has been enabled on the console.

**Note:** In the previous release, you were allowed to start the Login Chooser without shutting down the local window manager. In Release 3, you cannot start the Login Chooser without first shutting down the local window manager.

When the application is called, it issues a broadcast asking all hosts that are capable of supplying an X-session to respond. All hosts that do respond are listed (this is a configurable option) in the Login Chooser window, from where the user can select one. See 5.2.6, "Login" on page 133 for an example of a chooser window.

Typically, these hosts would be AIX systems. However, a WinCenter server or a MetaFrame server with UIS is also a host capable of supplying an X-session, and normally responds to the broadcast request made by the Login Chooser application.

The user then only needs to select the host listed in the chooser screens to initiate a connection to that host. Note that since this list is obtained from a broadcast request, only the hosts on the local LAN segment would respond as broadcasts are normally not crossing any routers or bridges.

The login command can also be issued from a menu button, with a destination host, but this assumes that you already have the Window Manager stopped. This can certainly be used though as an autostarted session in kiosk mode where the Window Manager has already been disabled.

## **17.7.2 Local Window Manager or WinCenter Window Manager?**

There is a choice here of using either the local IBM Network Station window manager or the WinCenter window manager. Which one is the best to use is more a question of preference.

### **17.7.2.1 Using the Local Window Manager**

The local window manager runs locally on the IBM Network Station and therefore requires less network bandwidth to operate. All applications such as emulators and browsers are displayed in windows with title bars and scroll bars and they can be moved, sized and minimized in the traditional fashion. A WinCenter desktop is displayed in a window just like the other local applications and behaves in the same fashion.

When windows are minimized, they appear as icons on the station's desktop.

If a session is maximized, it must be reduced or minimized in order to have access to the other active windows.

### **17.7.2.2 Using the WinCenter Window Manager**

If the WinCenter server window manager is used instead, it requires a greater amount of network bandwidth since all windows are effectively controlled by the server.

However, since all the windows on the IBM Network Station are managed by this window manager, the station must always have a WinCenter session active to manage all the other stations's application windows.

When using the WinCenter window manager, all application windows are minimized to the WinCenter desktop. There is no need to minimize or reduce the WinCenter window itself to get access to the other minimized icons since they appear on the WinCenter desktop.

If you require the NC Navigator browser started, it should be started after the WinCenter session is started in order to avoid color problems.

---

## **17.8 Issuing IBM Network Station Commands from a Windows Desktop**

When operating in kiosk mode, the user (in theory) does not have access to any of the IBM Network Station facilities since we disabled the menu bar.

If there are some of these facilities however that you want to provide to users, such as the Lock Screen function, you can cause a command execution on the IBM Network Station from the user's Windows desktop by issuing an RSH command with the IBM Network Station as the target.

For this to be possible, the IBM Network Station configuration must be set up to allow remote command execution. See 19.4.8, "Remote Command Execution Access" on page 376 and 19.5, "Launching Commands from a Remote Host" on page 376 for additional details on how to allow and cause remote command execution.

The way to accomplish this is to use, from the Windows desktop, an RSH command back to the IBM Network Station.

### 17.8.1 From a WinCenter Desktop

WinCenter provides for that purpose a command called `wcprsh`, the format of which is as follows:

```
WCPRSH [options] hostname command
```

Where options:

- `-l` username

Use username as the remote user name instead of your local user name.

- `-x`

Do not show an output window.

The following variables can be used in a command:

- `%display%`

The display name of the WinCenter client

- `%client%`

The name of the WinCenter client

- `%server%`

The name of the WinCenter server

For example, the following command issued on the WinCenter desktop is equivalent to the user using the lock function on the IBM Network Station console:

```
wcprsh -x %client% lock
```

Another example might be a command to start a 3270 emulator:

```
wcprsh -x %client% ns3270 xxxxxxxx
```

These commands can be preset as an icon in a folder on the WinCenter desktop. In the figure below, we create a folder called Network Station Commands, which we make available to any user logging on, into which we created icons for a few sample IBM Network Station commands, such as locking the station, logging out, starting the console, starting the show version application, etc.

The bottom part of the figure illustrates how we create the Lock Network Station icon by entering the `wcprsh` command with the required parameters. The Program Item Properties panel is obtained by clicking on the **File** pull-down from the main Program Manager panel, then selecting **New** to get the New Program Object panel, on which we select **Program Item** to get the panel shown below.

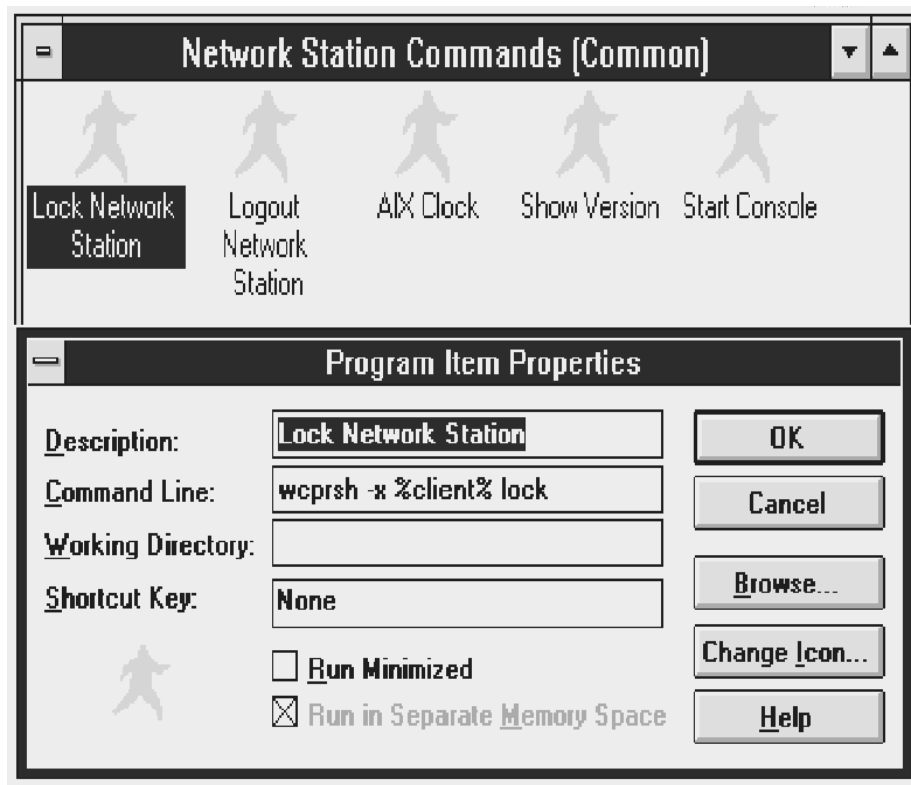


Figure 277. Creating Icons for wcpsh Commands

You can also accomplish the same thing by using a built-in WinCenter facility. Click on the **WinCenter Evaluation** folder, then on the **NCD WinCenter** icon, and on the **New Connection** tab on the panel entitled WinCenter.

Then click on the **Launch NCDware Application** radio button, enter the command you wish to issue, such as show version, in the Application field, and click on the **Start** button.

Note that you can also launch an X Window application on another host from here. For example, if you enter the name of an AIX host in the Remote Host field and an application name such as xclock in the Application field, and then select the Start button, you will see the xclock display appear on your IBM Network Station desktop, assuming that you have the proper authority to execute this application on the remote AIX machine.

### 17.8.2 From a MetaFrame Desktop

The WCPRSH command that was available with WinCenter is not available on a WTS server running UIS.

A normal RSH command can be used instead with the %clientname% variable if the -name option was used on the icacnt command to pass the IP address of the client when establishing the session.



---

## Chapter 18. Installing Applications on WTSE

This chapter discusses the issues associated with installing applications on multi-user systems such as Windows NT Server 4.0, Terminal Server Edition or WinFrame.

The issues have to do with the fact that applications are typically designed to be installed on a single-user system, or even as client/server applications, but not specifically to be shared simultaneously by multiple users on the same system.

---

### 18.1 Objectives

The main objective of this chapter is to make the average reader who may be unfamiliar with a multi-user environment understand the nature of the problems encountered when installing applications on a Windows NT Server 4.0, Terminal Server Edition or WinFrame system. The second objective is to provide sufficiently detailed and illustrated examples to make it easy for anyone to understand the solutions to these problems.

The targeted audience for this chapter is anyone with a need to understand these issues and any Windows NT administrator who has had little experience with these kinds of issues.

There is probably little information in this chapter that is new, and that has not been covered elsewhere in some document. What is new perhaps is that we try to do the following:

1. Consolidate in one place all the important pieces of information on this subject.
2. Structure the information in a logical fashion.
3. Include more basic explanations for the benefit of the less experienced administrator or any other person that is not already familiar with these notions and issues.
4. Illustrate the problems and the solutions with a few diagrams and examples.

For those who prefer to go to the original source of the actual information, we have identified in 18.3, "Sources of Information" on page 305 some of the different documents that we have consulted in order to build this particular section.

As well, since many of these products are still in beta at the time of this writing, it is likely that certain facts may change by the time the final version of the product becomes available, which is why we encourage the reader to consult the actual product documentation when it becomes available in order to get the most up-to-date information and to keep up with any new information through the many sources available on the World Wide Web.

### **Windows NT Server 4.0,**

In this document, we use the Windows NT Server 4.0, Terminal Server Edition (formerly known as Hydra) as the base for our examples.

In most cases however, whatever is true for a Windows Terminal Server system is also generally true for a WinFrame server. We try, throughout the text, to draw your attention whenever there is a difference for the WinFrame environment.

---

## **18.2 Overview**

Why do we need to dedicate a whole chapter to installing applications?

The reason is that we are discussing installing applications not on traditional single user systems but rather on a multi-user Windows NT server such as WinFrame or Windows NT Server 4.0, Terminal Server Edition, which presents particular problems.

The problems stem from the fact that even though a Windows NT system does have most of the facilities necessary to make it a multi-user system, many applications have not been designed to be installed on a multi-user system.

The problems created by installing applications on a multi-user system are termed compatibility issues. The issues consist of:

- Registry issues, where the application installation process writes Registry entries that are applicable to a specific user into the area of the Registry which is normally used for all users, and vice versa.
- File issues, where applications that use files to store data do not provide, during the installation process, the option to enter a specific path for the location of user files, leading to multiple instances of an application sharing the same file.
- Object problems where two instances of an application might share the same object, which is similar to the problems with files.

There are tools and techniques available to solve these compatibility issues such that most applications can be installed with relative ease. These are:

- The change user command. This is the main tool to use for all application installations. It puts the system in a special mode such that special events are recorded and saved so that they can be used later to solve some of the issues.
- Installation scripts. These are command files, available for some popular applications, that automate some of the modifications to Registry entries or INI files that need to be performed after an installation.
- User logon scripts. These are either supplied or custom-created by an administrator, to perform actions, such as copying files, at the time that a user logs on, to complement or supplement the installation scripts.
- Home drives. Use of a home drive is a technique that facilitates solving many of the file issues by identifying file paths as a generic drive.



- Compatibility flags. These are Registry entries that allow an administrator to alter the system's default actions at the time that a user logs on.
- MultiUser Application Manager. This is a tool specific to WinCenter which provides a user friendly interface for writing application scripts and logon scripts.

The main problem and challenge for an administrator remains the identification of the actions that need to be performed after the normal application installation process. For many of the popular applications, these actions are identified in applications notes supplied with the Windows NT Server 4.0, Terminal Server Edition, and installation scripts and logon scripts supplied to automate these actions. Where application notes are not available, it is up to the administrator to determine which actions are required.

In many cases, the use of the change user install command is the only action required; for other applications however, the actions required may be more complex and sometimes difficult to identify. Hopefully, most typical and popular applications already have installation scripts that simplify the job of the administrator.

The next pages describes in more details what the issues are, the tools that are available, how to use them, and presents a few practical examples to illustrate the use of the tools and techniques.

---

## 18.3 Sources of Information

We found multiple documents containing information on application compatibility issues, which we have consulted and used in order to build some of the information in this document.

These documents are:

- The terminal.doc file which is supplied with the Microsoft Windows NT Server 4.0, Terminal Server Edition Beta 2 code. It is located in the root directory of the beta CD.

This is an excellent detailed description of all the compatibility issues and should be your main source of information.

- There are White papers on Microsoft Windows NT that can be accessed at <http://www.microsoft.com/NTServer/Basics/TechPapers/default.asp>. One of those in particular, entitled *Guide To Microsoft Windows NT 4.0 Profiles and Policies* can be useful in this environment.
- The application installation scripts and user logon scripts supplied with the Windows NT Server 4.0, Terminal Server Edition beta2 code.

After the installation of the Windows NT Server 4.0, Terminal Server Edition, these are located in the \WTSRV\Application Compatibility directory.

- The NCD Inc. *WinCenter Connect System Administrator's Guide* publication, Chapter 3, entitled "Setting Up Multi-User Applications".

This publication is packaged with the WinCenter 3.1 code and it provides an excellent summary of the application compatibility issues and problems.

It also introduces a tool called the Multi-User Application Manager, which might be useful to administrators using WinCenter who want to build and customize their own application installation scripts.

- Application notes from NCD Inc. at their [www.ncd.com](http://www.ncd.com) Web site.
- Application notes and WinFrame Solutions Guide from Citrix Inc. available from the support area at their [www.citrix.com](http://www.citrix.com) Web site.
- The SG24-2127 redbook entitled *IBM Network Station Guide for Windows NT*.

---

## 18.4 Application Compatibility Issues

Application compatibility issues are the problems that an administrator runs into when installing applications on a multi-user Windows NT system, such as WinFrame or Windows NT Server 4.0, Terminal Server Edition, when these applications were originally designed to function on a single user system.

### 18.4.1 What Is the Cause of the Problem?

The main cause of the problem is that many applications do not make a clear distinction between machine configuration data (which applies to all users of a system) and user configuration data (which applies only to a specific user).

The base Windows NT system has most of the features and functions necessary for a multi-user operation, such as memory protection, preemptive multitasking, code reuse and separate storage of each user's application and configuration data, but all of these functions do not help if the application does not take advantage of them.

Here is a simplistic example that illustrates what this means.

Suppose that you install a simple application such as an editor, and this editor uses an INI file to store user preferences such as background color. During the installation process, the INI file is stored in the root directory of the system, for example `c:\WINNT`.

After installation, the user starts the editor, changes the background color preference to green, and stores his or her preference, which updates the INI file to indicate that the editor should always start with a green background.

If a second user now logs on to the same system and starts the editor, the editor reads the INI file from `c:\WINNT` and he or she gets a green background. If this second user now changes the preference to a red background and saves his or her preferences, the next user will now get red, and so on.

The solution to this problem is to ensure that there is a specific INI file for each user, and that the editor, upon starting, fetches the copy of the INI file which belongs to the user starting the editor, so that each user can conserve his or her own personal preferences and settings.

This particular example is most simplistic, and it applies to a typical 16-bit Windows application that uses an INI file instead of the Windows Registry, but it illustrates the basic problem involved in multi-user systems well.

Another consideration is the attention that the administrator must bring to protecting the system from being inadvertently modified by users, and from

protecting users from interfering with each other. In traditional multi-user systems such as VM or UNIX, it is taken for granted that this protection is automatic and an inherent part of the way that the system is designed. However, in Windows NT, it is up to the administrator to put in place the required mechanisms to effectively achieve this user separation and protection.

Now let's take a look more specifically at the different types of problems that can be encountered.

### 18.4.2 Application Compatibility Problems

The problems encountered are categorized into three main types:

1. Registry setting problems

Most problems in this area are caused by applications that do not make proper use of the Registry when they store configuration data that applies to a user in the section that applies to the whole system (HKEY\_LOCAL\_MACHINE) instead of storing this data in the user-specific section (HKEY\_CURRENT\_USER).

2. File problems

Many applications that make use of specific system and/or user files to store data do not provide, during the installation process, the option to enter a specific path for the location of user files.

Consequently, these paths are not user-specific and need to be modified so that they become applicable to all users.

3. Object problems

Objects are items such as events, devices, semaphores and sections that applications use to communicate with each other. Again, if two instances of an application share the same object (similar to the problems with files), this leads to problems.

### 18.4.3 Solutions, Tools and Techniques

Most of the above problems can be solved, in a relatively easy fashion, by a combination of functions and tools provided with the Windows NT Server 4.0, Terminal Server Edition (and WinFrame) system, in addition to using a structured approach or strategy for installing applications and defining users.

The main solutions, tools and techniques that an administrator can use are as follows:

1. The change user command

This command is the main tool to use in all cases. Using the change user /install command alerts the system, at the time that an administrator installs an application, to be on the lookout for particular events and to automatically record specific pieces of data (Registry entries, etc.) and save them in a special location.

After the installation is complete, the change user /execute command is issued to reset the system to normal operation mode.

For some applications, using the change user /install command during installation of the application is all that is required to solve all the compatibility issues for that application.

For other applications, use of the change user /install command alone is not sufficient and additional tools and techniques must be used. We see specific examples of this in 18.8, "The change user Command" on page 325.

## 2. Application installation scripts

These are DOS-style batch command files that are either supplied with Windows NT Server 4.0, Terminal Server Edition, or other systems, or that can be custom built by the administrator.

Each of these command files is specific to an application and is intended to simplify the job of the administrator by providing him or her with an automated way of making modifications that are required after the completion of the normal application installation process.

For example, this procedure can modify path entries in the Registry in order to make them user-specific, or it can change the permissions of certain files, or move shortcuts from a specific user's profile to all users' profiles, etc.

### Note

No matter how the administrator decides to use these command files in his or her particular environment or in his or her approach or strategy, the single most valuable information that these installation scripts provide is the identification of the changes that are required for a particular application.

In other words, if an administrator did not have these scripts supplied to him or her, the most difficult and time-consuming activity would be for him or her to identify the Registry entries created by the applications, the files used, whether they contain user-specific data, where the paths to these files are stored, etc.

In some cases, this may be a very simple task, especially if the application is simple and well-behaved, but in other cases this might require intimate knowledge of the application and may even require the help of the supplier of the application.

So, even if the administrator decides not to use the installation scripts as supplied the information they contain is invaluable for him or her to set up his or her own custom procedures.

## 3. User logon scripts

For some applications, there is a need to make modifications at the time that a user logs on.

This is usually accomplished through the use of logon scripts, which are also batch commands files, the execution of which can be triggered automatically at the time that the user logs on.

Logon scripts are also used to perform other general actions that may be needed at the time the user logs on.

## 4. Home drives

Many of the problems associated with the path of user-specific files can be elegantly solved by using a home drive. This is because a home drive consists only of a drive letter (as opposed to a specific path), and it can therefore be generic to all users.

In other words, if the specified path of a user file is indicated and recorded in the Registry as W:, and all users use W: as their home drive, the administrator can set it up such that the drive W:, for each user, points to the user's home directory. See 18.5.1, "What Is a Home Directory" on page 311 for more details on home directories and home drives.

#### 5. Approach/strategy

The last item of importance is the overall approach or strategy that the administrator decides he or she wants to use for his or her own particular environment.

The overriding factor here is probably the size of the installation, in terms of the number of servers and numbers of users that need to be defined, as well as the preferences of the administrator.

The issues here deal mainly with how much automation the administrator needs to build into his or her system. Clearly, if he or she has hundreds of users with new users being added every day, the emphasis will be more on a complete automated process so that defining and adding a new user becomes a simple task.

On the other hand, in a very small environment with a fixed population of users, the administrator may decide to accomplish many of the tasks in a manual fashion if these tasks do not need to be repeated frequently.

Let's take a detailed look now at each of these categories of problems, with examples, in order to gain a better understanding of the problems and the solutions and tools that can be used.

### 18.4.4 Registry Settings Problems

The Windows NT Registry is a system database containing configuration information for the system, applications and users. There are two areas of the Registry that concern us here:

1. The HKEY\_LOCAL\_MACHINE hive, which is where an application stores information that applies to the system as a whole. For example:
  - The components installed by the application
  - The paths to be used to load application modules
  - The path to a shared database
2. The HKEY\_CURRENT\_USER hive, which is where an application stores data that is specific to the current user only. For example:
  - Paths to custom files that are user-specific. These can be custom dictionaries, mailboxes, configuration files, etc.
  - Settings such as user preferences.

In fact, when a user logs on, his or her user profile (the ntuser.dat file) is loaded into the Registry and becomes HKEY\_CURRENT\_USER. When he or she logs off, any changes to HKEY\_CURRENT\_USER are written back to his or her user profile in order to be loaded the next time he or she logs on. (See 18.7, "User Profiles" on page 319 for additional details on user profiles.)

Typical problems dealing with the Registry are:

1. An application writes user-specific data into HKEY\_LOCAL\_MACHINE instead of HKEY\_CURRENT\_USER.
2. An application correctly writes user-specific information into HKEY\_CURRENT\_USER during product installation; however, the problem remains that this information is now available only to the user that performed the installation, and not to other users.
3. An application correctly writes user-specific information into HKEY\_CURRENT\_USER, but instead of doing so at installation time, it waits until the user executes the application for the first time.

Most of these Registry problems are solved with the use of the change user /install command and through the use of application installation scripts and user logon scripts. We provide an example in 18.9, "A Few Practical Examples" on page 331.

#### 18.4.5 File Problems

The files we are referring to here are typically files required by the application that are user-specific. For example, Lotus 123 needs a place to store the user's spreadsheets, and this is usually a directory such as d:\lotus\work\123 if the application was installed on the d: drive.

If multiple users now attempt to use this application as is, all users would store their spreadsheets in the same location (D:\lotus\work\123), which is not acceptable.

So the problem is that the application uses a public location instead of a user-specific location. For most applications, this is the primary problem and also typically the most difficult to solve.

The generic solution to this problem, as we see in a moment, is to update the path of these files so that they point to the user's home directory instead of a single public location.

However, the biggest difficulty lies in first being able to identify which files are actually user-specific and which ones are not. And once you have identified the user-specific files, then you need to find out where the application has stored the path to these files so that you can modify that path. These paths can be stored in various locations, such as:

- HKEY\_LOCAL\_MACHINE
- HKEY\_CURRENT\_USER
- A configuration file such as an INI file
- Hard coded into the application

Here also, once these files and the location of their path specifications have been identified, most of these file problems can be solved automatically with the use of the change user /install command and the use of application installation scripts and user logon scripts.

In fact, this is where the supplied application installation scripts come in very handy because someone has already done the most difficult part of the work in order to be able to generate these command files. If all you have to do as an

administrator is modify these command files, then you have already solved the biggest problem.

#### 18.4.6 Object Problems

A Windows application can create objects such as events, devices, semaphores and sections that are used to communicate with other applications. Each object has a name that is globally visible on the system, and this can create problems similar to the shared files.

If two instances of an application are running, they both require separate objects instead of sharing the same object.

This problem is solved automatically by Windows NT Server 4.0, Terminal Server Edition because it provides the ability to map an object name to a private instance of that object for each session.

An object that is shared by the entire system is called a *system global* object whereas an object specific to a user session is called a *user global* object.

However, note that if an application running from the console creates an object, that object remains a system global object and is not automatically created as user global. This is true as well of programs that run as NT Services because they run in the system context.

---

### 18.5 Home Directories and Home Drives

Using home drives and home directories is a key strategy to facilitate the installation of applications in a multi-user environment, so it is important to understand what they are and how they can be used.

#### 18.5.1 What Is a Home Directory

A home directory is a subdirectory that is the default directory for this user. When the user starts a command prompt for example, he or she is always automatically positioned at his or her home directory.

This directory is accessible only by the user to whom it belongs, and by no one else. The administrator, when creating a user account, specifies the location of the user's home directory and the system automatically creates this directory when the account is created.

#### 18.5.2 Creating a Home Directory

A user's home directory is created at the time that the administrator defines a user through the User Manager for Domains application. To start the application, select **Start=>Programs=> Administrative Tools=> User Manager for Domains** and after selecting an existing user or creating a new one, click on the **Profile** button to get the panel shown in the following figure:

User: Huebner (Edward Huebner)

User Profiles

User Profile Path:

Terminal Server Profile Path:

Logon Script Name:

Home Directory

☒ Local Path:

☐ Connect  To

Terminal Server Home Directory

☒ Local Path:

☐ Connect  To

☐ Map Root (Netware Home Dir Only)

OK Cancel Help

Figure 278. Specifying a Home Directory for a User

In the figure above, we define a new user called huebner, and we specify the home directory for user huebner as d:\users\huebner.

We can also enter d:\users\%username%, which causes the system to replace %username% with the actual user name that we are working with at this time. This is useful when defining a template account, meaning an account where we define most of the characteristics in advance, and then just use it as the source of a copy when creating a new user account. This saves keystrokes and allows a more rapid way of creating new accounts.

Click on **OK**, and then **Add** to add the user to the database. The system then creates the user account, and also creates the home directory that we have specified above as d:\users\huebner, and sets the permissions for that directory such that only this user has full control over this directory, and that no other user has access to it.

The figure below shows the d:\users subdirectory, which we have designated as the directory where we put all the users home directories. It currently contains the home directories for three users named huebner, newuser and userx1 respectively.



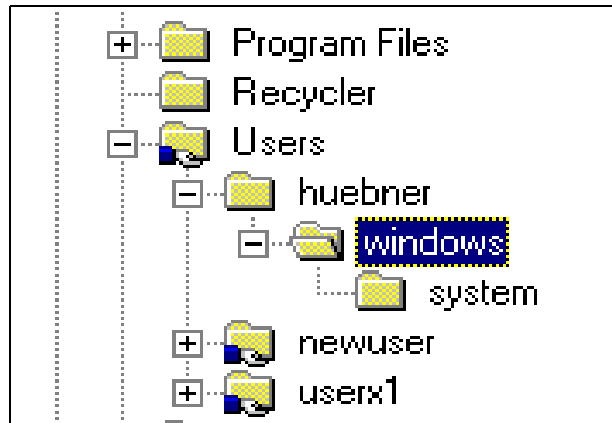


Figure 279. Home Directories

If we select the huebner subdirectory, and examine its properties (right click on the folder, and then select **Properties**), and then use the Security tab to select **Permissions**, we can verify, as is shown in the figure below, that only user huebner has full control.

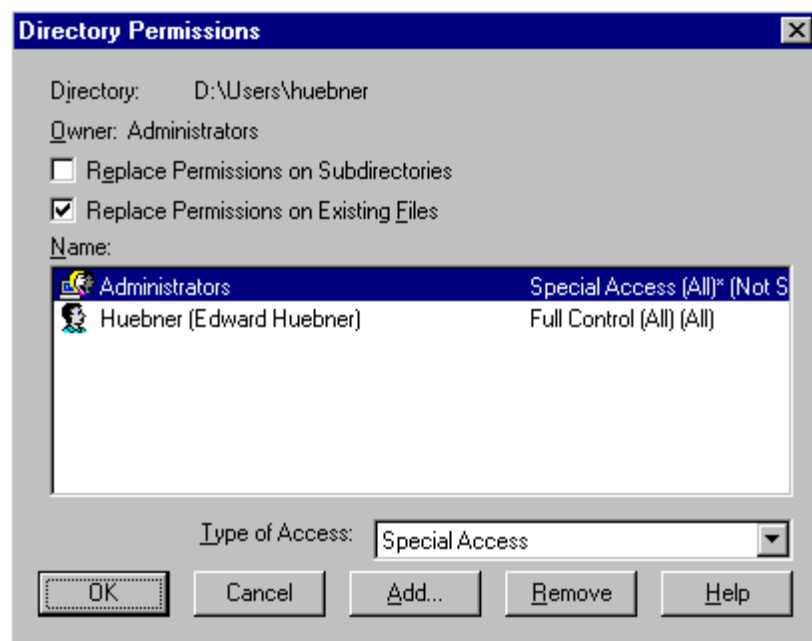


Figure 280. Permissions Set on the Home Directory

Now that the user has his or her own personal and private home directory, it can be used to store files that are not to be shared or viewed by any other user. This is where we store application files that we want to be unique to this user.

#### 18.5.2.1 The User's Windows Subdirectory

Notice in Figure 279 above that the system has not only created the base home directory called d:\users\huebner, but that it has also automatically created another directory called windows under the huebner subdirectory.

This is a function specific to Windows NT Server 4.0, Terminal Server Edition (and WinFrame) that is part of the processing accomplished through the use of the change user /install command.

This windows subdirectory is in effect the user's private Windows or %systemroot% directory. In other words, when an application issues the GetWindowsDirectory() call in order to find out from the system the path to the system directory, the system returns %homedrive%%homepath%\Windows, thereby pointing to the user's private version of the windows directory instead of the normal value, which could be C:\WINNT for example in the case of Windows NT 4.0, or C:\WinFrame in the case of WinFrame, or C:\WTSRV in the case of Windows NT Server 4.0, Terminal Server Edition.

Note that for applications operating under an administrator's session however, the %systemroot% variable evaluates to the actual and normal value of c:\WTSRV for example.

### 18.5.3 What Is a Home Drive?

A home drive is actually a generic way of referring to a home directory by using only a drive letter. This allows the home directory, in effect, to be referred to in a generic fashion so that it looks the same for every user.

This has a significant impact in facilitating the installation of applications in a multi-user environment because it provides a way of placing a path reference in the Registry that is applicable to all users.

How do we define a home drive then? The home directory must be created first, as we did in the example above. Then, there are a couple of ways of defining a home drive:

1. Using a SUBSTITUTE command
2. Using a shared directory

We need to examine these two methods in detail.

#### 18.5.3.1 Using the SUBSTITUTE Command

Using the SUBSTITUTE command, we equate a drive letter to a subdirectory. For example, if we use W: as the drive letter, issuing the following command makes the W: drive points to the home directory d:\users\huebner:

```
SUBST W: d:\users\huebner
```

After this command is issued in the user session (this would normally be done using a logon script at the time that the user logs on), the user effectively has a home drive called W:. In other words, an application that writes to W: actually writes to d:\users\huebner.

Why is this so important and what is the difference?

The significant difference is that W: is generic and is not specific to user huebner. Every other user also refers to his or her home directory as W: so that paths that get stored in the Registry that points to W: will correctly evaluate the proper user directory for every user.

For example, assume that you have an application X that reads and writes data to a file called workfile, and, in order to find the path to this file, it queries the Registry for the value of a variable called mypath, as illustrated in Figure 281 on page 315. If the value of mypath, as stored in the Registry, is set to d:\users\user1\workfile, all users would use the workfile of user1, but if the value of mypath is set to W:\, then application X executing in the user2 session correctly evaluates the mypath to W: which in turn evaluates correctly to d:\users\user2, thereby allowing each user to use his or her own private workfile file.

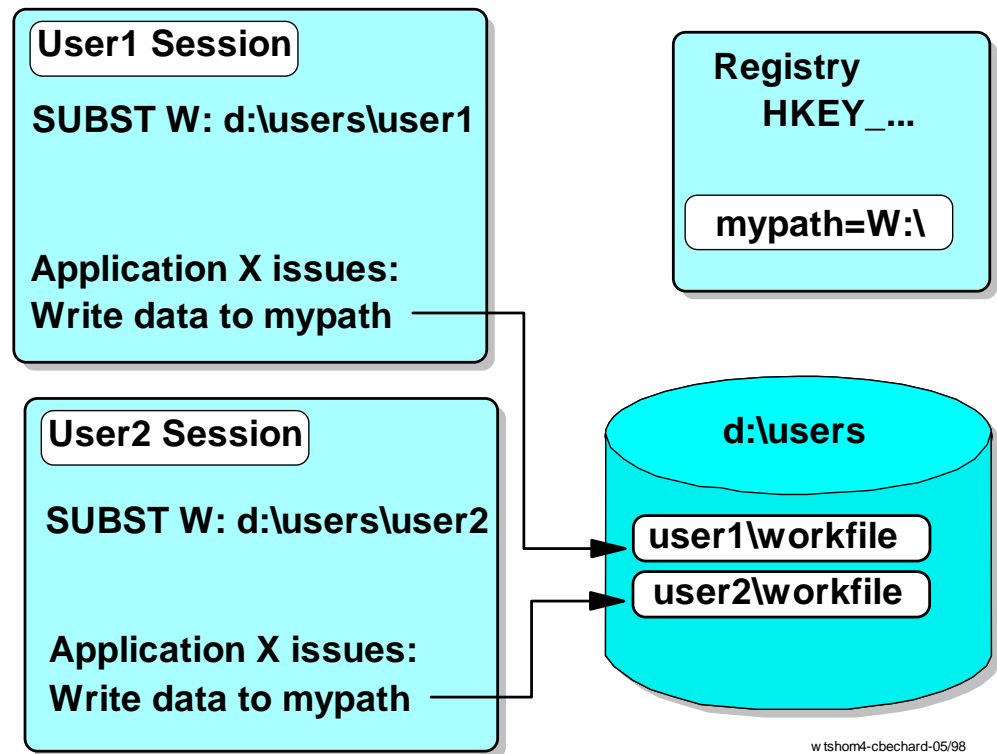


Figure 281. How a Home Drive Is Used

Using the SUBST command is the simplest of the two methods. However, there may be applications (we know Lotus Organizer is one of them) that do not recognize the SUBST command, in which case the second method may have to be used.

### 18.5.3.2 Using a Shared Directory

The second method to define a home drive is to make the user's home directory a shared drive, and then use the Connect To option in the user environment profile to equate a drive letter to this shared drive.

The procedure to accomplish this is as follows:

1. Create the shared drive.

Open the Windows NT Explorer, use a right mouse click on the user's home directory (d:\users\huebner in our example) and select the entry **Sharing**, which brings up the panel below:

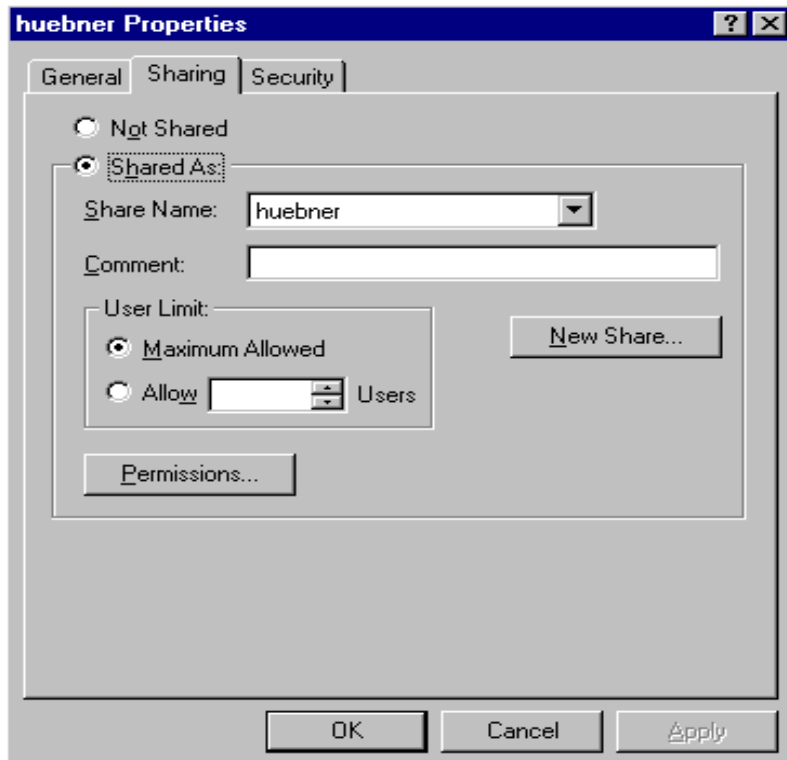


Figure 282. Making the Home Directory a Shared Drive

Select the **Shared As:** button, which automatically fills the Share Name with the name of the folder (in our example huebner), and click on **OK**. The huebner folder icon in the Explorer changes to one with a hand underneath, indicating that this is now a shared resource.

2. Modify the user profile.

Return to the User Manager for Domains application, open the huebner user account and click on the **Profile** tab to return to where we previously specified the location of the home directory, which brings up the following panel:

**User Environment Profile**

User: Huebner (Edward Huebner)

OK  
Cancel  
Help

**User Profiles**

User Profile Path:

Terminal Server Profile Path:

Logon Script Name:

**Home Directory**

☐ Local Path:

☒ Connect **W:** To

**Terminal Server Home Directory**

☒ Local Path:

☐ Connect  To

☐ Map Root (Netware Home Dir Only)

Figure 283. Using the Connect To Option for a Home Directory

In the Home Directory section of the panel, we had previously selected the Local Path button and had entered `d:\users\%username%`, which caused the system to create the home directory for that user (`d:\users\huebner`).

We now change this setting in the following manner:

- Click on the radio button labeled **Connect**.
- Select the letter **W** in the drop-down list.
- Enter `\\servername\sharename` in the field labeled To, where `servername` in our example is `nstationserver` and `sharename` is `huebner`.
- Click on **OK** to complete the process

Your Windows NT Explorer should now show a drive `W:`, which actually represents the `d:\users\huebner` directory.

Effectively, we have just accomplished the equivalent of using a SUBSTITUTE command to say `SUBST W: d:\users\huebner` and the `W:` drive is now pointing to the `d:\users\huebner` home directory.

This second method requires more work for the administrator than using the SUBSTITUTE command because it requires the definition of a shared directory for each user. However, if you have some applications that do not recognize the SUBSTITUTE command, this may be the only choice.

Note that in the case of WinFrame, this second method requires the Server Options Pack license to be installed on the WinFrame server in order to be able to define shared directories. The Server Options Pack license is a

separate license from the base WinFrame license, separately priced also, that allows the WinFrame server to function as a file and print server, and this is required in order to be able to create shared drives.

Notice that in the figure above (Figure 283 on page 317), you also have a section on the panel labeled Terminal Server Home Directory, in addition to the more familiar Home Directory section that we have used. This is used when you want to cause a different behavior when a user logs on as a Windows NT user or when he or she logs on as a terminal server user. If you make entries only in the Home Directory section, it applies to both Windows NT and Terminal Server logons.

### 18.5.3.3 Using Connect To to Create the Home Directory

Please note that the above method means that you need to define a shared drive for *every* user.

You might be tempted to think that you could save yourself a few definitions by making the user's subdirectory a shared directory, and then, in the Connect To field, where we previously specified \\servername\sharename as \\instationserver\huebner, to specify instead \\instationserver\users\%username%.

This indeed would cause W: to show as pointing to the same physical location, but the Connect To entry will not work properly. Indeed, when you use the drive W:, it only maps to the server name and share point, and does not reference directories beyond the share point. In other words, the sharename in \\servername\sharename *must* be the user's subdirectory for this to work properly.

In addition, if you use the Connect To option to trigger the system to create the home directory (instead of using the Local Path option), the directory does get created by the system but the permissions are set such that everyone has full control, which is not what you want for a home directory. It is therefore much preferable to use the method of the local path, as we have illustrated.

---

## 18.6 Logon Scripts

A logon script is a command file, or batch file, that is executed automatically at the time that a user logs on. It can be used, in this environment, to map a drive letter to a user's home directory if we use the substitute command for example, to copy files from a template user's home directory to the user's home directory, or any other task required to customize the user environment.

There are three methods that can be used to trigger the execution of a command file at logon time:

1. The command file is placed in the user's startup folder. This method is particularly applicable when you need to have a customized script for each user.
2. The command file can be placed in the All Users startup folder, if it is applicable to all users.
3. The command file can be specified in the user environment profile when defining the user account. An example of this is illustrated in the figure below, where we specify that a script called logon.bat be executed for the user called huebner.

**User Environment Profile**

User: Huebner (Edward Huebner)

**User Profiles**

User Profile Path:

Terminal Server Profile Path:

Logon Script Name:

**Home Directory**

☐ Local Path:

☒ Connect

**Terminal Server Home Directory**

☒ Local Path:

☐ Connect  To

☐ Map Root (Netware Home Dir Only)

OK  
Cancel  
Help

Figure 284. Specifying a Logon Script in the User Profile

This logon script can be applicable to all users, or it can be made specific to a group of users or to a specific user. The administrator decides, at the time that the user profile is created, which logon script needs to be executed for that particular user.

If no path is specified, but only a file name such as logon.bat as we used in the figure above, the logon.bat file must reside in the %systemroot%\system32\Rep\Import\Scripts directory.

## 18.7 User Profiles

A user profile is a series of settings that identifies the user's preferences and environment.

These settings and preferences are items such as the location of the icons on the desktop, and the color of the background, or the background bitmap, which appear in the Start menu, etc.

All of these settings are stored in a location from where they can be retrieved when the user logs on.

### 18.7.1 Location of the User Profile Settings

In Windows NT 4.0, the user profile is stored in %systemroot%\Profiles\Username, and consists of a set of folders and a file called ntuser.dat which contains the Registry settings.

The figure below illustrates the profile for user bechard on a typical Windows NT 4.0 system.

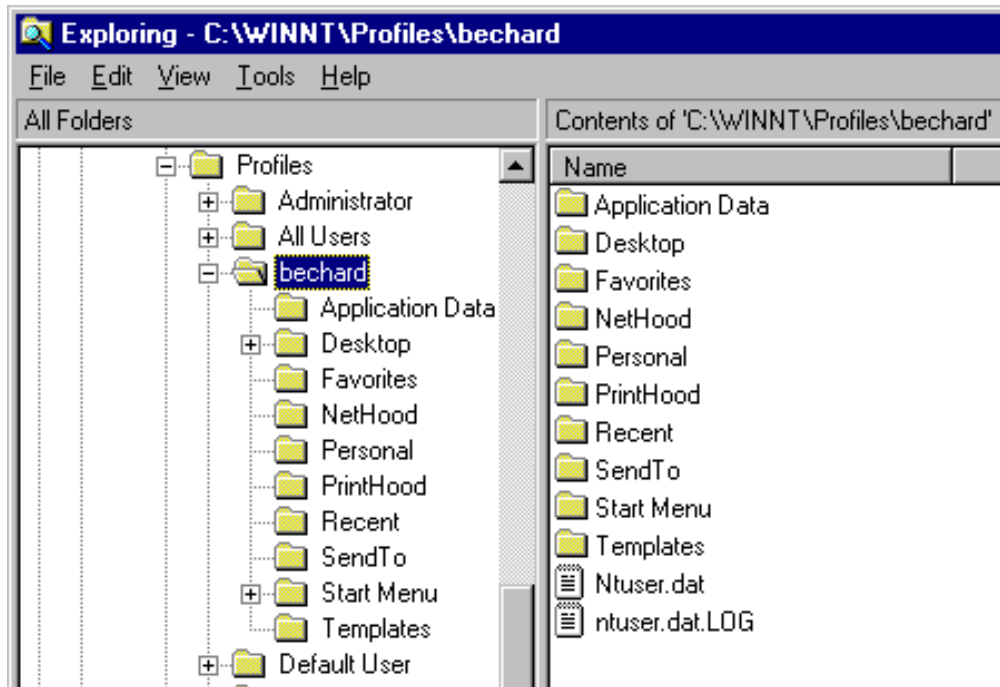


Figure 285. A User Profile

Notice that the folder username (bechard in this case) is located in c:\WINNT\Profiles. The root folder contains a file called Ntuser.dat that contains the Registry entries for this user. There are also 10 or so folders for a variety of settings. Note that some of these folders do not normally show up in Explorer unless the user has set the options to show all files, which is the case for the Desktop, NetHood, Personal, PrintHood and Recent folders.

### 18.7.2 Initial Creation of a User Profile

A profile gets initially created for a user in either of two ways:

1. If no entry is specified in the User Profile Path field of the User Environment Profile (see Figure 284 on page 319) when the user logs on for the first time, the system automatically generates a new profile using the Default User profile as a source.

The Default User profile appears in Figure 285 above, as the last profile listed.

2. If an entry is specified in the User Profile Path field of the User Environment Profile when the user logs on, the system fetches that copy of the profile in order to create a local copy of the user profile, and stores it in %systemroot%\Profiles\username.

This is called a *roaming* profile. Any changes the user makes to this profile is written back to where his or her roaming profile resides, but a local copy is



always kept for cases where the roaming profile cannot be accessed at logon time.

Notice in Figure 285 above that there is also a profile called All Users. Anything that appears in the All Users profile (for example, an icon in the Start Menu) also appears in all the other profiles.

Therefore, if you change either the Default User and/or the All Users profiles, the changes you make are reflected in any new profile created when a new user logs on for the first time.

Once a user has a profile of its own, any changes he or she makes to his or her environment (changing the location of the icons on his or her desktop for example) are saved in his or her own profile.

### 18.7.3 Example - Creating and Copying a User Profile

The easiest way to create a new user profile is to create a new user account using an administrator account (let's call it template1 for example), log on as that new user (template1), let the system generate a user profile (called template1) from the Default User profile, and then modify the profile by making changes in the user session, for example, add folders to the desktop, or to the Start Menu, and change background colors or bitmaps, etc.

When the environment has been set up the way that you want it to be, log off the template1 user account, log back on as administrator, and then copy the template1 user profile to a central location from where it can be accessed by any user.

To copy a profile, use the following procedure:

- Right-click on the **My Computer** icon on the desktop.
- Select **Properties** and then the **User Profiles** tab on the System Properties panel, which displays the panel illustrated below:

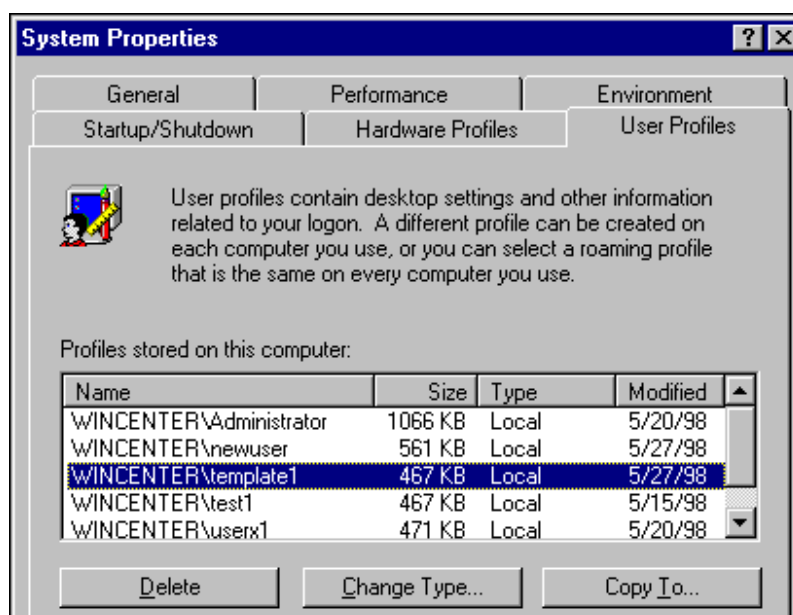


Figure 286. System Properties - User Profiles

- Select the user profile that you want to copy, in this case template1.  
In this illustration, the username template1 is preceded by WINCENTER, which is the computer name of the machine on which these profiles currently reside.
- Click on the **Copy To...** button, which brings up the following panel:

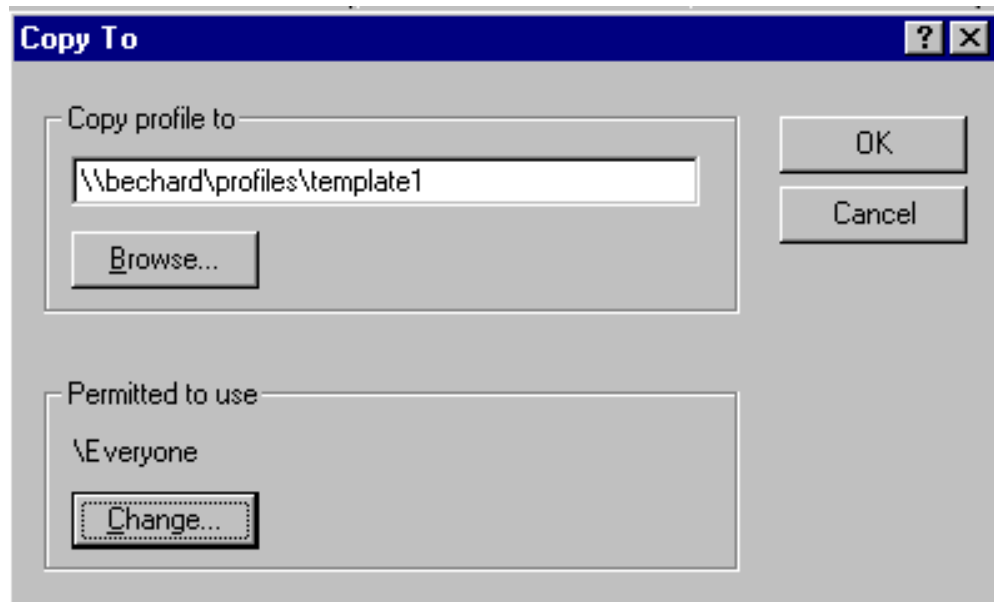


Figure 287. The Copy To Panel while Copying a User Profile

- In the Copy profile to field, enter the location where you want to store that user profile. In this example, we specify that it should be placed in a directory called template1 (if the directory does not exist, it will be created) and in a shared directory called profiles on the server called bechard.  
We had previously defined a directory called profiles on the server bechard, where we intended to store all user profiles and defined it as a shared directory with the same share name (profiles).
- In the Permitted to use section of the Copy To panel, we click on **Change** and select **Everyone** so that all users are able to use this profile (or leave it as is if we want to restrict that profile only to user template1).

#### 18.7.4 Specifying a User Profile Path in the User Account

Now that we have a user profile for our user called template1 stored in a central location, we need to identify that location in the user account definition.

To accomplish this, use the User Manager for Domains application to create or modify a template1 user account, and simply specify the path of the profile as \\bechard\profiles\%username%, where username is replaced by template1 when you exit the panel. This is illustrated in the figure below:

**User Environment Profile**

User: template1 (Template for creating user profile)

OK  
Cancel  
Help

User Profiles

User Profile Path: \\bechard\profiles\%username%

Terminal Server Profile Path:

Logon Script Name:

Home Directory

☒ Local Path:

☐ Connect To

Terminal Server Home Directory

☒ Local Path:

☐ Connect To

☐ Map Root (Netware Home Dir Only)

Figure 288. User Environment Profile - User Profile Path

When the user template1 logs on, the system accesses the copy of the user profile located at \\bechard\profiles\template1, and copies it to the local %systemroot%\profiles. From this point on, any changes the user makes to his or her environment are recorded in the local copy of the user profile. When the user logs off, these changes are copied back to the profile located in \\bechard\profiles\template1.

On any subsequent logons if the centrally stored copy is not available, the locally stored profile is used, and the user informed that the central copy cannot be accessed.

### 18.7.5 Local, Roaming and Mandatory User Profiles

There are three types of user profiles:

1. A *local* user profile is a profile that exists only on the local machine that the user typically uses every day, and it is located in %systemroot%\profiles, as we have seen in the examples above.
2. A *roaming* profile is a profile that is stored typically in a central location, such as a file server, so that it can be accessed by the user from multiple different workstations. As soon as you enter a value in the User Profile Path field of the User Environment Profile in the user account, it becomes a roaming profile.

If the user never logs on to a workstation other than his or her own, then a local profile is sufficient and a roaming profile is not required.

3. A *mandatory* profile is a roaming profile that cannot be modified. In other words, the profile is downloaded from a central location to the machine that user logs on to, but any changes that the user makes to his or her environment during his or her session are discarded when he or she logs off (instead of being written back to the central profile location). When he or she logs on the next time, whether from the same or a different machine, the user always gets the same unmodified user profile that he or she got the first time.

This is designed for cases where we do not wish users to make permanent changes to their profiles.

### 18.7.6 User Profile in a Multi-User Environment

Is there something special about a multi-user environment that should be taken into account concerning user profiles?

The answer depends on how the environment is set up.

1. If the environment is simple and small, with a single Windows NT Server 4.0, Terminal Server Edition being accessed by a fixed set of users, or multiple servers but always dedicated to a fixed set of users, then using local profiles is all that is required.

In other words, if the same user always logs on to the same physical server, there is no need to store his or her profile in a location other than the server he or she always accesses.

2. On the other hand, if the environment is made up of multiple servers with load balancing implemented, such that the user never knows which server he or she will actually be logging on to, then it is necessary to store his or her profile in a central location so that it can be downloaded at the time of the logon to the actual server being logged on to.

### 18.7.7 User Profiles in WinFrame

In WinFrame (Windows NT 3.51), the user profile is stored in a single hive (instead of a series of folders and a hive file like in NT 4.0).

This hive file is located in %systemroot%\system32\config and bears the name admin000, for example, for a user called administrator.

The way to save a profile in NT 3.51 is to use a tool called the Profile Editor, which is shown in the figure below:

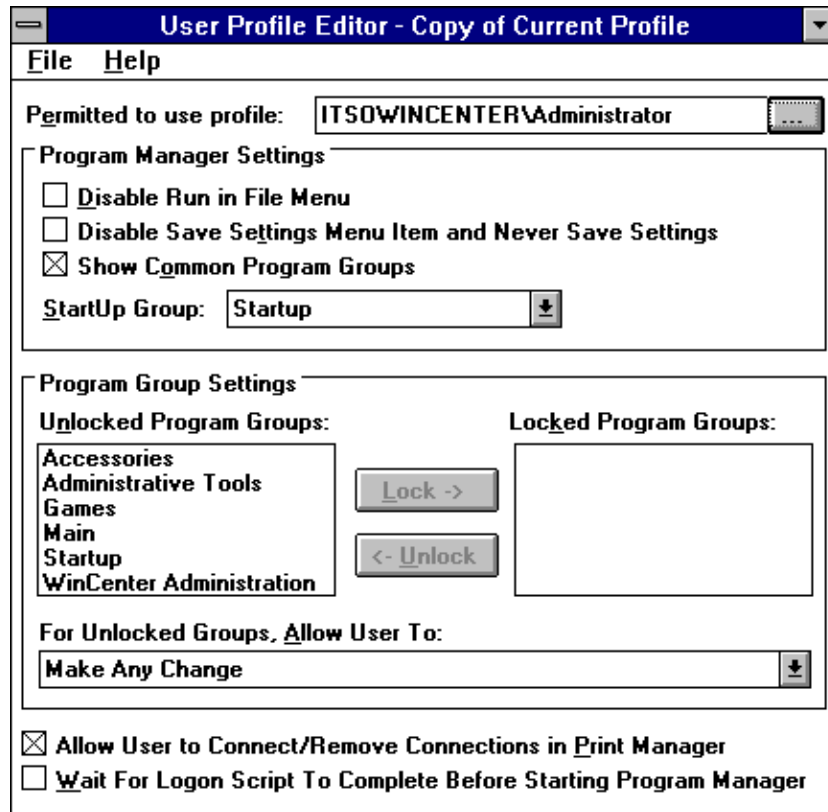


Figure 289. User Profile Editor in WinFrame

The administrator can log on to a user account, configure the desktop as required and then save the profile, using the User Profile Editor, to a central location to serve as a roaming profile.

This profile would be stored as a username.usr file for a roaming profile, or username.man for a mandatory profile. The profile name can also be made generic, by calling it user.usr, but storing it in a directory specific to a particular user, for example, \\servername\profiles\username\user.usr.

## 18.8 The change user Command

As previously stated, the change user command is the main tool to use when installing applications that need to be shared among multiple users on a Windows NT Server 4.0, Terminal Server Edition system, so let us take a look at the effect of this command.

The format of the change user command is either:

```
Change user /install
Change user /execute
Change user /query
```

### 18.8.1 The change user /install Command

The change user /install command is issued by the administrator, prior to the launch of an application's installation process, to put the system in install mode

and enable it to keep track of the Registry entries and initialization (INI) files added to the system during the application installation process.

The system in fact writes these entries to special locations from which they can be retrieved later for propagation to user-specific locations when a user logs on.

Note that using the Add/Remove Programs application in the Control Panel to install an application automatically puts the system in install mode.

The events are as follows, while in install mode:

1. If an application queries the system to find the location of the \windows directory using the GetWindowsDirectory API, the system returns the %systemroot% value, which evaluates to c:\WTSRV in the case of the Windows NT Server 4.0, Terminal Server Edition.
2. If any INI files entries are added using the WritePrivateProfileString API (or any new INI files added), they are added to the INI files under the %systemroot% directory, that is c:\WTSRV for Windows NT Server 4.0, Terminal Server Edition (and c:\winframe for WinFrame).
3. All Registry keys added by an application to HKEY\_LOCAL\_MACHINE are also copied to another location in the Registry.

For Windows NT Server 4.0, Terminal Server Edition this location is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Terminal Server\Install\MACHINE
```

For WinFrame, this location is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Install\MACHINE
```

4. All Registry keys added by an application to HKEY\_CURRENT\_USER are also copied to another location in the Registry.

For Windows NT Server 4.0, Terminal Server Edition, this location is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Terminal Server\Install\Software
```

For WinFrame, this location is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Install\Software
```

This process is illustrated in the next figure, where the values stored by application X in the HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER are copied to a central location.

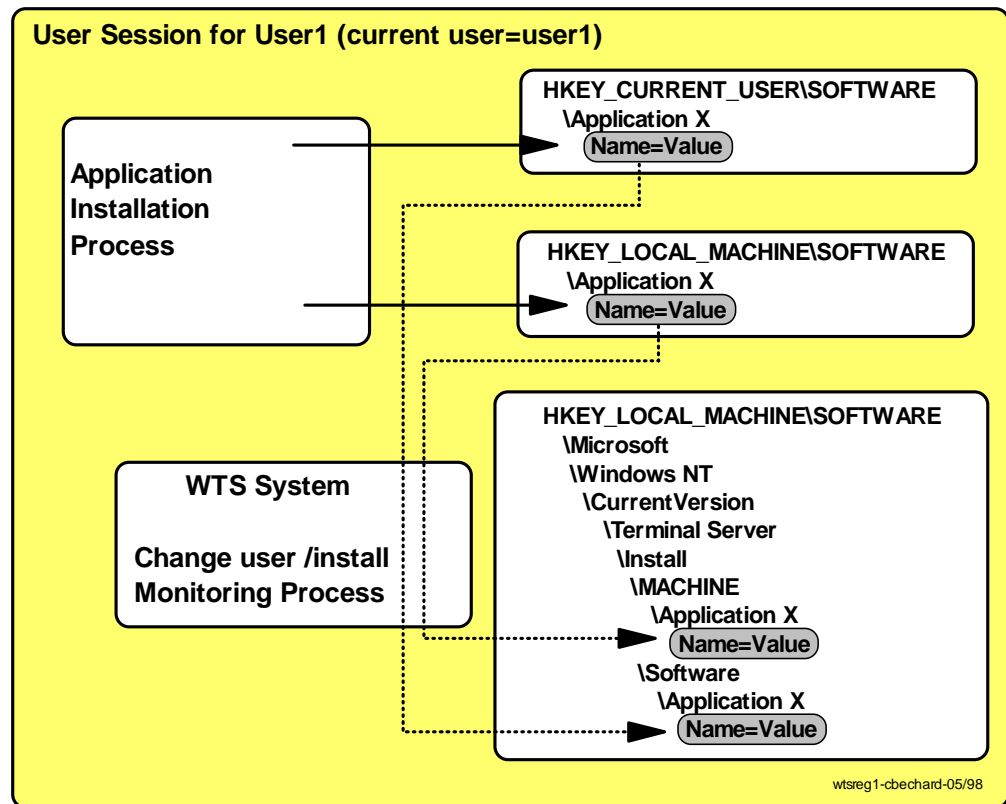


Figure 290. Copying Registry Entries to a Central Location

## 18.8.2 The change user /execute Command

The change user /execute command is issued by the administrator after the installation process completes, in order to put the system back into its normal operation mode. This causes the system to stop recording modifications made to Registry entries or INI files and to start monitoring user logons and application requests for INI files or Registry entries.

Note that if Add/Remove Programs was used to start the installation, then the system is automatically returned to the execute mode at the completion of the installation.

The following events happen when in execute mode:

1. When an application tries to read a Registry entry under HKEY\_CURRENT\_USER and the entry does not exist, the system checks under the following for the existence of this entry:

```
KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Terminal Server\Install
```

If the entry exists, the key and its subkeys are copied to the appropriate location under HKEY\_CURRENT\_USER.

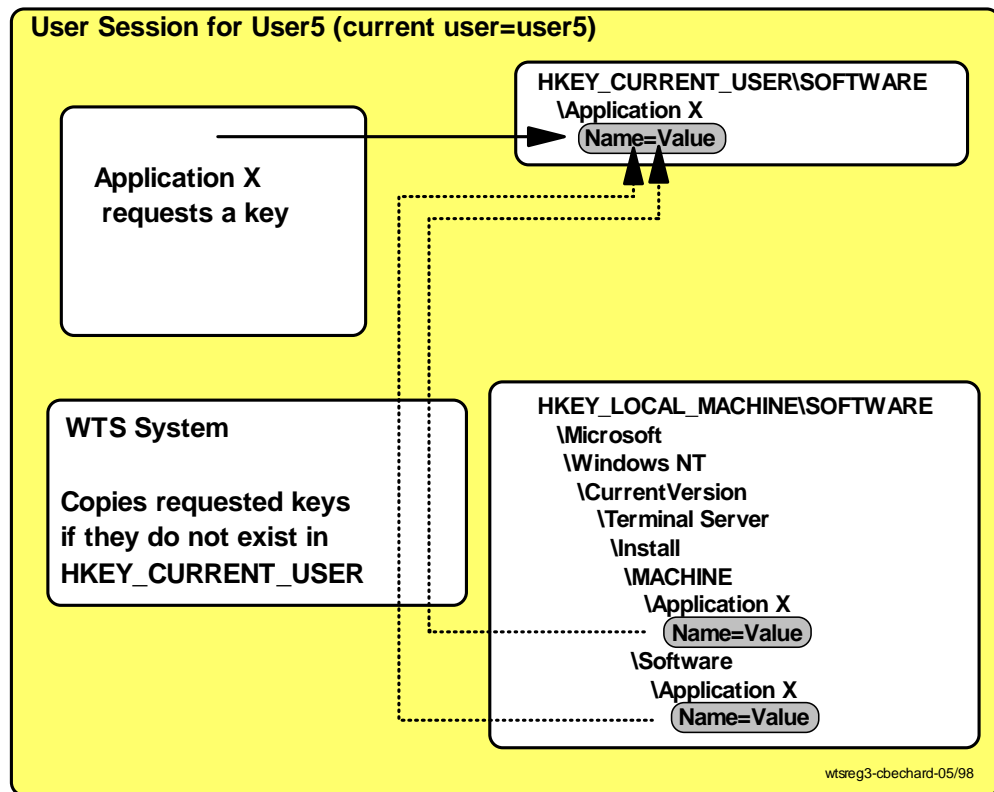


Figure 291. Copying Registry Entries to HKEY\_CURRENT\_USER

2. When an application issues a GetWindowsDirectory API call to get the path to the windows directory, the system returns the path to the windows directory located under the user's home directory.
3. When an application uses the GetPrivateProfileString API call to read an INI file and that file does not exist in the windows directory located in the user's home directory, the system checks for the existence of the INI file in the %systemroot% directory and, if it exists there, copies it to the user's private windows directory, as illustrated in the diagram following:



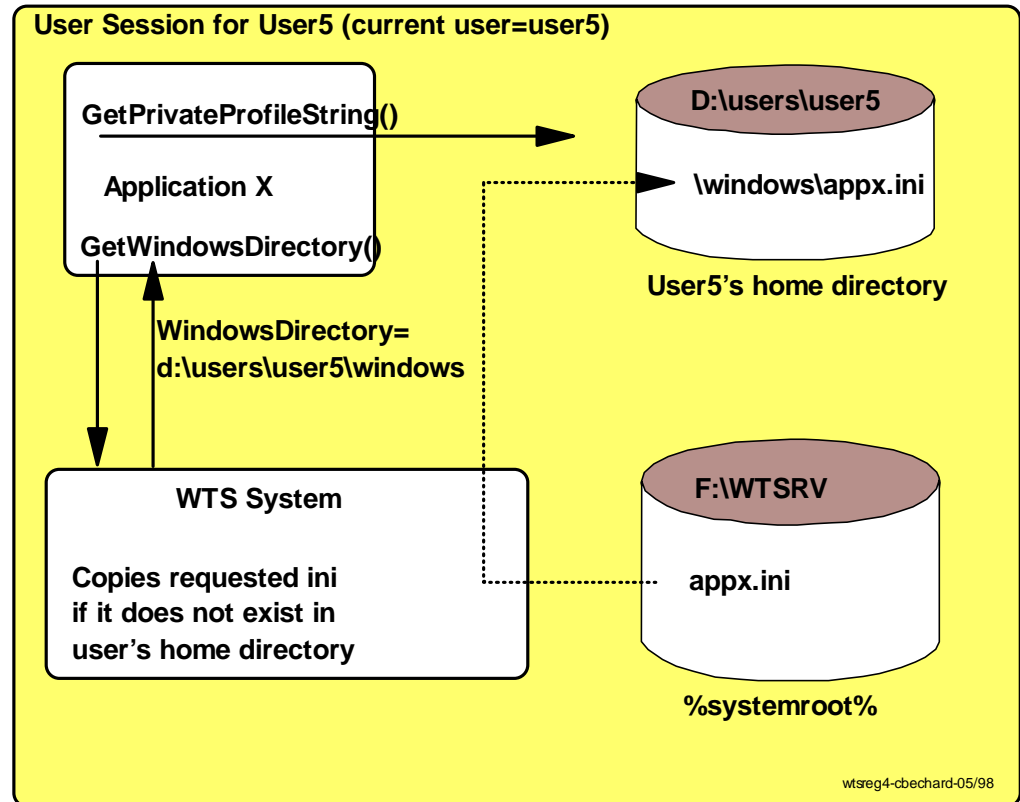


Figure 292. Copying INI Files to the User's Home Directory

The events above take place when an application starts executing and accessing resources in either an INI file or the Registry. However, there are also events that take place at the time that the user logs on.

4. When a user logs on, the system compares the date of the INI files located in the windows directory of the users' home directory with those in the %systemroot% directory. If an INI file in the %systemroot% directory is newer than the one in the user's private windows directory, the user's copy of the INI file is renamed to inifilename.ctx.

Then, when the application makes a request to read this INI file, a new copy of the INI file is created from the one located in the %systemroot% directory or from a merge of the old INI and the new INI.

Which action takes place (replace the old with the new, or merge the two) is driven by the setting of the INISYNC bit in the INI files compatibility flags.

See 18.10, "Controlling the Execute Mode" on page 346 for more details on using the compatibility flags.

5. When a user logs on, the system compares the Registry values under HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\Current Version\TerminalServer\Install with the user's version of these values under HKEY\_CURRENT\_USER. If the user's version is older, the user's version of these keys is deleted and replaced with the newer ones.

This action can be disabled, if necessary, by setting the appropriate compatibility flags. This can be done on an application basis or Registry entry basis.

See 18.10, “Controlling the Execute Mode” on page 346 for more details on using the compatibility flags.

In summary, the major steps illustrated in the figure below are:

1. The application X install process writes Registry entries in HKEY\_LOCAL\_MACHINE and/or HKEY\_CURRENT\_USER.
2. These entries are duplicated by the system (when the change user /install command is in effect) at a central location in HKEY\_LOCAL\_MACHINE.
3. These entries are copied to the current user’s HKEY\_CURRENT\_USER when the user logs on and executes application X.

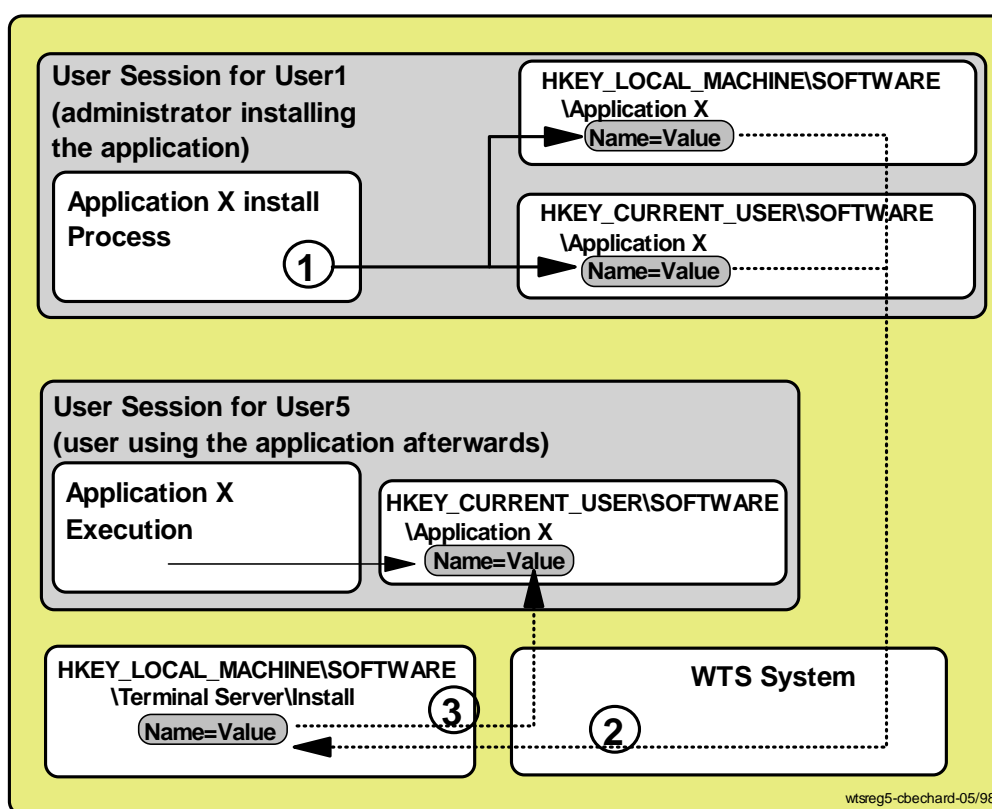


Figure 293. Summary - Change User Process

### 18.8.3 The change user /query Command

The change user /query command can be issued by the administrator in order to find out whether the system is already in install mode or in execute mode. This command is also used in application installation scripts in order to determine the status of the install mode.

An example of the use of this command in a command file is shown in Figure 302 on page 343.

---

## 18.9 A Few Practical Examples

In this section, we illustrate an installation process with actual examples in order to provide a better understanding of how this works. We use three examples:

1. A very simple application that uses only an INI file.

We use the PFE editor application for that purpose.

2. An application that uses Registry entries and user files, but that does not require modifications to the Registry entries after installation when using the home drive approach.

For this, we use the Lotus SmartSuite 97 application.

3. An application that uses Registry entries and user files, but that does require modifications to Registry entries after installation.

We use the Internet Explorer 3.0 application for that purpose.

This example also gives us the opportunity to show a case that makes use of the application installation scripts provided with the Windows NT Server 4.0, Terminal Server Edition beta2 code.

In order to make it easier to follow the examples, here is the environment that we use for all these examples:

- We define a user account with administrator's privilege, called Newuser, and we always use this account to perform the installation of the applications.
- We also use the Newuser account, once the required applications have been installed under this account, as a template to clone other user accounts that inherit all the characteristics of this account.
- We define a second user account called user1, which becomes our Windows NT Server 4.0, Terminal Server Edition user who logs on in order to use the application as any typical user.
- In order to simplify the examples first, we proceed as if we only had a few users, and we do not automate the process of automatically copying files with logon scripts. Instead we perform those steps manually, to better illustrate the process.
- We install all applications on the d: drive.
- The user's home directory is on d:\users. So, our Newuser's home directory is d:\users\newuser and our user1's home directory is d:\users\user1.
- The Windows NT Server 4.0, Terminal Server Edition system is installed on F:. It would normally be on C: but our test machine was already loaded with a copy of WinFrame on C: so we just used another drive.

### 18.9.1 An Application Using Only an INI File

This first example is the simplest case, where no additional action, apart from issuing the change user /install command, is required on the part of the administrator.

The application we use is called Programmer's File Editor (PFE), which is a free editor available from Alan Phillips at <http://www.lancs.ac.uk/people/cpaap/pfe>.

We chose this particular application because it is very simple (and a nice editor by the way) and because the latest version can in fact function both with an INI file or with Registry entries, dependent on what the user chooses.

This editor does not have an installation process. You just place the files in a directory of your choice, and simply execute PFE32.EXE. In this example, we use it simply as a 16-bit application that uses an INI file. No configuration action is required on the part of the user to use it that way.

Here are the steps that we follow:

1. We log on to the Newuser account, download the editor from the Web site we referenced above, and store the executable in a general directory called d:\tools.
2. At this time, the only thing we need to know is that this application, on being executed the first time by a user, requires an INI file to store the user's preferences. We could elect to have PFE store these preferences in the Registry if we wanted to, but let's assume that we do not use this feature for now; we only want to use an INI file.

If the INI file does not exist when the user starts the application for the first time, PFE creates one, which makes our job very easy, because it means that all we have to do is to make sure that user1 can access the PFE32.EXE file in D:\tools.

3. To make it easier for all users to start the PFE editor, we create a shortcut and put it in the All Users Start menu. This is all we need to do so we log off.
4. We then log on as user1. If this is the first time that we log on as user1, our home directory on d:\users\user1 is empty.
  - User1 starts the PFE Editor using the shortcut in our Start menu or directly from d:\tools\pfe32.exe.
  - The editor queries the system for the windows directory, and the system returns the value d:\users\user1\windows.
  - Since there is no PFE32.INI file in existence yet, the editor creates a copy of it on d:\users\user1\windows.
  - User1 uses the editor, sets a few preferences, which get stored in our own private copy of PFE32.INI, and then logs off.

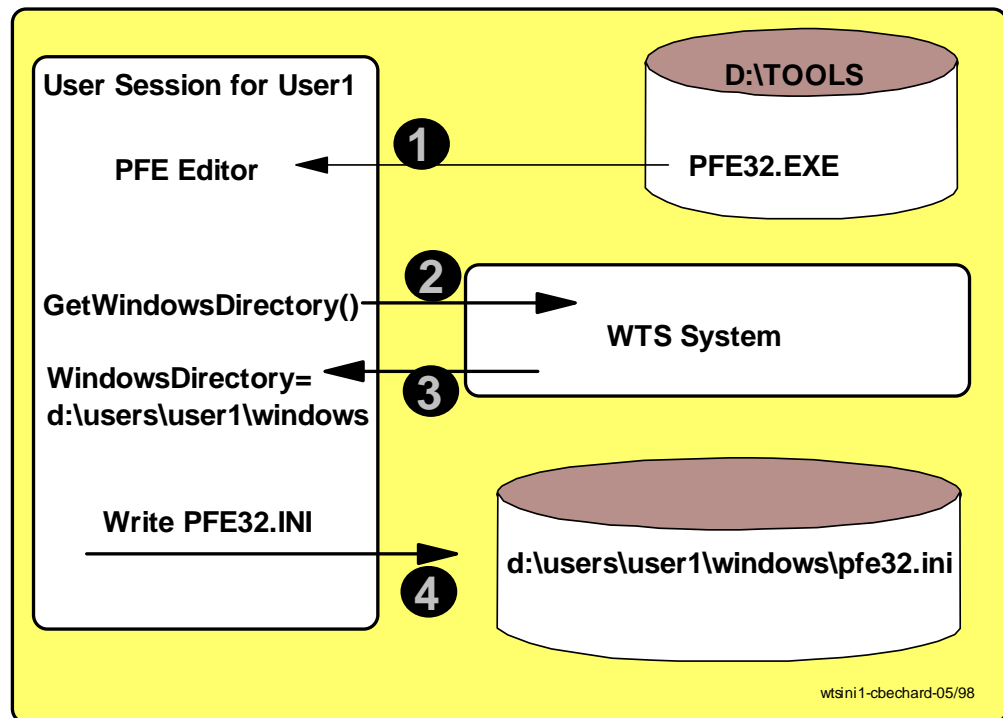


Figure 294. Creating a pfe32.ini File

5. Any other user logging on and going through the same process also gets a copy of the PFE32.INI created in his or her `d:\users\userx\windows` directory.

## 18.9.2 An Application Using Registry Entries and User Files

In this example, the Lotus SmartSuite 97 application installation process has a server install process and a node install process, which makes it easy to install in a multi-user environment.

In other words, SmartSuite has already been designed to be used in a client/server fashion, whereas the general code can be shared among users, and where individual users can keep a copy of their own private files.

Therefore, in the case of this application, all Registry entries that pertain to the application in general (that which applies to all users that might use this application) are stored in `HKEY_LOCAL_MACHINE`. On the other hand, when the user runs the node install portion of the installation, the entries are made in `HKEY_CURRENT_USER`, and, during that portion of the install, the user gets to specify where he or she wants the user files to be located.

In this case, the user files are files such as `\lotus\work\flg`, where the Freelance Graphics presentations get stored, or `\lotus\work\123` for spreadsheet files, or `\lotus\work\wordpro` for WordPro files.

Finally, even though this is a 32-bit application that makes use of Registry entries, strangely enough, it also uses a INI file such as `lotus.ini`.

### 18.9.2.1 Server Install Process

Let's examine the server install process first.

Our objective is to focus only on the aspects that are relevant to understanding the multi-user install process, so this is not a step-by-step description of the complete application installation process.

The main steps are as follows:

1. We log on as Newuser, and before starting the application installation process, we issue the change user /install command.
2. Equally important, we have defined this user just like all the other users, such that our home directory is d:\users\newuser and we have a home drive of W: that points to d:\users\newuser. This is an important part of the preparations, as we will see in a moment.
3. We then start the SmartSuite installation process, and when prompted, we select the file server or multiple users install. When prompted for the location of the installation files, we enter D: as the target drive. (Remember that this is the location where we decided to install all applications.)
4. There are then other choices we must make such as which applications within the SmartSuite the user wants to install, after which the server install process is basically complete.

So far, only the server portion of the application installation process has been done. Since we have more installation tasks to do, we want to remain within the change user /install mode for the next step.

Before we do the next step however, let's take a look and verify the actions that have taken place so far:

- Since drive d: was the specified installation target drive, the directories and files created by the server install process have been placed on D:. The figure below shows that the lotus directory was created on D:

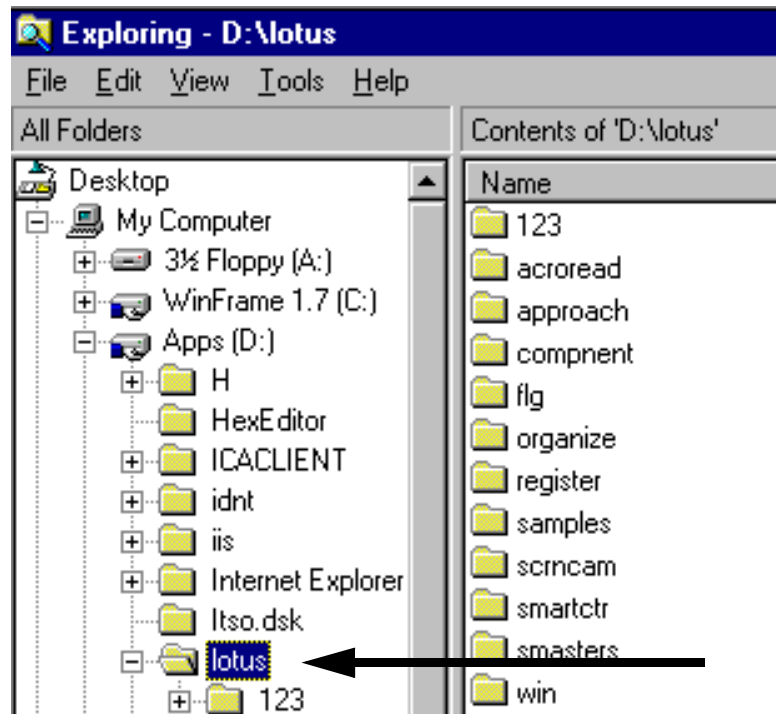


Figure 295. The SmartSuite Files Installed by the Server Install Process

- Many entries were made in HKEY\_LOCAL\_MACHINE for all the applications that are part of SmartSuite, such as WordPro, Freelance Graphics, 123, etc.

The next figure shows that a Lotus key (and many other subkeys) were added to HKEY\_LOCAL\_MACHINE/Software. The key currently selected for display is the Lotus/Freelance/97.0 key.

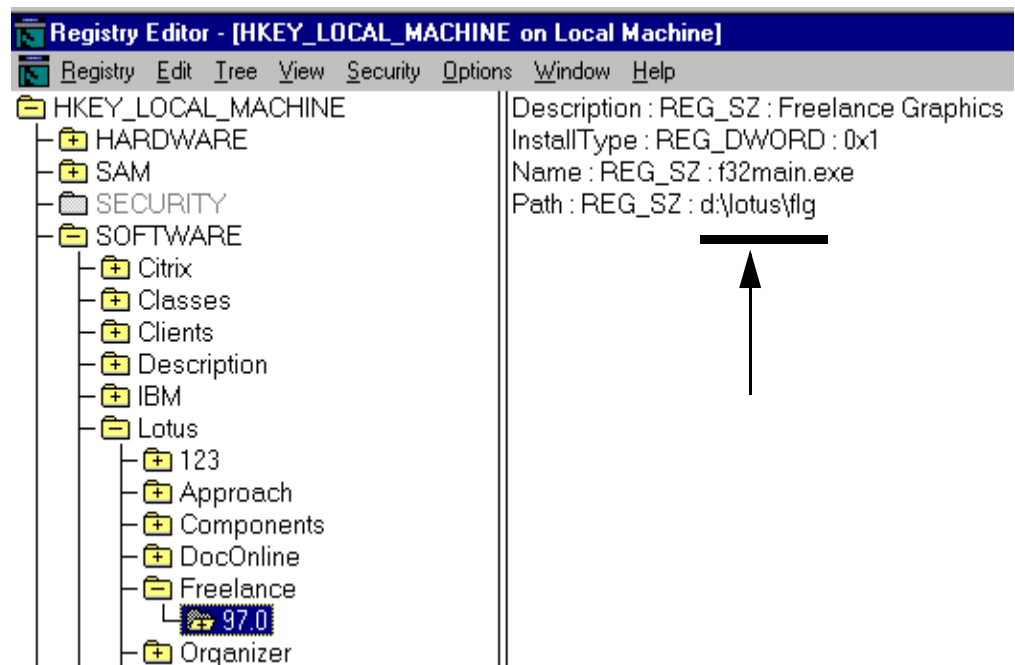


Figure 296. SmartSuite Entries in HKEY\_LOCAL\_MACHINE after Server Install

In the figure above (Figure 296), notice that the path of the main executable for Freelance is recorded in the Registry as D:\lotus\flg, which is correct, since this is where all users fetch the executable from.

- It is probably at this time as well (we have not verified exactly when this takes actually place) that a lotus.ini gets written to the windows directory.

#### **18.9.2.2 Node Install Process**

We are now ready to start the node install.

This is accomplished by opening up the SmartSuite folder and selecting **SmartSuite Node Install**. The steps are as follows:

1. At this point, if this was a normal single user installation, we would most likely specify the location of the target install directory for user files as d: since this is where the rest of the application components are located. However, in this case, we specify W: as the target destination, which is our home drive (meaning the home drive of user Newuser).
2. The process copies files, and then terminates, and we are asked if we would like to restart. We answer no in order to be able to issue a change user /execute command, now that the installation is complete.
3. We issue the change user /execute command in order to turn off the install process recording by the system.

Let's take a look at the results of the above node install process. The following key events took place:

- User files were created on the user's home drive (W:) which actually means that the files were created in d:\users\newuser, as is shown in the next figure. These user files are currently accessible only to the Newuser user, but every user will need a copy of these files in his or her own home directories as we will see in a moment.



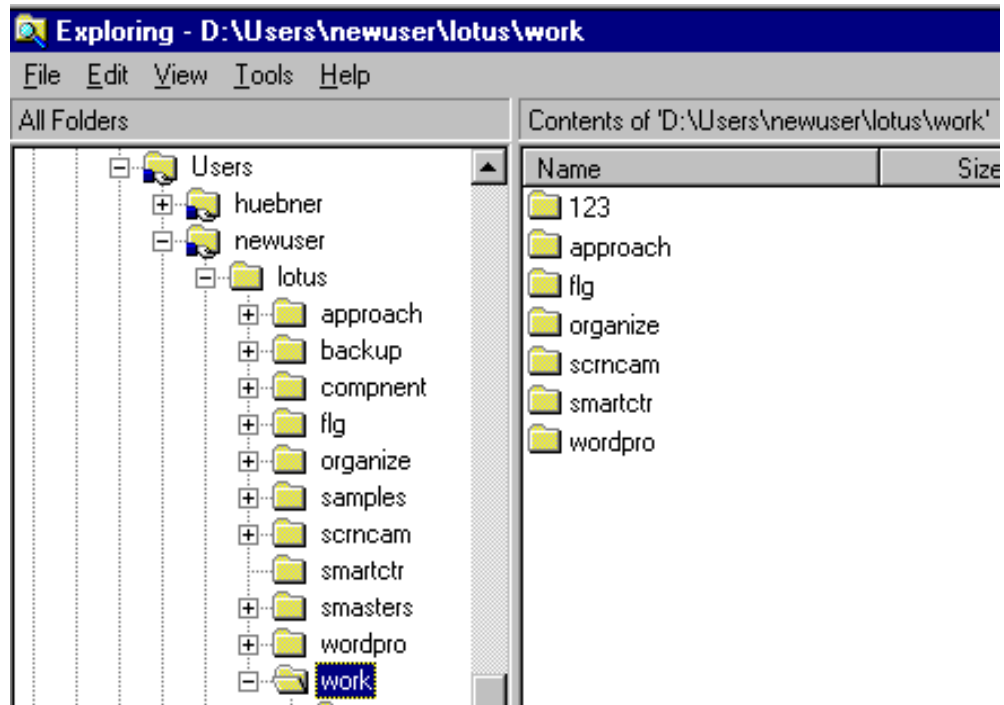


Figure 297. User Files for SmartSuite in the User's Home Directory

- Registry Entries were created in HKEY\_CURRENT\_USER to indicate the location of these user files. Many keys were created, because the SmartSuite includes many components and applications, so we can only show a few that are representative.

In the next figure, we highlight the key called Work for the Lotus 123 application to show that the path is indicated as w:\lotus\Work\123.

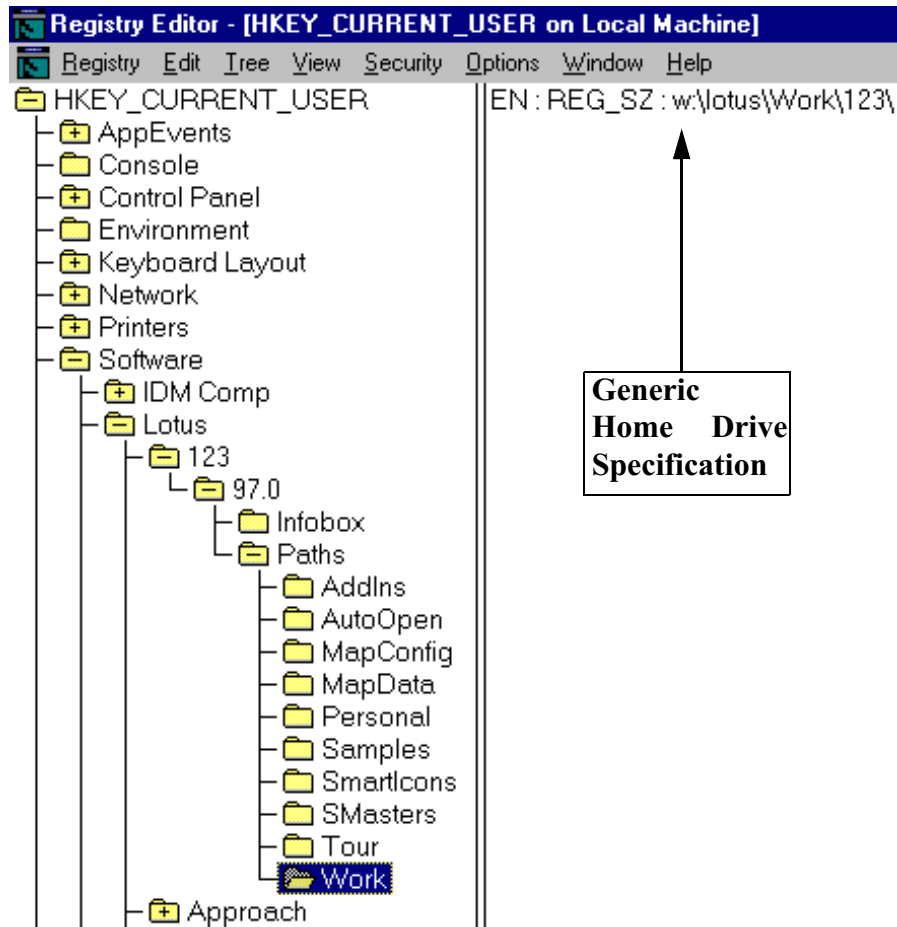


Figure 298. HKEY\_CURRENT\_USER Registry Entries after SmartSuite Node Install

- The entries that we see in the figure above have also been copied to a central location in HKEY\_LOCAL\_MACHINE, so that they can be copied to other users' HKEY\_CURRENT\_USER when these users log on later on.

Since these other users also have a W: home drive (but pointing to a different physical home directory), this entry (w:\lotus\work\123) is already generic and applicable to all other users that have a W: home drive.

We display, in the next figure, the same entries as they appear in the central location where they have been copied to. We could not show the whole path above the Terminal Server\Install\Software keys, but it is HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\Current Version.

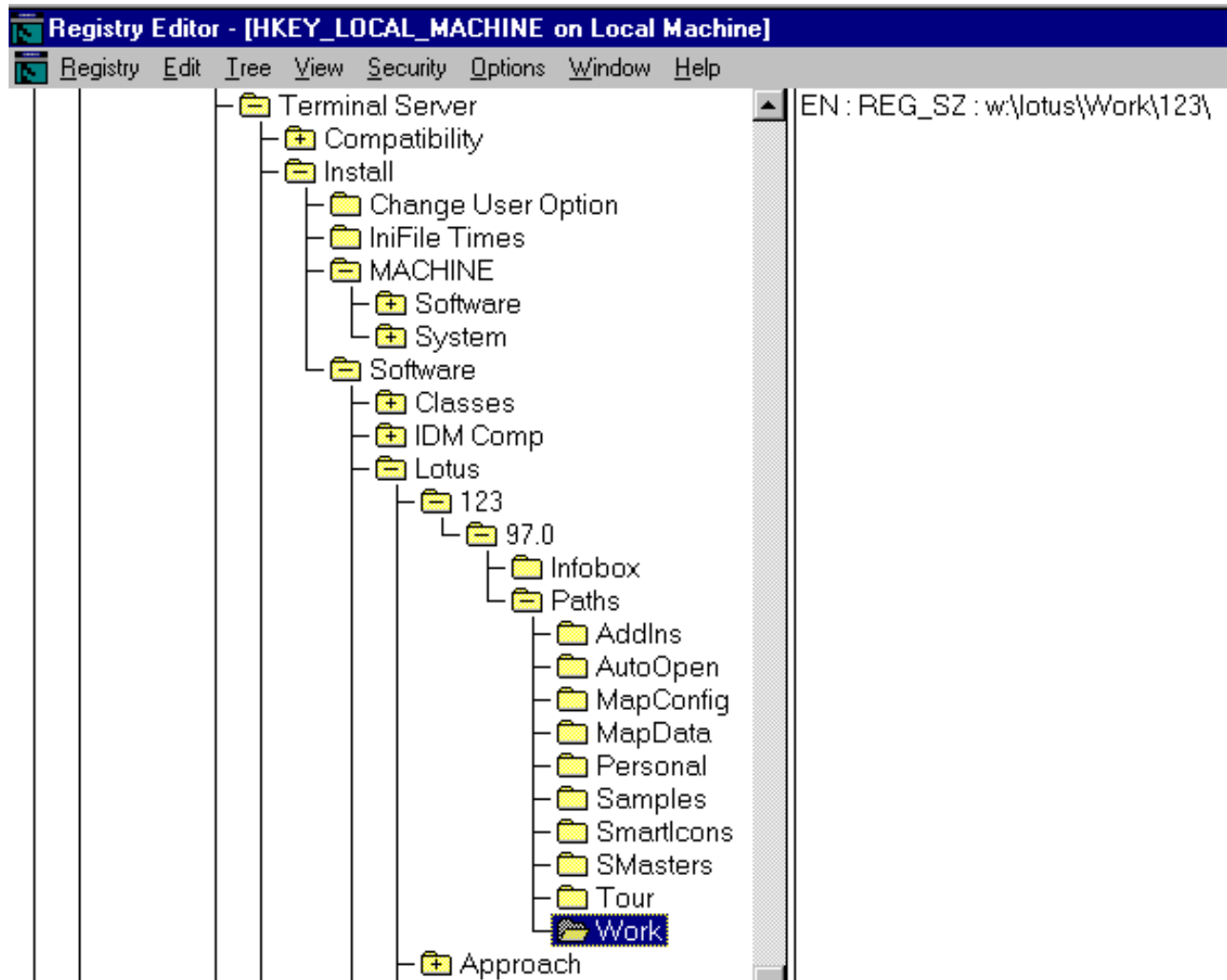


Figure 299. Terminal Server\Install\Software Registry Entries

### 18.9.2.3 Additional Installation Steps

There are still two tasks required so that user1, when he or she logs on, is able to use the SmartSuite applications:

1. The Start menu of user1 must include the SmartSuite application.

There are a few ways of doing this. In this case, we just copy the Start menu entries from the Newuser user to the All Users Start menu.

Another way is to copy the entire user profile from Newuser to user1 for example. See 18.7.3, "Example - Creating and Copying a User Profile" on page 321 for directions on how to copy a user profile.

2. The \lotus directory and all its subdirectories and files must be copied from the Newuser's home directory to the user1's home directory.

Here also, there are many ways of doing this, but in this example, for the sake of simplicity, we simply make a manual copy after we log on as user1. In order to do this, we set the permissions on the Newuser's home directory so that it can be read by everyone.

In a real environment, you would probably make this copy operation (for this application and all other applications) part of a logon script that gets executed at user logon time.

**Note:** The application script provided with the Windows NT Server 4.0, Terminal Server Edition beta2 suggests, for this application, that the user executes, at logon time, the node install procedure, which is another way of proceeding to accomplish the same objective. However, we find that copying the files provides an easier and simpler environment, especially if there are other files, for other applications, that need to be copied as well.

#### 18.9.2.4 User1 Logon Process

Everything is now in place for user1 to use the SmartSuite applications so we now logon as user1. The following events take place:

1. To simulate the logon script that we would normally have specified to be executed at this time, we manually copy the \lotus directory from d:\users\newuser to our own home directory d:\users\user1, or simply to w:, which is the same location.
2. We then execute one of the SmartSuite applications available on our Start menu.

This causes the application to request some Registry entries from HKEY\_CURRENT\_USER. Since these entries are not found there, this causes the system to copy all the required entries from the central location (HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\Current Version\Terminal Server\Install) to our HKEY\_CURRENT\_USER.

3. The lotus.ini file is also requested by the application from the user's private windows directory. Since it is not found, it also causes it to be copied from the systemroot to our d:\user\user1\windows directory.
4. The application can then properly execute and since all the Registry entries for user1 files point to w:\lotus\work\..., our user1 data gets stored in users1's own private home directory location.

In summary, the overall installation process for this application was pretty simple and required few special steps mainly because of the availability of a node install process that allowed the user to specify where the user files were to be located (that is, the user's home drive W:)

Let us now move on to an application that does not have such a process, and writes Registry entries only to HKEY\_LOCAL\_MACHINE to see what extra steps are needed to fix this.

### 18.9.3 An Application Using Registry Entries That Require Modifications

Our last application installation example is Microsoft's Internet Explorer 3.0 application.

We chose this particular application because it illustrates some of the Registry changes that are required when the application's installation process is not designed for a client/server environment.

This particular application also gives us the opportunity to demonstrate the use of one of the application scripts that are supplied with the Windows NT Server 4.0, Terminal Server Edition Beta2 to help with these types of problems.

### 18.9.3.1 WTSE Application Notes

In the online documentation that accompanies the Windows NT Server 4.0, Terminal Server Edition, the application notes for the Microsoft Internet Explorer 3.x application read as follows:

<i>Microsoft Internet Explorer 3.x</i>
<b>Description of Issues</b> By default, Internet Explorer stores the user's history, cookies, and temporary Internet files in the %systemroot% directory. Since this directory is read-only for normal users, they are unable to run Internet Explorer. Also, all users would share the same set of data, which is undesirable.
<b>How to Solve</b> After installing Internet Explorer, run the %systemroot%\Application Compatibility Scripts\Install\MSIE30.cmd script. This will change the directories used for the items listed above to W:\MSIE30, which is in the user's home directory.
<b>Customization</b> If the user's home directory is mapped to a drive letter other than W:, update the path in %systemroot%\Application Compatibility Scripts\Install\MSIE30.key.
<b>Limitations</b> None

Figure 300. WTSE Application Notes for MS Internet Explorer 3.x

More specifically, the IE 3.x installation process writes entries in HKEY\_LOCAL\_MACHINE that point to the following six locations. (In our example, remember that our %systemroot% is F:\WTSRV.)

- F:\WTSRV\Temporary Internet Files
- F:\WTSRV\Temporary Internet Files\Cache1
- F:\WTSRV\Temporary Internet Files\Cache2
- F:\WTSRV\Temporary Internet Files\Cache3
- F:\WTSRV\Temporary Internet Files\Cache4
- F:\WTSRV\Cookies

These entries actually are written to:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current  
Version\Internet Settings\Cache\Paths

and

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current Version\Internet  
Settings\Cache\Special Paths\Cookies

At this point, with what we understand already of what must take place (given the other examples we have looked at), the problem with this specific application is

that these Registry entries point to a specific location and are not generic enough to be used by all users.

Since the application did not give us the opportunity during the installation process to specify where we wanted these files to be located (so that we could have asked to place them on the W; home drive), we must correct this situation after the fact by modifying these Registry entries.

If we were not supplied with a pre-written script to perform this change, we would have to write a small command file. However, we do have one that is supplied to us, so let's examine how this works.

### 18.9.3.2 WTSE Application Scripts

These installation and logon scripts are located in the %systemroot%\Application Compatibility Scripts folder, as shown in the figure below:

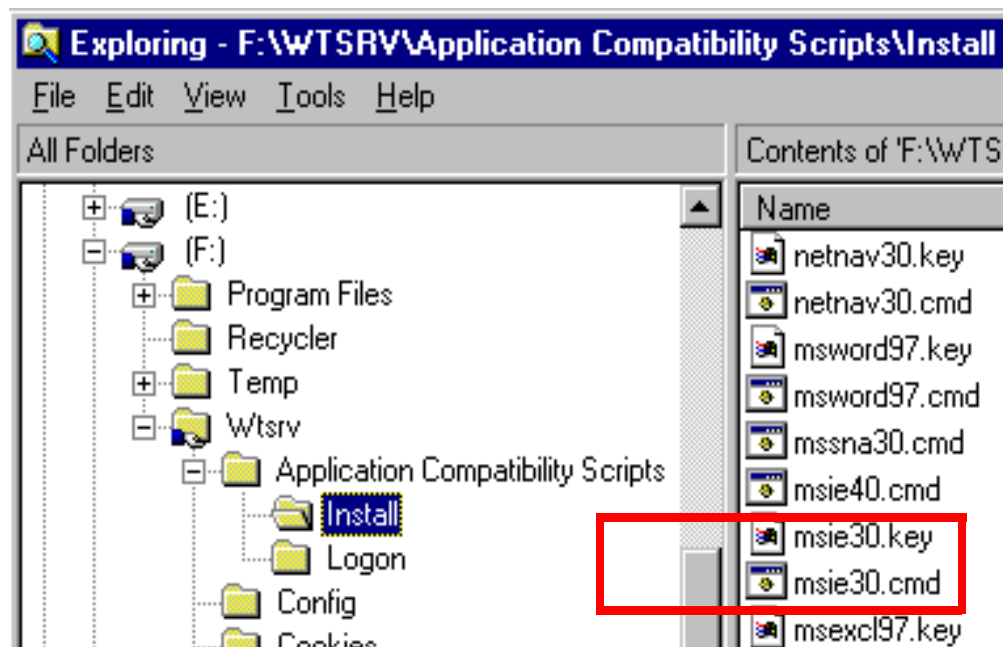


Figure 301. Application Installation and Logon Scripts

The script for this particular application is called msie30.cmd. Notice in the bottom right-hand corner of the above figure that there is also a file called msie30.key. This file is used by the msie30.cmd file and it contains the Registry key changes that need to be done.

Let's take a look at the actual content of the msie30.cmd file:

```

@Echo Off
Rem
Rem This script updates the installation of Microsoft Internet
Rem Explorer 3.x. It changes the path of the cache directory,
Rem history directory, and cookies file to the user's home
Rem directory.
Rem
Rem This script only needs to be run once after the installation,
Rem not for each user.
Rem
Rem NOTE: IF YOU MAP THE USER'S HOME DIRECTORY TO A DRIVE LETTER
Rem       OTHER THAN W: THEN THE MSIE30.KEY FILE MUST BE UPDATED
Rem       TO REFLECT THIS CHANGE.
Rem

Rem If not currently in Install Mode, change to Install Mode.
Set __OrigMode=Install
ChgUsr /query > Nul:
if Not ErrorLevel 101 Goto Begin
Set __OrigMode=Exec
Change User /Install > Nul:
:Begin

regini msie30.key > Nul:

Rem If original mode was execute, change back to Execute Mode.
If "%__OrigMode%" == "Exec" Change User /Execute > Nul:
Set __OrigMode=

Echo Microsoft Internet Explorer 3.x Multi-user Application Tuning Complete

```

Figure 302. The msie30.cmd File

What the above command file actually does, in plain language, is:

1. Check to ensure that the install mode is in effect, and, if not, change to install mode. This is required so that the system can record changes made to the Registry by this command file so that they can be propagated later to all users.
2. Issue the regini filename command, where filename is the accompanying msie30.key file that is complimentary to this msie30.cmd file. The content of that file is displayed in the next figure (Figure 303).

The regini command is a utility, supplied with the Windows NT 4.0 Server Resource Kit that uses batch files to add keys to the Registry by specifying a Registry script.

#### Important

Changes to the Registry entries should not be manually because a manual editing does not alter the time stamp for the entry, which prevents the changes to be propagated automatically by the system.

As is shown in the msie30.key file below, the regini command execution causes the paths of the six files we identified earlier to be changed to W:\MSIE30\etc.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Cache
  Paths
    Directory = DELETE
    Path1
      CachePath = DELETE
    Path2
      CachePath = DELETE
    Path3
      CachePath = DELETE
    Path4
      CachePath = DELETE
  Special Paths
    Cookies
      Directory = DELETE

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Cache
  Paths
    Directory = W:\MSIE30\Temporary Internet Files
    Path1
      CachePath = W:\MSIE30\Temporary Internet Files\Cache1
    Path2
      CachePath = W:\MSIE30\Temporary Internet Files\Cache2
    Path3
      CachePath = W:\MSIE30\Temporary Internet Files\Cache3
    Path4
      CachePath = W:\MSIE30\Temporary Internet Files\Cache4
  Special Paths
    Cookies
      Directory = W:\MSIE30\Cookies
```

Figure 303. The msie30.key File

Note that these files (Cache1, Cache2, Cache3, Cache4 and Cookies) get created by the application at execution time; therefore there is no need to copy these files from Newuser to user1, as we did in the previous example for the Lotus files.

This also means that you should not execute the application before executing the msie30.cmd script that changes the paths since these files would then be created in the wrong location.

Another important point mentioned and highlighted in the installation script is that the administrator needs to update the script to change the home drive specification if he or she uses a home drive letter other than W:.

The figure below shows one of these paths in the Registry. The path above the Windows key is HKEY\_LOCAL\_MACHINE\Software\Microsoft\.



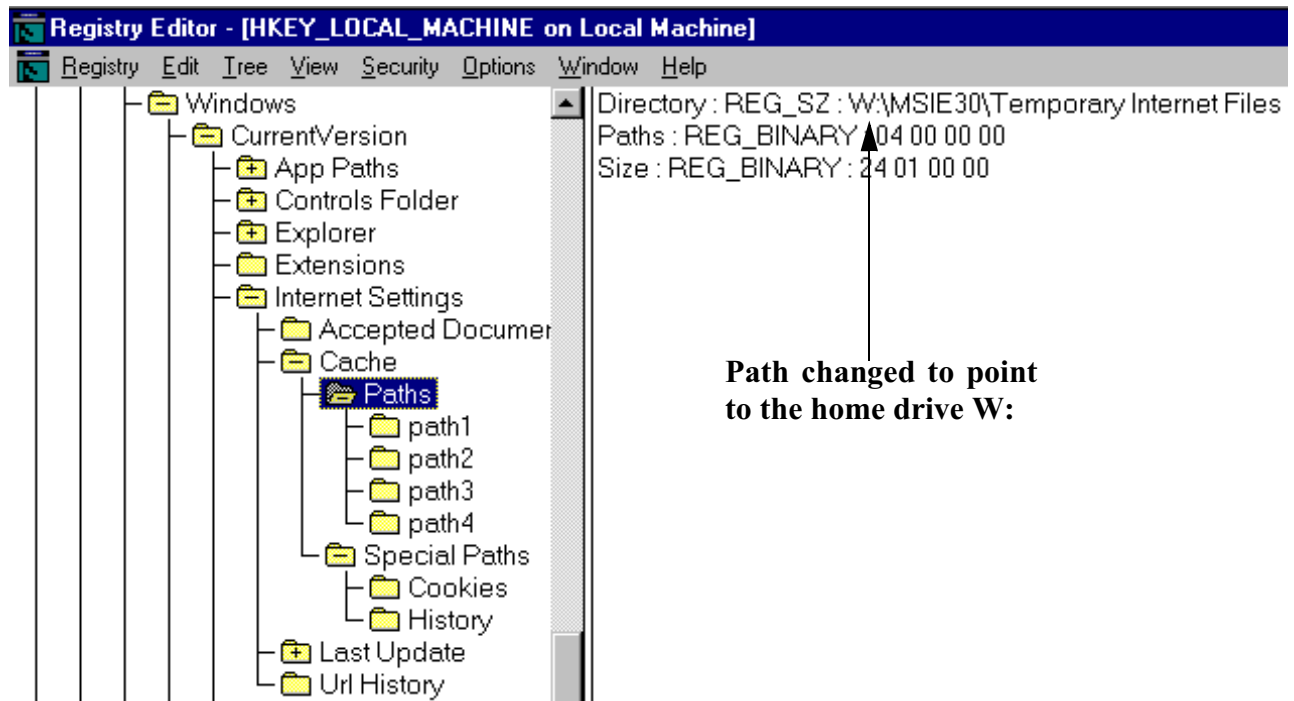


Figure 304. Registry Entries after the msie30.cmd Script Execution

### 18.9.3.3 MSIE30 Application Installation Steps

Now that we are familiar with the application and the changes that are required, and we have examined the scripts, we are ready to proceed with the actual installation.

The steps are as follows:

1. We log on to the Newuser account.
2. We issue the command `change user /install`.
3. We run the application installation process and let it complete. This has created the Registry entries in HKEY\_LOCAL\_MACHINE, with paths pointing to F:\WTSRV.
4. We now execute the msie30.cmd file to change the Registry entries such that the paths point to our home drive W:.
5. We issue the command `change user /execute` to get out of install mode.
6. We do not need to copy the application shortcuts to the All Users Start menu since it is already there by default (in the case of the Internet Explorer).
7. We log off the Newuser account.
8. We log back on as user1 and execute the Internet Explorer.

The application fetches the paths from the Registry entries in HKEY\_LOCAL\_MACHINE and since these now point to W:, the required files are created in the d:\users\user1\msie30 directory.

There are a couple of other files used by the Internet Explorer, such as a History folder and a Favorites folder (bookmarks) that do not need to be changed in any way. The Favorites folder is stored under the user's profile, which makes it

automatically specific to each user. Similarly, the History folder is a special folder that is shared by users but without creating any problems.

#### 18.9.4 Summary - Examples

This concludes this section on practical examples. We could go through many other examples, but they would all be somewhat similar in the sense that the same techniques can be used to solve most compatibility issues.

Of course, many applications can exhibit some particularities that have not been encountered before that might require some special action to be taken, but overall, the techniques illustrated above will function for the majority of applications.

There are many more scripts that are supplied with the Windows NT Server 4.0, Terminal Server Edition. See 18.15, "Application Notes in Windows NT Server 4.0, Terminal Server Edition" on page 354 for a list of the other applications notes available.

---

### 18.10 Controlling the Execute Mode

As discussed above in 18.8.2, "The change user /execute Command" on page 327, there are many actions and events that take place at the time that the user logs on, such as comparing the dates of the INI files in %systemroot% with those in the user's home directory, and comparing the time stamps of Registry entries in the central location with those of the HKEY\_CURRENT\_USER location.

An administrator can influence how the system behaves (and override the default behavior) at the time that the user logs on by setting some special Registry entries called compatibility flags.

For example, if the administrator has updated an INI file and he or she now wants the same INI file which is located in the user's home directory to be replaced with this new one the next time that the user logs on, he or she can set a bit in the IniFiles Registry key to alter the default behavior of the system, which is to merge the INI files instead of replacing them.

There are three Registry keys that contain compatibility flags:

- Applications
- IniFiles
- Registry Entries

These keys are located as shown below:

1. For Windows NT Server 4.0, Terminal Server Edition:

```
HKEY_LOCAL_MACHINE
\Software
\Microsoft
\Windows NT
\Current Version
\Terminal Server
\Compatibility
\Applications
\IniFiles
```

\Registry Entries

## 2. For WinFrame

```
HKEY_LOCAL_MACHINE
  \Software
    \Microsoft
      \Citrix
        \Compatibility
          \Applications
            \IniFiles
              \Registry Entries
```

The figure below displays these keys, but starting at the Terminal Server key. Notice as well the Install key (which is the next key after the Compatibility key), under which the MACHINE and Software keys reside, which are used to store Registry entries created while the system is in change user /install mode.

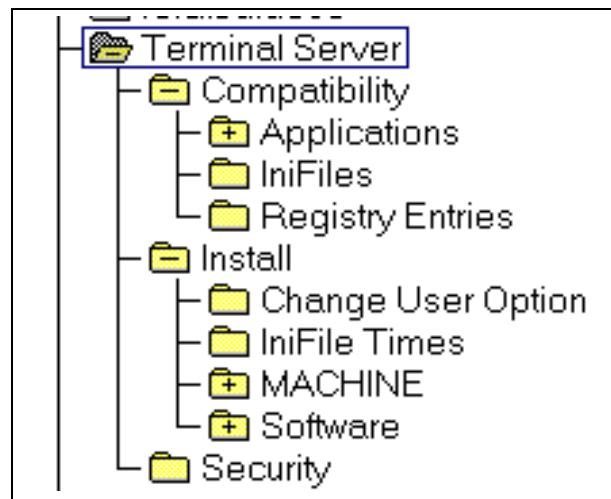


Figure 305. WTSE Registry Compatibility Keys

### 18.10.1 Applications Compatibility Flags

Under the Applications key, you can add new keys for each application whose behavior you need to influence. The key to be added is made up of the application's executable file name. For example, the PFE editor's executable name is pfe32.exe, so the key name would be Compatibility\Applications\pfe32.

You then create a name called Flags under that key, and set its value according to the following table:

Table 9. Applications Compatibility Flags Settings

Action or Condition	Flags Setting
DOS application	0x00000001
OS/2 application	0x00000002
Windows 16-bit application	0x00000004
Windows 32-bit application	0x00000008

Action or Condition	Flags Setting
Return username instead of computername	0x00000010
Return Citrix build number	0x00000020
Disable Registry mapping for this application	0x00000100
Do not substitute user Windows directory	0x00000400

Here is a brief explanation of some of the entries applicable to the table above and the two other tables that follow:

- For each application, you can indicate the type of application (DOS, OS/2, Windows 16-bit or Windows 32-bit). This is useful if you have multiple files that have the same executable name for example, but are of different types.
- The Return username instead of computername flag is used for applications that use the computer name as a unique identifier. In a multi-user environment, using the computername for each copy of the running applications does not provide the required uniqueness, but if username is used instead of computername, then each instance of the application has a unique identifier.
- The Disable Registry mapping for this application flag causes the system to add new entries from the system master Registry image to the user's Registry when the application is started, without deleting any existing entries. The default action is for the system to delete and overwrite the user's Registry data if it is older than the system master Registry data.
- The Do not substitute user windows directory flag instructs the system to return the real %systemroot% directory when the application issues the GetWindowsDirectory API call instead of returning the user's windows directory located in the user's home directory.
- The Synchronize user INI file to system version flag causes the system to add new entries from the system master INI file to the user's version of the INI file when the application is started, without deleting any existing entries. The default action is for the system to delete and overwrite the user's INI file if it is older than the system master INI file.

The next figure shows an example of setting the compatibility flag for the REGEDIT.EXE application to 0x108. This indicates that we use the Disable Registry mapping (0x00000100) for this Windows 32-bit application (0x00000008).

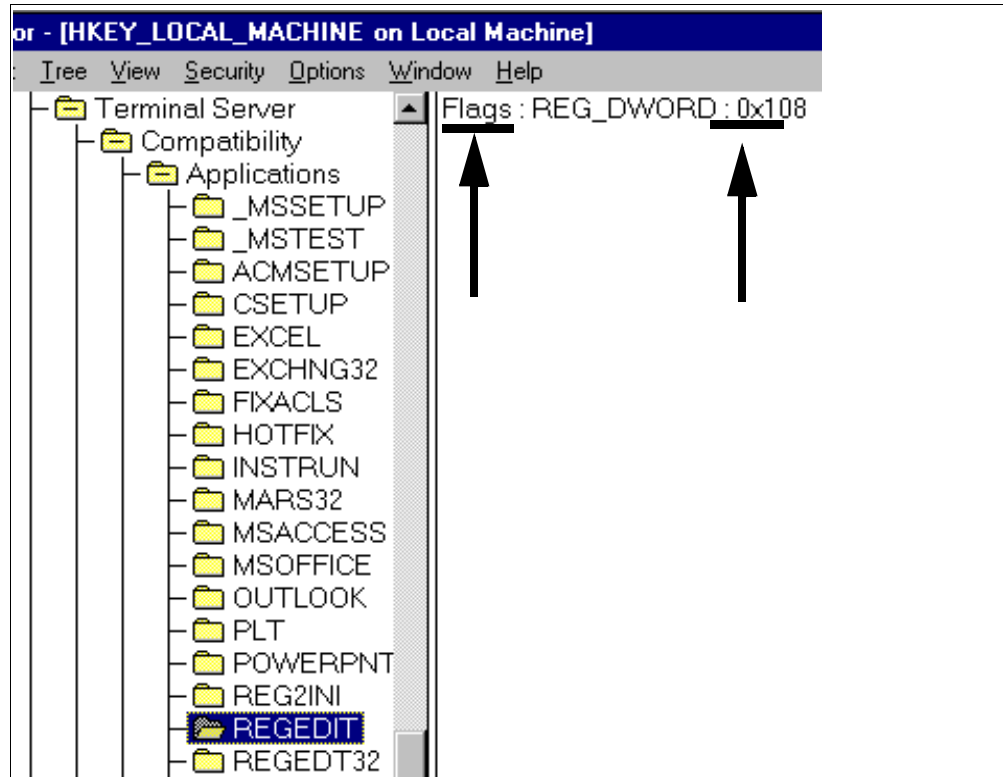


Figure 306. Example - Compatibility Flags for the REGEDIT Application

### 18.10.2 IniFiles Compatibility Flags

Similarly, the compatibility flags settings for IniFiles are as follows:

Table 10. IniFiles Compatibility Flags Settings

Action or Condition	Flag Settings
Windows 16-bit application	0x00000004
Windows 32-bit application	0x00000008
Synchronize user INI file to system version	0x00000040
Do not substitute user windows directory	0x00000080

### 18.10.3 Registry Entries Compatibility Flags

The flags for the Registry entries are as follows:

Table 11. Registry Entries Compatibility Flags Settings

Action or Condition	Flag Settings
Windows 32-bit application	0x00000008
Disable Registry mapping for application	0x00000100

---

## 18.11 Networking Applications Limitations

For applications that need to use the networking facilities of the server, there are some potential limitations, dependent on how a particular application is designed to operate.

The potential limitations are as follows:

- Unique network address

To operate properly in a multi-user environment, an application must be able to negotiate a unique private socket for each instance of the application that is started. Using a hard-coded socket and relying on a network interface card's address as the unique identifier does not permit applications to operate properly in a multi-user environment.

- NetBEUI and NetBIOS

Applications that use a specific name as the unique identifier will not operate properly because all users would use the same name.

- Gateways

Applications connecting to mainframes that use the network interface card's address as the session and user identification are limited to only one user. The solution here is to use a gateway so that the application, if it uses a virtual socket-based protocol, can allow multiple concurrent users.

- Novel NetWare NDS requirements

Users can be authenticated by, and use the resources of a NetWare NDS (NetWare 4.x) environment, but they must be able to operate in a NetWare bindery environment because NDS-specific APIs are not supported.

---

## 18.12 Updating INI Files and Registry Entries

If there is a need to edit the win.ini or system.ini files, even though they appear as text files, they should not be modified using a standard text editor such as the Windows NT Notepad because the changes made that way are not propagated by the system.

Instead, the SYSEDIT utility should be used after issuing the change user /install command. In other words, any changes to INI files must be made through the proper API calls, that is GetPrivateProfileString to read an INI file and WritePrivateProfileString to write an INI file, in order to enable the system to monitor these activities when in change user /install mode.

Similarly, Registry keys must be created and updated using the proper Registry API calls, such as RegOpenKeyEx, RegCloseKeyEx, RegEnumKeyEx, RegDeleteKeyEx, RegQueryValueEx and RegSetValueEx. If keys are manually edited, a time stamp on the Registry entry is not done and this prevents these keys from being properly propagated when the user logs on.

---

## 18.13 Using the Registry Editor

As you learn how to deal with these compatibility issues, you need to use the Registry editor in many cases to examine the contents of Registry keys. To open the editor, click on **Start**, then **Run**, and enter either regedt32 or regedit.

### Caution

The Windows NT Registry is a system database which, if improperly modified, can cause you to have to re-install your system, so you should exercise caution in the use of the Registry editor.

The first precaution to take before working with the Registry is to make a backup copy. You can use the Repair utility (rdisk.exe) for that purpose, as it stores a backup copy of the Registry in the Repair folder (and on the Repair diskette if you create one), but this is not a substitute for a real backup of your system.

There are two versions of the Registry editor that provide a similar but slightly different display of the Registry keys.

We have not done an extensive analysis of these two versions, but the main visual difference is in the right-hand side of the display where regedit displays icons to identify the type of value (string, word, binary) as opposed to the REG\_SZ, REG\_DWORD and REG\_BINARY keywords used by regedt32. The regedit version also displays all the hives in the same window whereas regedt32 uses a separate window for each hive.

Another difference is in the search capability; regedit allows you to specify whether you are searching for a key, a value or data whereas regedt32 only searches for a key. This search facility is of great help given the size of the Registry, when looking for a particular piece of data. (The Windows NT Resource kit also contains a regfind.exe command line utility that can be used to look for data in the Registry.)

Finally, regedit also lets you save a key name to the clipboard by selecting **Copy Key Name** after a right mouse click on the key that you want. This is useful for including Registry keys in documents or command files.

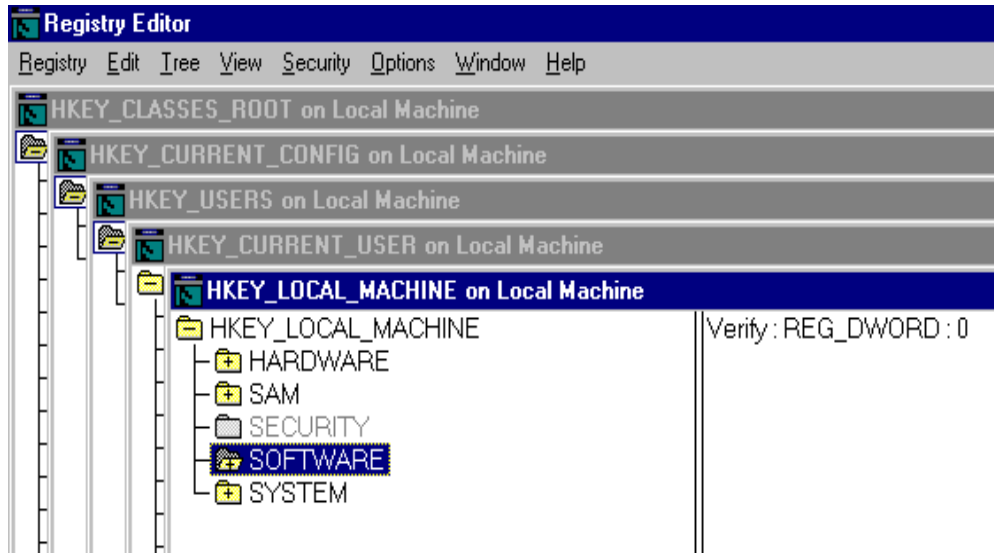


Figure 307. REGEDT32 Version of the Registry Editor

The figure above illustrates the REGEDT32 version of the Registry editor. Note that the name Verify is indicated as REG\_DWORD: 0 whereas the same value displayed in the next figure shows as the name Verify with an icon representing the fact that this is a DWORD.

The other important visual difference that can be seen between these two panels is that each Registry hive in the figure above is a separate window whereas the same hives appear, in the figure below, on the same window but as different tree branches.

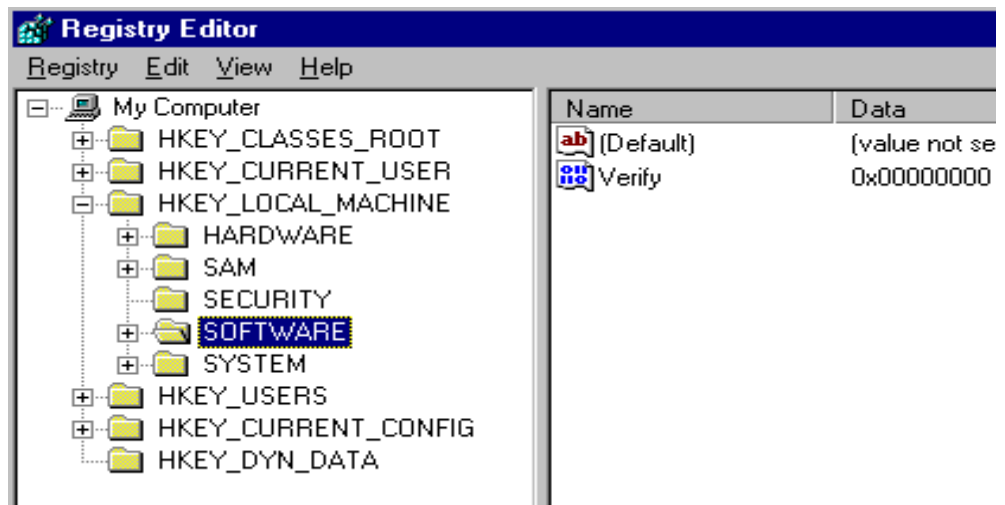


Figure 308. REGEDIT Version of the Registry Editor

## 18.14 Summary

Summarizing all of the steps and notions we have covered here is not necessarily easy, but let us attempt to do this using the following diagram:



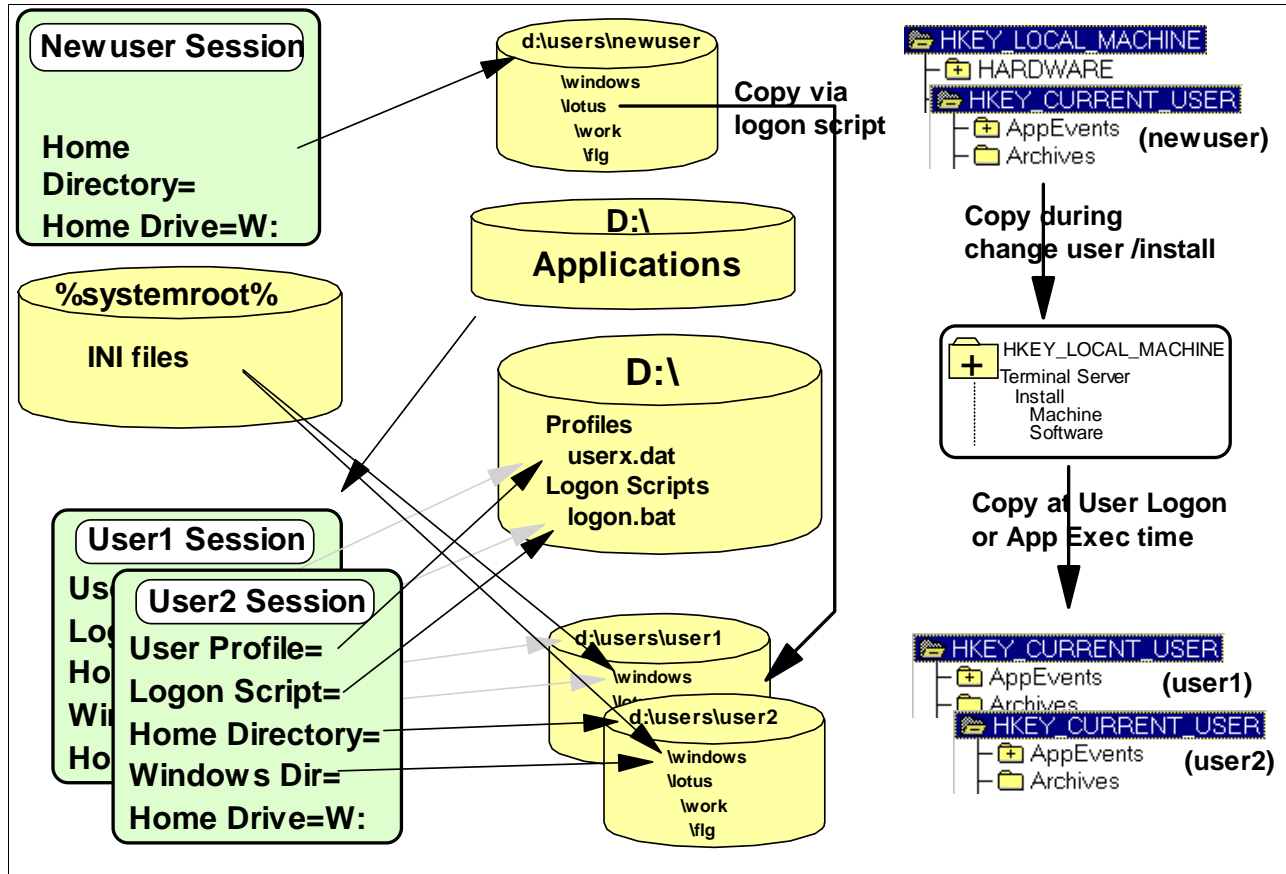


Figure 309. Summary

Assume that we use the Lotus SmartSuite application that we used as an example previously, and let us review the major steps that we would take, as an administrator, to install that application.

Since you are now familiar with the tools, techniques and components involved, and how the system is supposed to function, this final summary example might help to put it all in perspective.

The general simplified procedure would be as follows:

1. We log on as user Newuser. This user is already set up with a home directory and a home drive W:.
2. We issue the change user /install command.
3. We start the application installation process and specify D: as the target for the server part of the installation (that is, all general application files go on D:), and W: as the target if there is a node install portion to specify the location of the user-specific files.
4. While in Install mode, the system registers all changes made to the Registry and copies these entries to a central location in HKEY\_LOCAL\_MACHINE. It also copies any INI files created to the %systemroot% directory.
5. When the installation completes, we issue change user /execute.

6. After installing all the required applications, we copy the Newuser profile to a central location, say somewhere on a file server for example. When we define users, we specify that location as the location of the profile so that all users get the same profile (if appropriate, because you can also have many profiles, such as engineering users, accounting users, and so on).
7. We build a logon script to be used by all users, which copies user application files from the newuser home directory to the user's home directory in order to complete the duplication of the Newuser user to all users. When we define users, we specify the location of that logon script.
8. When we define a new user, say user1, we build his or her account such that we identify his or her profile as the centrally stored profile. We identify the logon script to be used at logon time, his or her home directory and home drive.
9. When user 1 logs on, all the user files from the template account Newuser are copied to the user's home directory, and when the user starts the SmartSuite application(s), required INI files are copied from the %systemroot% to the user's windows directory on his or her home directory location, Registry entries are copied from the central location to his or her HKEY\_CURRENT\_USER, and he or she is ready to use the application without interfering with any other users.

---

## 18.15 Application Notes in Windows NT Server 4.0, Terminal Server Edition

With the Windows NT Server 4.0, Terminal Server Edition code, there are application notes supplied for a number of applications which we list below.

We have illustrated above (see Figure 300 on page 341) the application notes for Internet Explorer 3.x as an example. Other application notes are similar and also describe the issues involved for a particular application and how to solve these issues, either through manual changes or through installation scripts and/or logon scripts, how to customize these scripts if required and finally lists any limitations if there are any.

Application notes are supplied for the following applications, which are taken directly from the terminal.doc document in the root directory of the WTS GA CD:

- Corel Office7
- Corel WordPerfect Suite 8
- Executive Software Diskeeper 2.0
- Lotus SmartSuite 97
- Microsoft BackOffice 2.5
- Microsoft BackOffice 4.0
- Microsoft Clipboard Viewer
- Microsoft Dr. Watson
- Microsoft Excel 97 (stand-alone installation)
- Microsoft Exchange 4.0 and 5.0 and higher
- Microsoft Exchange Server 5.5
- Microsoft FoxPro 2.6a
- Microsoft FrontPage 98
- Microsoft Internet Explorer 3.x
- Microsoft Internet Explorer 4.0
- Microsoft Network Monitor

- Microsoft ODBC
- Microsoft Office 4.3 and Office 4.3 Applications
- Microsoft Office 95 and Office 95 Applications
- Microsoft Office 97 and Office 97 Applications
- Microsoft Project 95
- Microsoft Project 98
- Microsoft SNA Server 3.0
- Microsoft SNA Server and Client 4.0
- Microsoft Word 97 (stand-alone installation)
- Netscape Communicator 4.x
- Netscape Navigator 3.x
- Novell IntraNetWare Client for Windows NT 4.11a
- Seagate Backup Exec 7.0
- Sybase SQL Anywhere

---

## 18.16 WinCenter's Multi-User Application Manager

If you are using WinCenter, there is another tool that the administrator can use to help with making applications available to multiple users. This is not a replacement for the change user /install facility, but it can be used *in addition to* the change user /install facility, and even in addition to installation scripts, in order to supplement them with additional actions that may need to be performed.

### 18.16.1 What Is Multi-User Application Manager (MAM)?

This tool is called the Multi-User Application Manager (MAM); it is a user friendly GUI front end that is used to create command files that perform actions equivalent to what application installation scripts and user logon scripts perform.

In other words, instead of using the application installation and logon scripts that we have seen in the previous chapters, or in the case where there are no application scripts supplied for the application that you need to install, the MAM tool provides an easy way of generating these scripts, provided that you already know which actions need to be performed.

There are two terms that you should be familiar with when discussing the MAM tool: templates and policies.

### 18.16.2 MAM Templates

A template describes a series of actions to be performed. It is therefore the equivalent of an installation and logon script. It is created with the MAM tool, and it can include the following actions:

1. Create, modify or delete Registry entries

For example, this could be similar to the changes we made using the msie30.cmd and msie30.key files in 18.9.3, "An Application Using Registry Entries That Require Modifications" on page 340.

2. Modify INI files

This tool makes modifications to INI files using the proper API calls, so that these changes are properly handled by the system while in change user /execute mode.

3. Create, delete and rename directories

#### 4. Copy files from one location to another

This can be used to copy files from a template user's home directory to a new user's home directory, such as the lotus\work files we copied in one of the previous examples.

#### 5. Execute commands

This can be any additional commands that need to be executed, in addition to all of the above.

The main advantage of this tool is that it makes it easy and safe for an administrator to make modifications to the Registry or to INI files for example without any special knowledge of how to write command files.

Note that even though this tool helps with creating command files, the administrator must still be aware of exactly which actions need to be performed before he or she can use this tool.

### 18.16.3 MAM Policies

Once you have one or more templates created, you can also define a policy that specifies which particular template(s) should be executed for a particular user or group of users.

The MAM tool can therefore, through the use of policies, control which specific actions need to be performed for a particular user.

### 18.16.4 MAM Edit and Execution Mode

The MAM tool has two modes:

1. When in Edit mode, it is used by an administrator to create templates and policies.
2. When in Execute mode, it is used to execute the actions defined in the template files. If policies have been defined, the templates specified by those policies are executed.

### 18.16.5 Should I Use MAM or Not?

When is it appropriate to use MAM?

This MAM tool is a WinCenter based-tool and is therefore applicable only if you use WinCenter. If you only have a WinFrame or Windows NT Server 4.0, Terminal Server Edition, then MAM is not applicable.

However, if you are using WinCenter the use of MAM is not mandatory. For example, if the installation scripts supplied with Windows NT Server 4.0, Terminal Server Edition are sufficient for your needs and you are setting up a generic logon script for all users, you do not have to use MAM.

On the other hand, if you want to further customize the existing scripts, create brand new ones, or use policies to control the actions to take place at user logon time, then MAM is certainly an appropriate tool for those purposes, especially if you are somewhat unfamiliar with writing command files.

For more details on MAM, see the NCD's *WinCenter Connect System Administrator's Guide*, Chapter 3, entitled "Setting Up Multi-User Applications".

### 18.16.6 Sample MAM User Interface

The figure below illustrates the main MAM panel, when used in Edit mode to create templates.

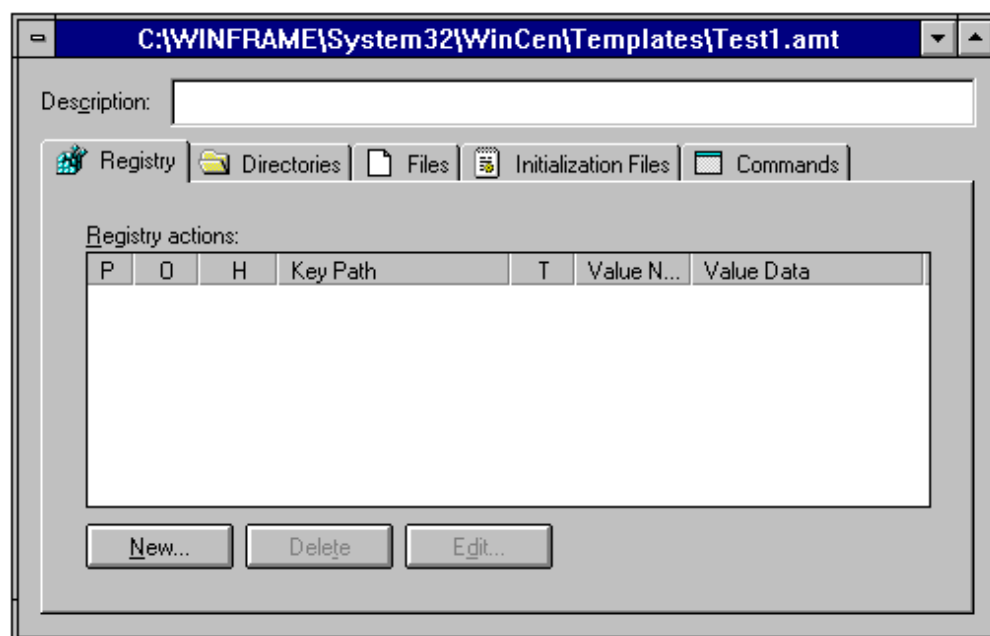


Figure 310. The MAM Template Editor - Main Panel

Notice that the above window has five tabs, one for each of the main category of actions that can be performed:

1. Registry
2. Directories
3. Files
4. Initialization Files
5. Commands

Let's take the Directories tab first to illustrate how this works.

Assuming that we want to either create directories or delete directories, when this template is executed, we can specify the actions desired as follows:

- In the figure below (Figure 311), if we click on the New... button, we get the New Directory Action panel, where we can specify a Directory path and the action to be performed, be it Make Directory as is chosen on this panel, or delete a directory.
- Notice as well the right pointing arrow to the right of the directory pathname, which produces the list displayed here in the bottom right-hand corner of the figure.

This action is similar on all the other panels that follow.

- This list allows the user to easily include some useful and typical paths such as, in this example, the user's home directory. By selecting that entry in the list, the %HOMEDRIVE%%HOMEPATH% variable is automatically inserted in

the directory pathname, to which the user can append a specific unique directory name.

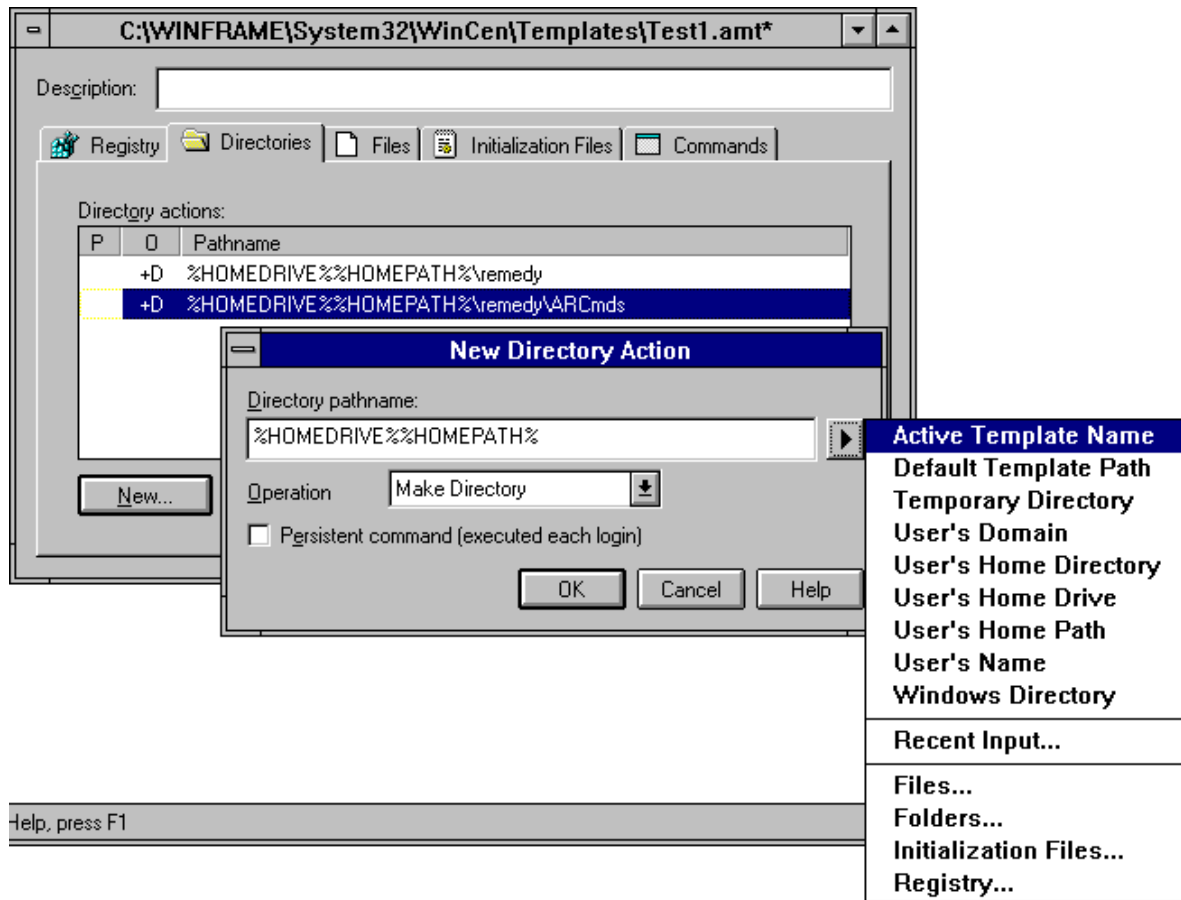


Figure 311. MAM Templates - Directories Actions

- Notice as well that you can select Recent Input... to select previous entries without having to re-key them.
- The last four entries (Files, Folders, Initialization Files and Registry) are a shortcut that takes you directly to browsing files, folders, INI files or the Registry.

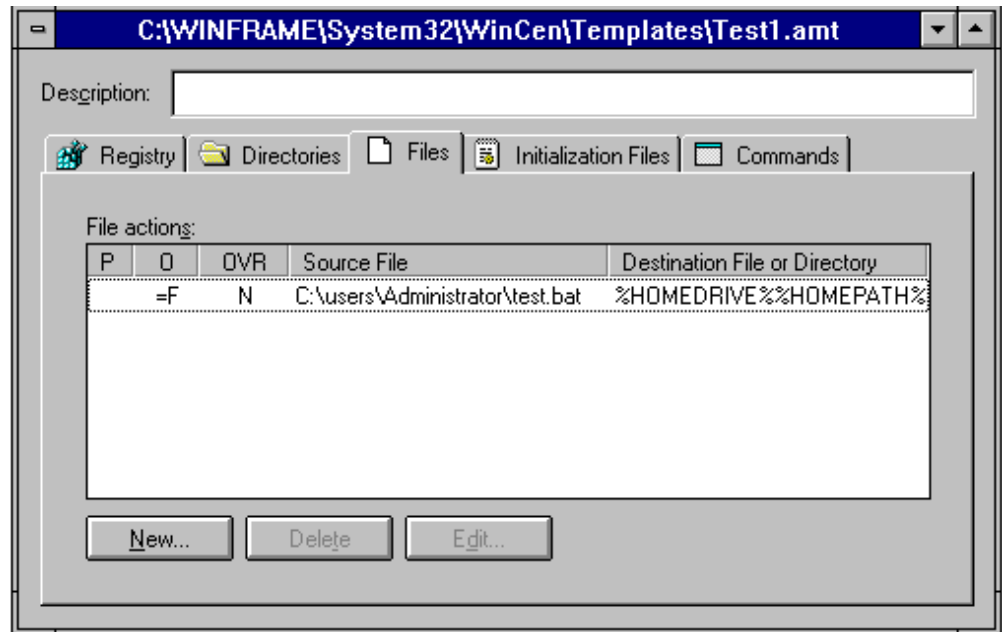


Figure 312. MAM Templates - File Actions

An example of the File actions is shown in the above figure (Figure 312), where the indicated action is to copy the C:\users\Administrator\test.bat file to a directory called Remedy in the user's home directory. (The last portion of the Destination is not visible in the display above but it is in the figure below.)

If that particular (and only line) is selected, a click on **Edit...** displays the panel in the next figure:

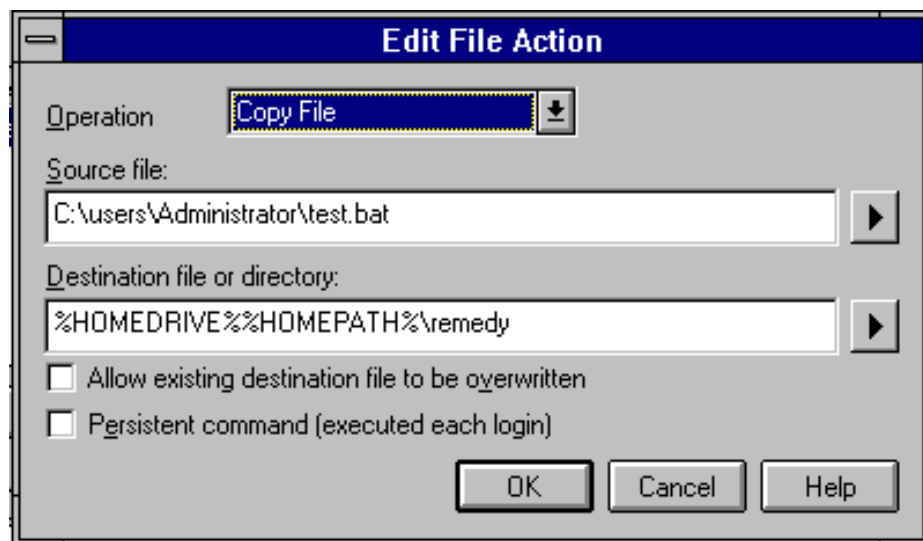


Figure 313. MAM Templates - Edit File Action

Notice in the above panel that you can indicate that this is a command to be executed in a persistent fashion (that is, each time that the user logs on) and also that you are allowing the existing file to be overwritten.

The next figure (Figure 314) displays the Registry action panel. This is an easy way to add, delete and modify Registry entries.

Notice that you can specify the Registry action to be taken, on which Registry hive, and the target path, as well as the value type, name and data.

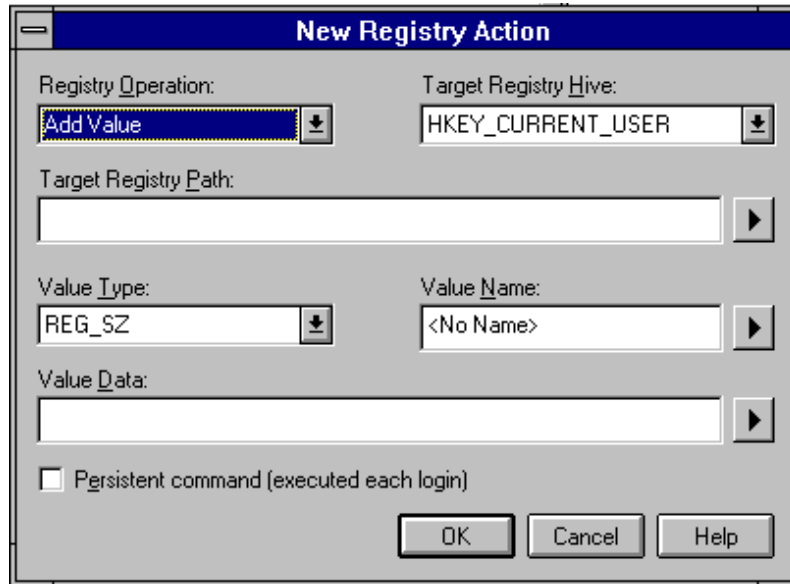
The dialog box is titled "New Registry Action". It contains several fields: "Registry Operation" with a dropdown menu showing "Add Value"; "Target Registry Hive" with a dropdown menu showing "HKEY\_CURRENT\_USER"; "Target Registry Path" with an empty text box and a right-pointing arrow button; "Value Type" with a dropdown menu showing "REG\_SZ"; "Value Name" with a text box containing "<No Name>" and a right-pointing arrow button; "Value Data" with an empty text box and a right-pointing arrow button; and a checkbox labeled "Persistent command (executed each login)". At the bottom are "OK", "Cancel", and "Help" buttons.

Figure 314. MAM Templates - Registry Actions

The next figure (Figure 315) displays the panel for specifying INI file actions.

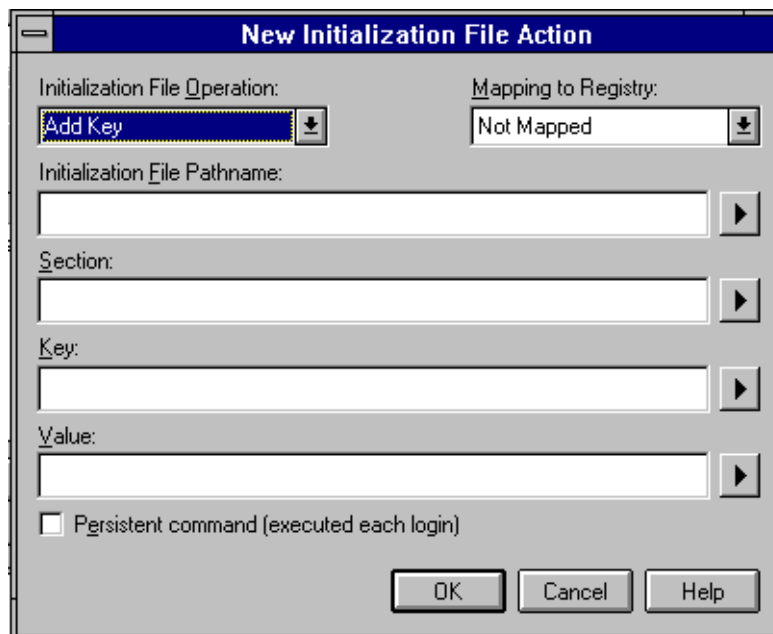
The dialog box is titled "New Initialization File Action". It contains several fields: "Initialization File Operation" with a dropdown menu showing "Add Key"; "Mapping to Registry" with a dropdown menu showing "Not Mapped"; "Initialization File Pathname" with an empty text box and a right-pointing arrow button; "Section" with an empty text box and a right-pointing arrow button; "Key" with an empty text box and a right-pointing arrow button; "Value" with an empty text box and a right-pointing arrow button; and a checkbox labeled "Persistent command (executed each login)". At the bottom are "OK", "Cancel", and "Help" buttons.

Figure 315. MAM Templates - INI Files Actions

And finally, if you need to simply execute a command, it can be specified as displayed in the figure below by entering the path to the command file.



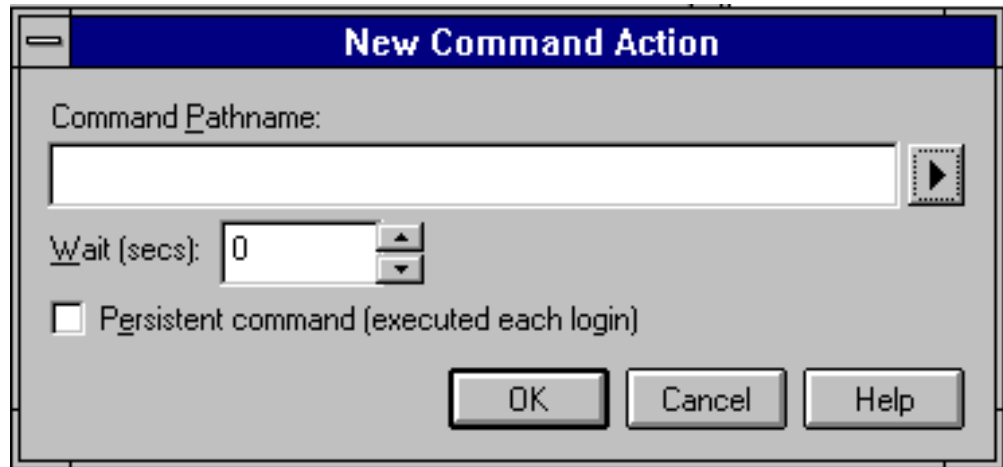


Figure 316. MAM Templates - Command Actions

All of these actions make up a template, which is given a name, and can be triggered for execution at the time that the user logs on.

As discussed previously, policies are defined to indicate which template or templates are to be executed for which user or group of users.

For example, if we wanted a template called test1 to be executed for user bechard, we use the File pull-down on the main MAM panel, select **New**, then **Policy**, which displays the panel shown in the figure below:

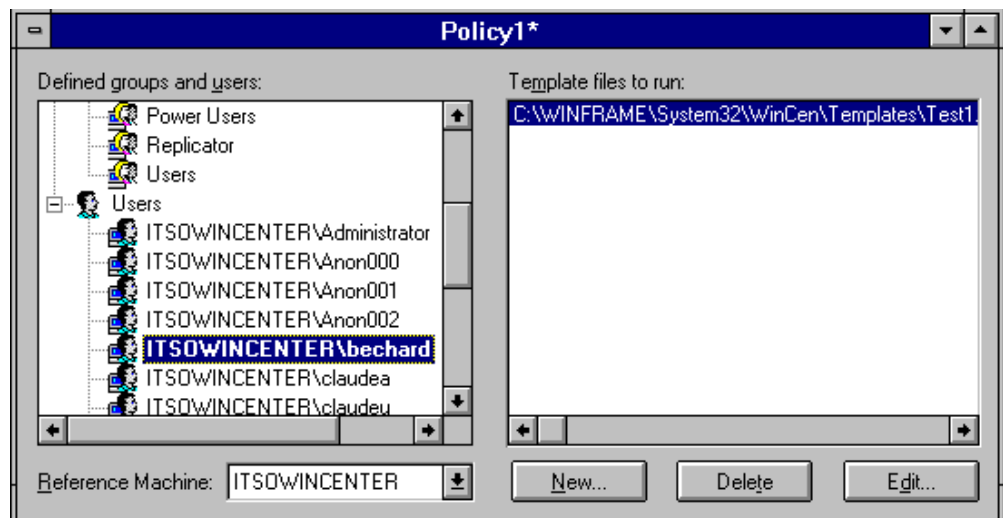


Figure 317. A Sample Policy

This policy, applicable to user bechard on the ITSOWINCENTER machine, calls for the execution of the test1 template.



---

## Chapter 19. Problem Determination - Tools, Tips and Techniques

In this chapter we take a look at some of the tools and techniques that can be useful to an administrator to do problem determination related to the IBM Network Station.

This is not meant as an all-encompassing list but as a guide to some common and typical tools used in a Windows NT environment.

Some tools and techniques that we examine are:

- The IBM Network Station Message Log
- How to access the log remotely and how to save messages to a file for further analysis
- How to use the NT's Event Viewer to look at three important NT message logs: the System log, the Security log and the Application log
- How to use the DHCP log files and the Web server log files
- How to use NT's Network Monitor to trace frames on the LAN
- How to launch commands on the IBM Network Station from a remote location
- How to start applications on the IBM Network Station with tracing or debugging options
- How to use the boot monitor commands
- How to upload dump files from the IBM Network Station to the boot server

---

### 19.1 The IBM Network Station Message Log

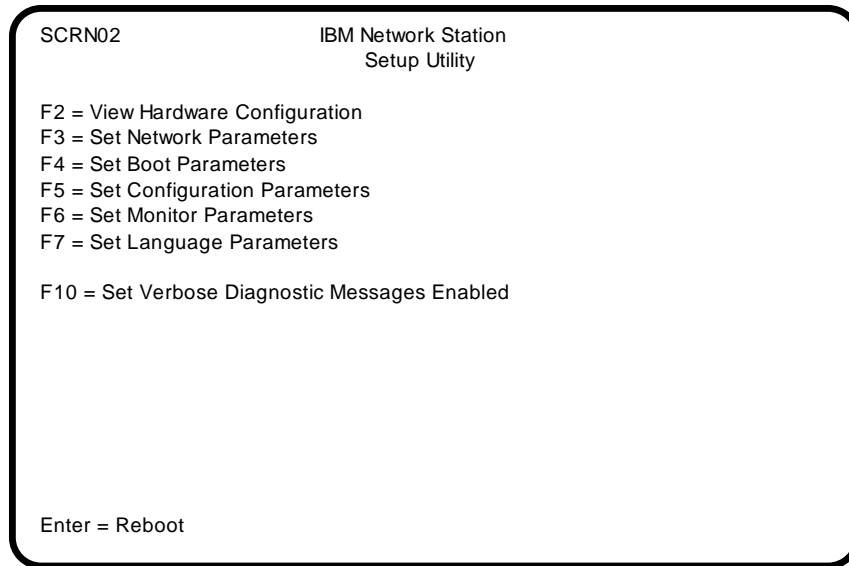
From the moment the IBM Network Station opens its network adapter to communicate with its boot server, it starts logging messages to its console. These messages can be viewed in a few different ways, such as:

- On the IBM Network Station screen during the boot process
- Using the message log on the IBM Network Station console
- Using TELNET to port 5998 from the IBM Network Station itself
- Using TELNET to port 5998 from a remote host

We examine each of these below.

#### 19.1.1 On-Screen Messages during the Boot Process

During the actual boot process, these messages are displayed on the IBM Network Station display if the verbose option has been enabled (F10) when configuring the IBM Network Station, on the main Setup Utility screen, as shown below.



*Figure 318. IBM Network Station Setup Utility - Diagnostic Verbose Option*

If the verbose option is disabled, which would be the default (the typical user does not really need to see these messages), these messages only appear as a series of dots across a line on the screen, providing a visual indication to the user that the boot process is taking place, but not providing any details.

Whether these messages are displayed or not, they still get saved in the IBM Network Station memory and are available for display from the Network Station console.

### **19.1.2 Messages on the IBM Network Station Console**

Shown below is the Network Station console. To display messages, the user clicks on the **Messages** check box situated right below the Console pull-down on the menu bar.

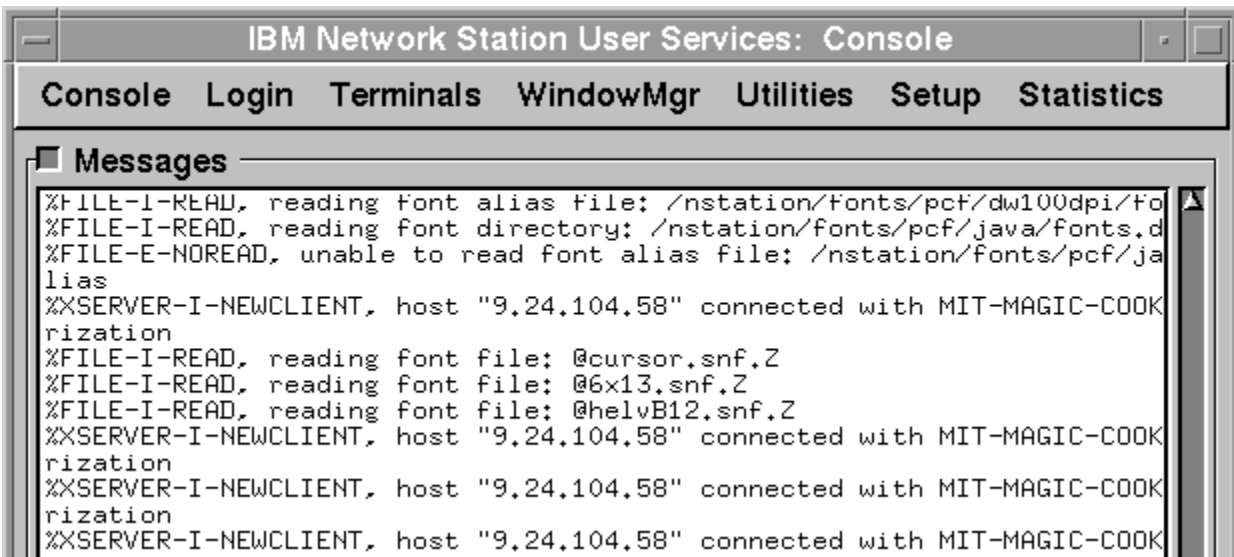


Figure 319. IBM Network Station Console Messages

The user here has only limited scrolling capability to examine messages. This message console facility is useful to the user mainly for looking at messages as they are issued. For example, if the user starts an application such as a 3270 emulator session by clicking on a menu bar item, he or she can see the result of this action, in terms of the actual commands that get executed on the IBM Network Station, by looking at the console messages being displayed as the commands are issued and executed.

### 19.1.3 Message Log via TELNET from the IBM Network Station

Another way to look at these messages is to use TELNET from the IBM Network Station itself. This is possible if the Terminals pull-down is enabled on the console.

If it is, the user can TELNET into itself (using the loopback interface address of 127.0.0.1) to port 5998 (for example, TELNET 127.0.0.1 5998). This results in a TELNET session displaying the message log. This can also be done by choosing the Diag port in the list that appears when using the Terminals pull-down and choosing **Terminals**, and then the **Diag** function. This is equivalent to issuing TELNET 127.0.0.1 5998 and is illustrated in the figure below.

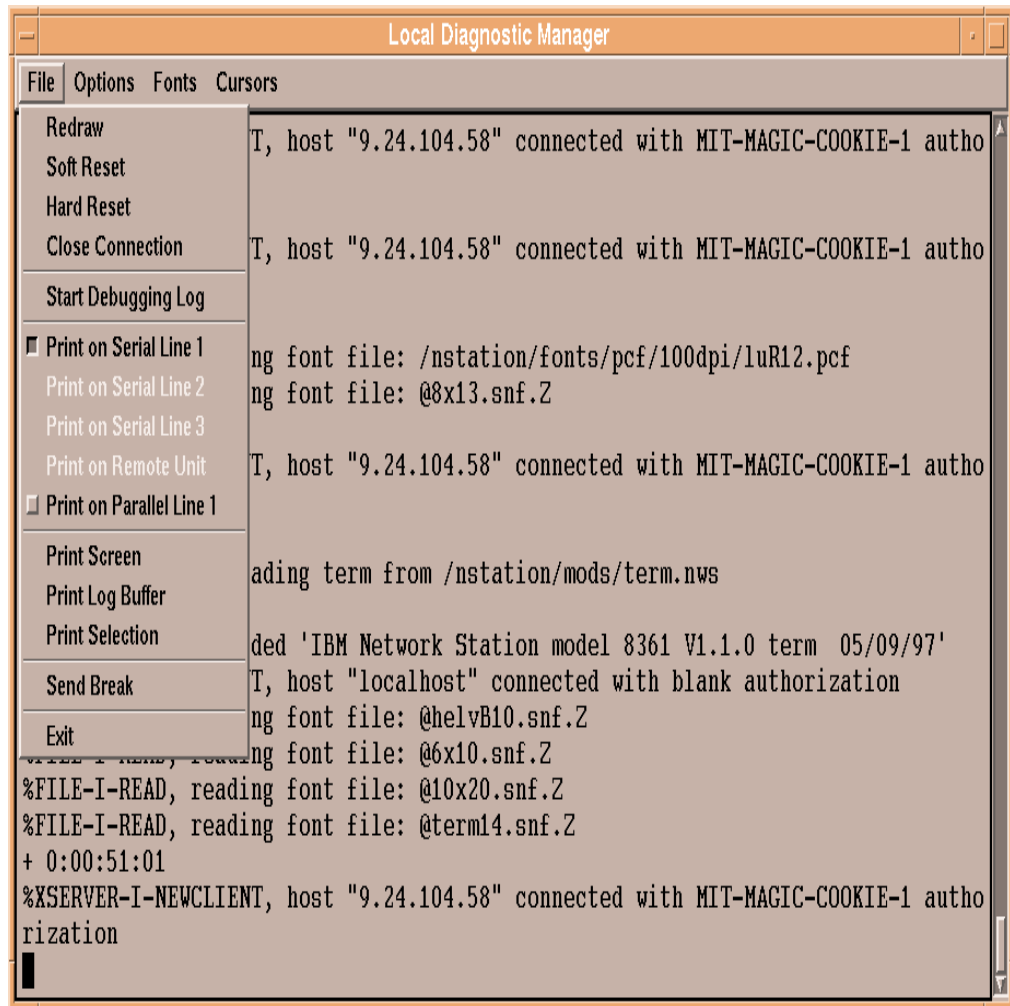


Figure 320. IBM Network Station Console Messages via Diag Port

The advantage of this method over the message list on the console is that the pull-down menus offer a few additional choices, such as changing the display fonts, printing if a printer is available, etc. It is also fast, with good scrolling capabilities. The figure below illustrates the items available on the Options pull-down.

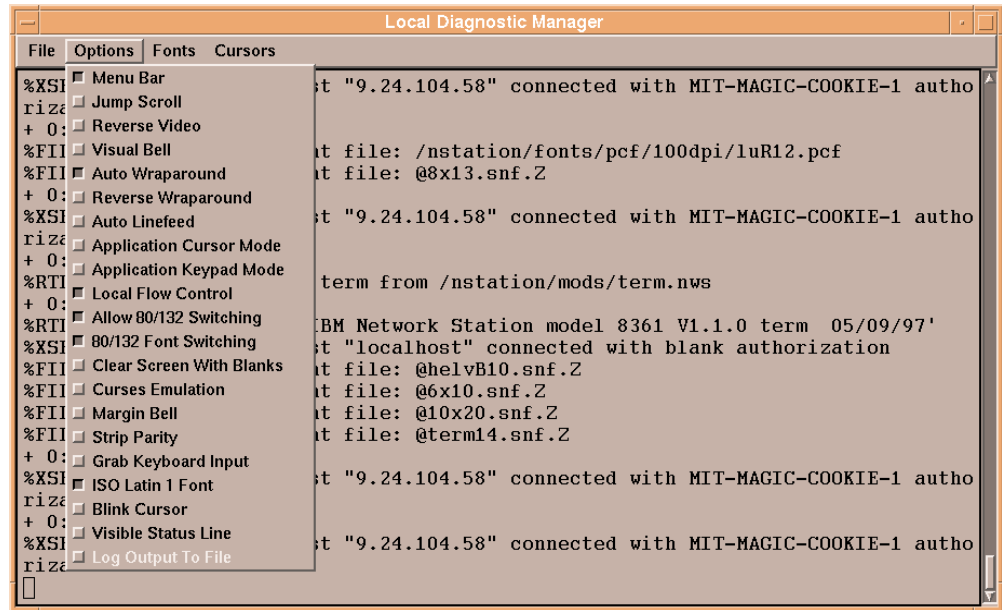


Figure 321. IBM Network Station Console - Options

#### 19.1.4 Message Log from a Remote Host Using TELNET

However, if one needs to examine the log more closely and look for specific entries when doing specific problem determination, then one must have the capability to save this log to a file and use an editor to search the log.

The way to save the log to a file is to TELNET into the IBM Network Station from the server or any other PC or host with a TELNET capability and to use the logging capability of the TELNET utility to save the file.

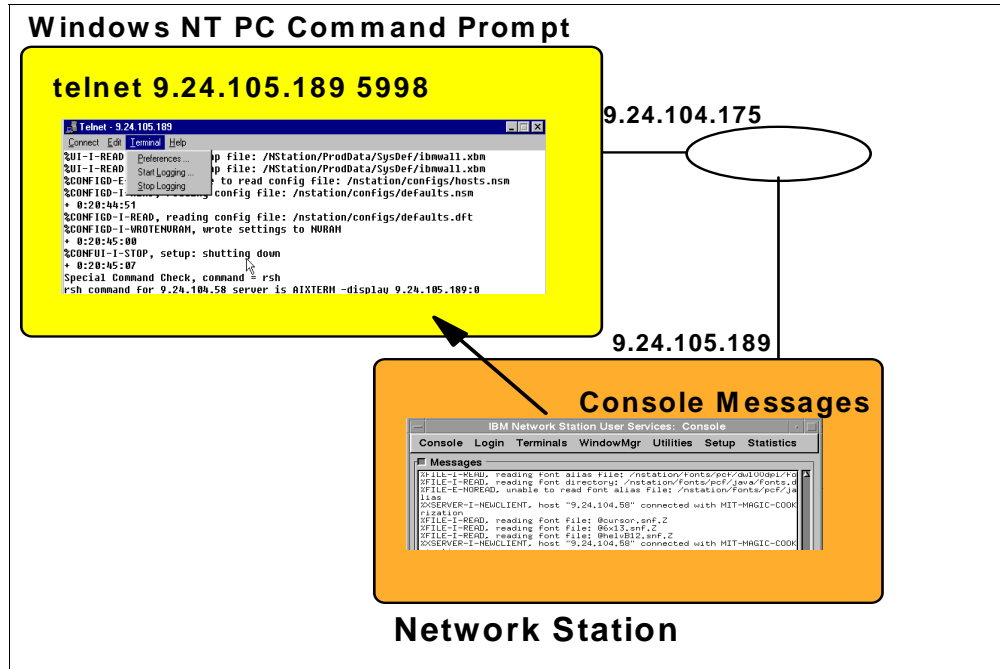


Figure 322. Accessing Messages Remotely

When you TELNET into the IBM Network Station, you get all the messages since they started to be logged, from the beginning, and you can therefore see/save them all in one file.

Assume that the IP address of our IBM Network Station is 9.24.105.189. The command is simply TELNET 9.24.105.189 5998. The result is illustrated below where we do a TELNET from a Windows NT workstation.

Use the **Start Logging** option on the Terminal pull-down on the telnet session menu bar, and select a name and directory to store the log file.

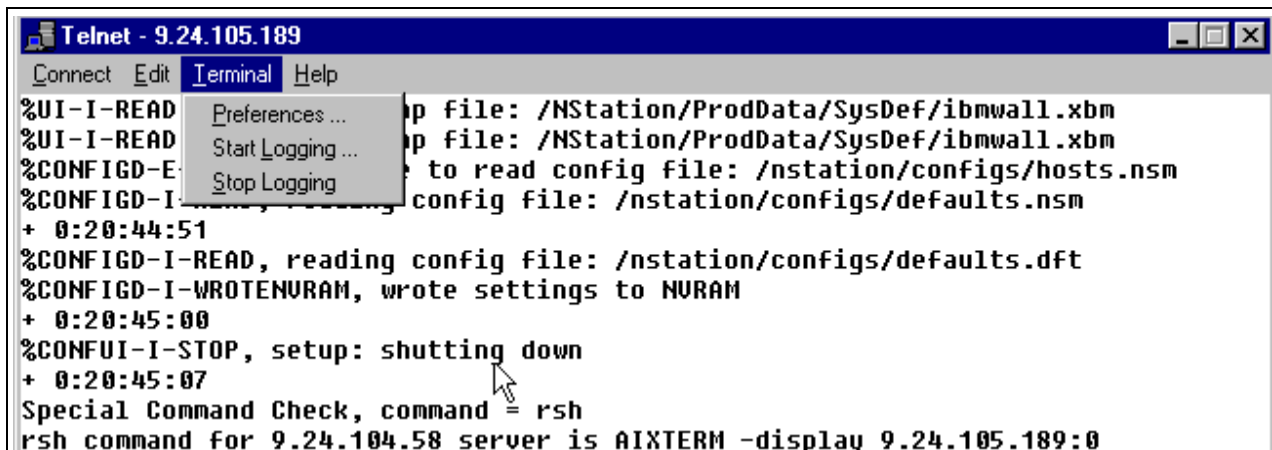


Figure 323. IBM Network Station Console Messages via Telnet 5998



### 19.1.5 Sample Message Log

Most messages in the Message log are fairly self-explanatory. Each message is usually preceded by some identifier such as %CONFIGD-I-READ for example. The %CONFIGD indicates that this message is issued from the configuration daemon on the IBM Network Station, the I indicates that this is an informational message, and the READ indicates the operation performed. This is usually followed by a more complete message such as,

```
reading config file:/nstation/configs/standard.nsm
```

Below is a sample log showing typical messages issued at boot time.

```
%TOKENRING-I-ADDRESS, address for this unit: 00:00:e5:68:bf:ad
IBM Network Station Model 8361-200 nws V1.1.0 #18238 05/13/97 downloaded:
LAN PP
P StdPkg XTRAP Audio
Copyright 1988-1997 Network Computing Devices, Inc.
BSD TCP/IP Copyright 1980, 1982-83, 1985-88 Regents of the University of
California
DECwindows is a trademark of Digital Equipment Corporation
X Window System is a trademark of X Consortium, Inc.

5733A07 (C) Copyright IBM Corp. 1997,
5733A06 (C) Copyright IBM Corp. 1997,
All rights reserved. US Government Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

JAVA(tm) Copyright (c) 1993-1996 Sun Microsystems, Inc. All Rights
Reserved.
+ 0:00:00:01
%CONFIGD-I-IPADDR, IP address for this unit: 9.24.104.189
%TOKENRING-I-WAITING, waiting for adapter initialization
+ 0:00:00:05
%TOKENRING-I-OPEN, adapter open, interface active
+ 0:00:00:06
%CONFIGD-E-MOUNTFAILED, failed to mount local filesystem
%CONFIGD-I-READ, reading config file: /nstation/configs/standard.nsm
%CONFIGD-I-READ, reading config file: /nstation/configs/required.nsm
+ 0:00:00:07
%CONFIGD-E-SYNTAX, line 54: syntax error at tcpip
%CONFIGD-I-READ, reading config file: /nstation/configs/control.nsm
%UI-I-READ, reading bitmap file: /NStation/ProdData/SysDef/ibmwall.xbm
%UI-I-READ, reading bitmap file: /NStation/ProdData/SysDef/ibmwall.xbm
%CONFIGD-E-NOREAD, unable to read config file: /nstation/configs/hosts.nsm
%CONFIGD-E-NOREAD, unable to read config file: /nstation/configs/hosts.nsm
%CONFIGD-I-READ, reading config file: /nstation/configs/defaults.nsm
%CONFIGD-I-READ, reading config file: /nstation/configs/defaults.dft
%CONFIGD-I-WROTEENV, wrote settings to NVRAM
+ 0:00:00:08
%FILE-I-READ, reading RGB file: /nstation/rgb.txt
%FILE-I-READ, reading file: /nstation/XKeysymDB
```

Figure 324. Sample Messages in the Message Log

---

## 19.2 The Network Station Console

The Network Station console can be a very useful tool when testing and doing problem determination if one is working at the Network Station itself.

Please refer to 5.2, "The IBM Network Station Console" on page 124 for an overview of the console facilities. In particular, note the availability of:

- The Test Network under the Utilities pull-down, which is a PING application allowing you to determine if you have IP connectivity to another host.
- The Setup pull-down, from which you have access to all the configuration parameters using an easy graphical interface. You can even work on a remote station's parameters from here by selecting **Connect to New Unit** from the File pull-down. See 19.6, "Accessing the Setup Panels from Another Network Station" on page 382 for more details.
- The Statistics pull-down provides a wealth of information on the version level of the software, addresses, memory usage, IP usage, etc.

For example, this is where you can verify which TCP connections are currently active, between which addresses and which ports. For this, use the TCP section under Statistics and look for the Connection table, which lists the local IP address, local port, remote IP address, remote port, and state.

- The Terminals pull-down allows the start of a TELNET session with other hosts or with your own station for the diagnostics, file or config services.

---

## 19.3 NT's Event Viewer

The next place where one should look for information while doing problem determination is the event logs on the server maintained by the Windows NT operating system.

With Release 3, there are more components now that write messages to these logs, such as NSM, NSLD (network station login daemon), DHCPSPD, NAMED, Lotus GO, eNODInstall, etc. so it is a good idea to check this source.

There are three types of event logs, which can all be examined by using NT's Event Viewer. They can sometimes provide valuable information leading to the source of a problem.

- The System log
- The Security log
- The Application log

The Event Viewer is accessed by clicking **Start=>Programs=>Administrative Tools=>Event Viewer**. Below is an illustration of a typical Event Viewer display:

Date	Time	Source	Category	Event	User	Comput
8/28/98	4:06:00 PM	LotusDominoGoWe	None	100	N/A	BECH
8/28/98	3:51:12 PM	NFSD	None	17773	N/A	BECH
8/28/98	3:51:12 PM	NFSD	None	17773	N/A	BECH
8/28/98	3:37:59 PM	LicenseService	None	202	N/A	BECH
8/28/98	8:44:36 AM	DHCPD	None	0	N/A	BECH
8/28/98	8:44:34 AM	LotusDominoGoWe	None	100	N/A	BECH
8/28/98	8:44:34 AM	NAMED	None	115	N/A	BECH
8/28/98	8:44:26 AM	LPR Print Monitor	None	2007	N/A	BECH
8/27/98	3:59:01 PM	LicenseService	None	202	N/A	BECH
8/27/98	2:20:11 PM	NAMED	None	115	N/A	BECH
8/27/98	2:20:05 PM	NAMED	None	179	N/A	BECH
8/27/98	1:57:22 PM	NAMED	None	115	N/A	BECH
8/27/98	1:57:17 PM	NAMED	None	179	N/A	BECH
8/27/98	1:53:26 PM	NAMED	None	115	N/A	BECH
8/27/98	1:53:20 PM	NAMED	None	179	N/A	BECH
8/27/98	1:51:17 PM	NAMED	None	115	N/A	BECH
8/27/98	1:51:11 PM	NAMED	None	179	N/A	BECH

Figure 325. NT Event Viewer

A double-click on a specific event brings up additional details on the event.

**Event Detail**

Date: 8/28/98      Event ID: 100  
Time: 4:06:00 PM      Source: LotusDominoGoWebserver  
User: N/A      Type: Information  
Computer: BECHARD      Category: None

Description:  
The Lotus Domino Go Webserver is running.

Data: ☒ Bytes ☐ Words

Close Previous Next Help

Figure 326. NT Event Viewer - Details of an Event

The Security log displays the successes or failures of a user attempting a logon, or of a file being accessed for read or read/write if specific permissions were applied to that file.

Finally, the system log shows system-related events such as the inability to open a network adapter.

The options available on the Event Viewer pull-down menus allow the user to:

- Save a specific log to a file.

This can be very useful when there is a need to forward this information to a Service Specialist. Choose the **Save As...** item on the Log pull-down.

- Find specific information in the log, looking for specific data.
- Filter the messages. The size of a log can be reduced for easier analysis by asking to display only messages that are of a specific type, source or origin application, as well as time and date. This filter is accessed through the View pull-down by selecting **Filter Events...**, and is illustrated below:

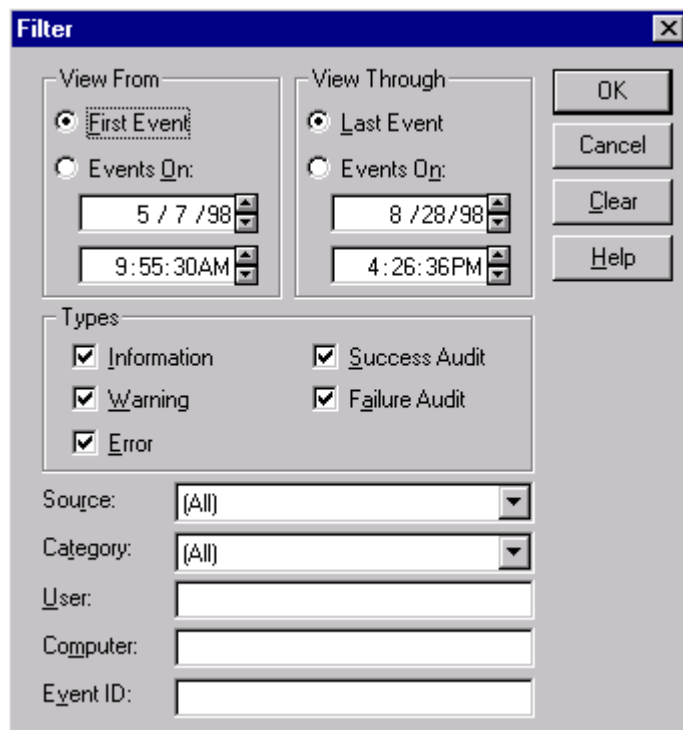


Figure 327. NT Event Viewer - Specifying a Display Filter

---

## 19.4 Controlling Access to the IBM Network Station

There are access control parameters that allow you to specify how the IBM Network Station handles local and remote access requests.

In most cases, you can specify whether you want to enforce access control, by turning it on or off.

- If access control is turned off (for example, set `exec-access-control-enabled = false`, meaning that you are *not* enabling access control), then any IP host is allowed access.
- If turned on (for example, set `exec-access-control-enabled = true`), you then need to configure an access control table that lists the names or addresses of the hosts that are allowed access.

For example:

```
set exec-access-control-list = {
  {"myserver.itso.ral.ibm.com" tcpip}
  {"9.24.104.175" tcpip} }
```

Access control can be enabled for the following areas or services:

- X server
- Config daemon
- User preference daemon
- Diagnostic daemon
- NFS
- File manager
- Local command execution daemon
- Serial and parallel daemon

### 19.4.1 X Server Access

The Network Station is an X server station; this means that an X client located on a remote machine can connect into the X server on the IBM Network Station to display the output of an application running on this remote machine.

For example, a simple application that can be used as an example is the `xclock` application running on an RS/6000 AIX machine. From the IBM Network Station, one can connect into the RS/6000 machine and ask to start the `xclock` application, and specify that the output of the application (which is a clock icon displaying the current time) be displayed not on the RS/6000 but on the Network Station's display.

This requires the `xclock` application on the RS/6000 to use another application called an X client, whose purpose it is to connect to a counterpart application called an X server, running on the Network Station, and transmit the output of the `xclock` application so that it is displayed on the Network Station's display.

There are two ways in which you can enable X clients to use your Network Station's X server:

1. Allow all or any X clients to access the X server
2. Allow only specific pre-determined X clients to access the X server

The first option is the easiest because you do not need to individually specify each client to which you want to grant access to the X server.

To grant X-server access in IBM Network Station Manager, select **Hardware=>Workstation**, then either System, Workstation, Group or User Defaults and then **Local Services**, and click **Yes**, as illustrated below:



Figure 328. X Server Access Control

You can also specify the following in the defaults.dft configuration file:

```
set xserver-access-control-enabled = false
```

To grant access to specific X clients, you can add the following to the defaults.dft file, where hostname is the IP hostname or address of the x client and family is tcpip:

```
set xserver-access-control-enabled = true
set xserver-access-control-list = {{ hostname family }}
```

Actually, in IBM Network Station Manager, whenever you add a remote program entry (either through startup programs or menus), NSM automatically adds a command to the startup list which dynamically adds the remote host to the access control list.

This is done through the xhost command and is sort of the equivalent of specifying a specific access control list for X clients.

#### 19.4.2 Console Access

If you wish to set a password in order to control user access to the console, you can configure this using the following parameter:

```
set config-console-enforce-password-locally = true
```

When this parameter is set to true, the user is prompted for a password when requesting the console utility.

You can set the password using the following parameter:

```
set config-console-display-password = my_password
```

You may choose to enable this parameter to prevent the general user from having access to the IBM Network Station console as a whole. But, you might also control user access to the console facilities by enabling and disabling certain pull-downs and commands on the console.

#### 19.4.3 Configuration and User Preference Information Access

It is also possible to prompt users for a password when they try to access configuration or user preference information locally. Use the following parameter to enable this function:

```
set config-enforce-passwords-locally = true
```

To set the configuration passwords, use the following, dependent on whether you want to set the read-only or the read-write passwords, or both:

```
set config-read-only-password = my_password
set config-read-write-password = my_password
```

To do the same for user preferences, use the following:

```
set config-pref-enforce-passwords-locally = true
```

To set the configuration preferences passwords, use the following, dependent on whether you want to set the read-only or the read-write passwords, or both:

```
set config-pref-read-only-password = my_password
set config-pref-read-write-password = my_password
```

#### 19.4.4 Diagnostic Access

A helpful problem determination source of information is the IBM Network Station's message log. If you need to restrict access to the message log, use the following:

```
set diag-access-control-enabled = true
```

#### 19.4.5 File Manager Password

To set the password to obtain access to the file manager, use the following:

```
set file-manager-password = my_password
```

#### 19.4.6 Screen Lock Password

You can set the screen lock password every time you lock the screen. You can also pre-specify the password to use with the following statement:

```
set pref-console-lock-screen-default-password = my_password
```

However, when you do so, the user is asked to confirm that password before the screen will lock. If the user does not know the password, he or she can override it with his or her own password by entering it twice. Therefore, we see little use for this particular statement.

#### 19.4.7 Unit Global Password

The password required to obtain read-write access to the configuration, preferences, SNMP, and file daemons is called the unit global password.

This is also called the Administrator password. In fact, this is the what it is called in IBM Network Station Manager, where it can be set selecting **Hardware=>Workstation=>System Defaults=>Miscellaneous**, as illustrated in the next figure.

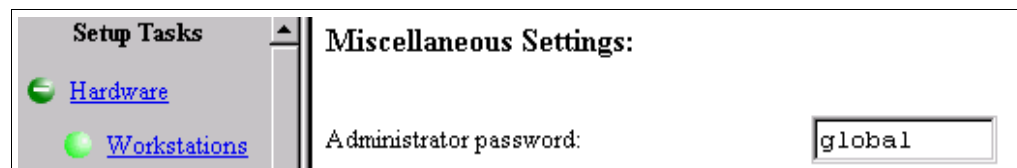


Figure 329. Setting the Administrator Password

The result of entering the above password causes IBM Network Station Manager to add to its defaults.nsm configuration file the following statement:

```
set unit-global-password="<ENCODED>%E9%52%BA%6A%49%C7"
```

Notice that the password has been encoded and this is therefore a more secure method. However, you can also be set the password by using the following statement in your defaults.dft file, in an unencoded form:

```
set unit-global-password = my_password
```

The method above sets an administrator password for all stations since this is done at the system level, and this is certainly the easiest way to proceed. In fact, if you want to use the remote reboot capability and be able to specify a range of stations to be rebooted, all the passwords must be the same, which is another reason for an administrator to use the same global password for all stations.

See 19.14, "Rebooting IBM Network Stations Remotely" on page 392 for instructions on how to use the remote reboot capability.

If there is a need to set a different password for a particular station, it can be done by including the set unit-global-password in the "name".trm file for the specific workstation.

#### 19.4.8 Remote Command Execution Access

You can cause the execution of commands on an IBM Network Station, from a remote host, by issuing the RSH (remote shell) command.

You most likely need to restrict this access by allowing only specific hosts, such as an administrator's host, to issue commands remotely when doing problem determination.

For example, as an administrator, you may wish to start a 3270 emulator with the debug option on a remote Network Station for debug purposes.

The parameter that controls access to the local command execution daemon is the following:

```
set exec-access-control-enabled = true
```

Set this value to true if you want to prohibit undefined hosts from executing applications on the network station, and specify the associated access control list to define which hosts do have access.

```
set exec-access-control-list = {  
  {"127.0.0.1" tcpip}  
  {"wincenter.itso.ral.ibm.com" tcpip}  
}
```

This specifies that you can issue commands to yourself (the 127.0.0.1 loopback interface) and that the host called wincenter.itso.ral.ibm.com also has the ability to run commands on this station.

---

### 19.5 Launching Commands from a Remote Host

Even though there is a local command execution daemon running on the Network Station, which can accept commands from pre-programmed buttons on the menu bar for example, there is actually no real command line facility that a user can use to issue commands for local execution. However, commands can be issued from



a remote machine through an rsh (remote shell) facility, effectively providing a remote command line facility that can be used for testing and problem determination.

For example, say that the user has an item on his or her menu bar that starts a 3270 emulator session with a specific host. The command executed by the Network Station, as a result of the user clicking on the menu item, would be something similar to NS3270 10.14.12.1 -graphics; this command starts a 3270 session with the 10.14.12.1 host as a session using graphics.

If there is a problem with that session and the administrator needs to start this session with an additional option called -debug, he or she has the choice of changing the menu item description by editing the configuration files or using the Network Station Manager, reloading the Network Station configuration files, and starting the 3270 session again with a click on the modified menu bar button, or he or she can simply issue an RSH command to start the command execution remotely and include the additional parameters interactively.

In this case, from a remote machine, he or she would issue:

```
RSH IP-address-of-netstation ns3270 10.14.12.1 -graphics -debug
```

This command starts the 3270 session on the Network Station and the -debug option causes additional messages to be logged to the message log.

### 19.5.1 Commands

Not all commands can be issued remotely using rsh, but here is a list of commands we have been able to use:

#### Output of Commands

Be aware that the remote execution of these commands, when involving the display of information, displays the information on the network station display and not on the remote display from where the rsh command was issued.

However, this might still be very useful to an administrator who is doing problem determination while talking to the end user on the phone. The end user might be able to relay the information to the specialist attempting to identify the cause of the problem.

If the administrator had disabled certain functions, he or she might still be able to execute them remotely and ask the user to read some information such as version number, etc.

- SHOW version - Shows the model of the Network Station, the software and boot monitor level, MAC addresses, etc.
- SHOW Memory - Shows memory usage.
- SHOW Connections - Displays X connections and resource usage.
- STATS - Displays a panel allowing to get statistics on Ethernet, font usage, IP, etc.
- TEST net - Starts the PING application.

- TERM - Opens the terminal host chooser.
- TERM -ctype telnet - Opens a TELNET session.
- TERM -ctype telnet rs600026 - Opens a TELNET session with host RS600026.
- TELNET rs600026 - Same as above.
- LOGIN - Starts the Login Chooser.
- LOGIN wincenter.itso.ral.ibm.com - Starts the Login Chooser with the specified host as the target host.
- QUICKSETUP - Starts the Quick Setup utility.
- SETUP - Starts the Setup utility.
- PREF - Starts the User Preferences utility.
- NS3270 host -options - Starts a 3270 session with host and options.
- NS5250 host -options - Starts a 5250 session with host and options.
- CONSOLE - Starts the console.
- WM - Starts the Window Manager.

**Note**

The above commands can be executed remotely as long as they have not been disabled and as long as remote command execution is allowed by setting the exec-access-control-enabled parameter.

If only the pull-down menu on the console has been disabled, but not the command execution, then the command can still be executed.

Notice that in the configuration statements below, the Setup pull-down menu on the console has been disabled (using the `ncdconsole.disableSetupMenu: true` statement). These configuration statements are in the `required.nsm` file. This prevents a user at the Network Station from using the three items that are on this pull-down, that is, Quick Setup, Setup and User Preferences.

However, out of these three commands, only the `quicksetup` command itself has been disabled (using the `{ quicksetup }` entry on the `set exec-disabled-commands =` statement where there is no `#` sign besides the entry to make it inoperative).

The result is that an administrator can start the `setup` and `pref` commands remotely using RSH but cannot start the `quicksetup` command.

```
set xserver-initial-x-resources = "nccconsole.disableReboot: false\n\
nccconsole.disableLoginMenu: false\n\
nccconsole.disableTerminalMenu: false\n\
nccconsole.disableSetupMenu: true"

set exec-disabled-commands = {
# { login }
# { logout }
# { serial }
# { dialer }
# { quicksetup }
# { setup }
# { pref }
```

### 19.5.2 Help on Commands

Some help information is available for some of these commands. We have used the following, from a remote host, to get information on the navio command, which loads the Navio browser:

```
rsh netstation_address loadb nsb -help
```

This produced the information below:

```
usage: navio [ options ... ]
      where options include:

      -help                to show this message.
      -version             to show the version number and build date.
      -display <dpy>       to specify the X server to use.
      -geometry =WxH+X+Y   to position and size the window.
      -visual <id-or-number> to use a specific server visual.
      -install             to install a private colormap.
      -no-install          to use the default colormap.
      -ncols <N>           when not using -install, set the maximum
                           number of colors to allocate for images.
      -mono                to force 1-bit-deep image display.
      -iconic              to start up iconified.
      -xrm <resource-spec> to set a specific X resource.

      -remote <remote-command> to execute a command in an already-running
                           Navio process. For more info, see
                           http://home.netscape.com/newsref/std/x-remote.html
      -id <window-id>        the id of an X window to which the -remote
                           commands should be sent; if unspecified,
                           the first window found will be used.
      -raise               whether following -remote commands should
                           cause the window to raise itself to the top
                           (this is the default.)
      -noraise             the opposite of -raise: following -remote
                           commands will not auto-raise the window.

      Arguments which are not switches are interpreted as either files or
      URLs to be loaded.

      Most customizations can be performed through the Options menu.
```

Figure 330. Help on the Navio Command

Here are a few other examples, such as the ns3270 command, the ns5250 command, the telnet or term command, and a few other miscellaneous commands.

```
Usage: ns3270 [3270_options] [X-Windows_options] hostname

3270_options:
-----
[-cols columns] [-debug] [-graphics] [-ims] [-LANGID language_id]
[-MRIPATH MRInnn] [-nographics] [-pfkeys] [-port port]
[-rows rows] [-title title] [-trace] [-version]

X-Windows_options:
-----
[-help]
```

Figure 331. Help on the ns3270 Command

```
Usage: ns5250 [-help] [-display hostname:number.screen]
[-trace] [-debug]
[-W] [-iconic] [-port port]
[-fn normal font list] [-fb bold_font]
[-ms mouse_color] [-cr cursor_color]
[-cursor cursor_name]
[-printcmd command] [-keyfile filename]
hostname
```

Figure 332. Help on the ns5250 Command

```
telnet or TERM usage:
  NCDterm VT320 terminal emulator

  The available options are:

      -/+132          enable/disable 132 column mode
      -b             <margin>    inner margin
      -bd            <color>     border color
      -bg            <color>     background color
      -bw            <border>     border width
      -cr            <color>     cursor color
      -ctype         <comntype>  connection type to start, valid ones:
                                telnet lat cterm serial
      -/+cu           enable/disable curses emulation
      -fg            <color>     foreground color
      -fn            <fontname>   specifies the font name for normal text
      -geometry       <geometry> where to place NCDterm and size
      -help           this help text
      -host           <hostname> specify the host to start on
      -iconic         start in iconic form
      -/+j            enable/disable jump scrolling
      -/+mb           enable/disable margin bell
      -ms            <color>     pointer color
      -n             <icon_name> icon name
      -name           <classname> classname for the window
      -nb            <number>    margin bell in characters from right end
      -rv            reverse video
      -/+rw           enable/disable reverse-wraparound
      -/+sb           enable/disable scrollbar
      -title         <titlebar> title for the window (single token)
      -/+vb           enable/disable visual bell
      -xrm           <resource_string>
                                resource to be used in this instance of ncdterm
                                (may be specified more than once)
```

Figure 333. Help on telnet or term

```
usage: show version | memory | connections

usage: login [-indirect] [hostname[:]]

usage: test net

usage: net [-display dpy] [-tcpip] [-ncdnet] [host]
```

Figure 334. Help on Miscellaneous Other Commands

---

## 19.6 Accessing the Setup Panels from Another Network Station

The best and easiest way to access the configuration data of another (remote) IBM Network Station is to use the console functions on one IBM Network Station to access data on another IBM Network Station. To do this, use the Setup pull-down on the console. On any of the three commands under that pull-down (Quick Setup, Setup or User Preferences), the File pull-down has an entry called Connect to New Unit. A click on that entry brings up the following panel:

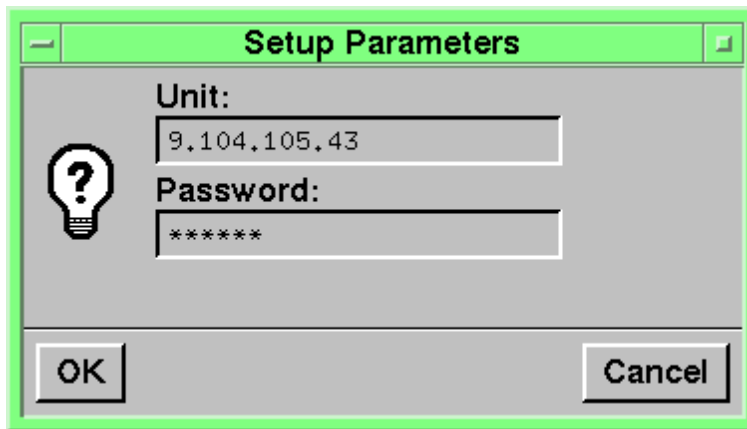


Figure 335. Connecting to a Remote Station

Enter the remote station IP address or hostname, and a password. This password can be either the read-only password (which, by default, is normally PUBLIC) or the read-write password.

Once connected with the proper authorization, the user has basically the same capabilities as on his or her own station.

**Note:** Interestingly, you can cause the remote Network Station to reread its configuration files from its server by clicking on the **Defaults** button, or by using **Restore Defaults** on the File pull-down.

---

## 19.7 Using the Config Daemon from a Remote Location

If you do not have an IBM Network Station that you can use to access another remote station, but you still require access to the configuration data of a remote IBM Network Station, you can use a telnet facility from any PC.

This facility is not as easy as using Connect into New Unit because it is a command line type of facility, but in a situation where it is the only facility available to you, you can at least view and change some configuration data.

It is however a fast way of viewing any of the Network Station parameters settings and you do not need any special access since the read only password is the word public, by default.

Remember, as always, that the preferred method of making any configuration changes is to use the IBM Network Station Manager, but in cases where you need to test temporary configuration changes, this is an acceptable method.

Provided that the required access control is in effect, the administrator can remotely alter the contents of the configuration parameters in NVRAM through the remote configuration daemon. This is possible if a global unit password has been set, or a specific config daemon read-write password.

#### Note

Note that changes applied to the NVRAM settings to alter configuration parameters are only valid until the next reboot, when the Network Station reads its configuration data from the boot server. So, if the changes are to be permanent, they must be made in the configuration files on the server.

The configuration daemon can be accessed as read-only, with a password of public (lowercase), or as read-write if using the read-write password.

The way to access the configuration daemon is to TELNET into the Network Station with port 5999, for example TELNET 9.24.105.189 5999. When prompted for a password, if the password is *public* (the default password for read-only), then the user can execute the following functions. These are obtained by typing ? on the command line.

```
*** NCD X Terminal Configuration ***
Password: public
> ?
get < param>
  - get parameter value (alias 'show')
get [< group> | groups | all] [read-only | read-write]
  - get parameter values (alias 'show')
get [changes | admin-changes | user-changes]
  - get changes to parameter values (alias 'show')
info [< param> | < group> | all]
  - provide detailed type information about the specified parameter(s)
quit - disconnect session
help - this command
```

Figure 336. Config Daemon Commands for Read-Only

For example, to get a list of all the groups of parameters (there are about 40 groups), issue the command get groups.

After the groups are listed, choose the one you are interested in. For example, to see the contents of the IP routing table, you need to see the parameters in the IP group, so you would issue the command GET IP, which lists all the parameters that are part of the IP group, one of which is the routing table.

If the password entered is the password for read-write, the command is much more extensive as it allows you to not only read the parameters but also to set them and write them to NVRAM, as shown below:

```
*** NCD X Terminal Configuration ***
Password:
> ?
  get < param>
    - get parameter value (alias 'show')
  get [< group> | groups | all] [read-only | read-write]
    - get parameter values (alias 'show')
  get [changes | admin-changes | user-changes]
    - get changes to parameter values (alias 'show')
  [set] < param> = < value>
    - set parameter value
  read nvram
    - read data from nvram (alias 'include' and 'load')
  read < file>
    - read commands from a file (alias 'include' and 'load')
  verify < file>
    - verify a configuration file by echoing executed commands
  write nvram
    - write data to nvram (alias 'dump' and 'save')
  write < file> < param>
    - write value to file (alias 'dump' and 'save')
  write < file> [< group> | changes | all] [read-only | read-write]
    - write values to file (alias 'dump' and 'save')
  zero < parameter or group>
    - zero a specific parameter or all parameters within a group
  pending - display pending sets
  apply - apply pending sets
  cancel - cancel pending sets
  lock - gain exclusive control of configuration
  unlock - release exclusive control of configuration
  protect [< param> | < group> | all]
    - protect against get or set operations of the specified parameter(s)
  get-protect [< param> | < group> | all]
    - protect against get operations of the specified parameter(s)
  set-protect [< param> | < group> | all]
    - protect against set operations of the specified parameter(s)
  info [< param> | < group> | all]
    - provide detailed type information about the specified parameter(s)
  quit - disconnect session
  help - this command
```

Figure 337. Config Daemon Commands for Read-Write



The user must know the name of the configuration parameters in order to use these commands.

You can see the settings for each available parameter by issuing the get all command. The result is a complete listing of all the parameters and their current values, which produces a listing of about 850 lines. The figure below shows a few lines of such a listing. Note that the values of some parameters, such as passwords, are protected from being displayed; only the value GET-PROTECTED is displayed.

```
config-add-domain-to-unit-name-as-filename = false
config-auto-save-file = false
config-auto-save-file-name =
"/netstation/prodbase/configs/9.24.104.189.stp"
config-auto-save-nvram = true
config-auto-saved-info = user-changes
# config-console-display-password = <GET-PROTECTED>
config-console-enforce-password-locally = true
config-custom-file = nil
config-default-file = "/netstation/prodbase/configs/9.24.104.189"
config-enforce-passwords-locally = false
config-generic-file = true
config-load-initial-file = true
config-persistent-loading = false
config-pref-enforce-passwords-locally = false
# config-pref-read-only-password = nil
# config-pref-read-write-password = nil
config-pref-tcp-port = 5977
config-pref-telnet-port = 5997
# config-read-only-password = <GET-PROTECTED>
# config-read-write-password = <GET-PROTECTED>
config-tcp-port = 5979
config-telnet-port = 5999
config-unit-ethernet-address-file = true
config-unit-ip-address-file = true
config-unit-name-file = true
config-unix-directory = "/netstation/prodbase/configs/"
config-use-decimal-ip-address-notation-as-filename = true
config-vms-directory = "NCD_ROOT:[CONFIGS]"

diag-abort-on-exception = true
diag-access-control-enabled = false
diag-access-control-list = {
}
diag-add-timestamps = true
```

Figure 338. Sample Partial get all Parameters List

A typical use of these commands would be for the administrator to use the set command to set the values of some of these parameters, then use the pending command to show all changes made, then use the apply command to commit these changes and the write nvram to write out the values into the Network Station's NVRAM.

The administrator would then try the commands or applications he or she is trying to do problem determination on, and maybe set other parameters, and so on.

---

## 19.8 Using the Boot Monitor Commands

There are 20 or so commands recognized by the boot monitor program that the administrator might need to use in some cases.

Below is a summary list of these commands; the description, in most cases, is pretty self-explanatory. This can be obtained by typing a ? at the boot monitor prompt.

```
BL [file] boot locally
BN [file] [local-IP host-IP] [gateway-IP] [subnet mask] boot via nfs
BR [retries] booting retries
BT [file] [local-IP host-IP] [gateway-IP] [subnet mask] boot via tftp
DA display addresses
DM [addr] [len] display memory
DR display registers
DS display booting statistics
EX extended tests
KM keyboard mapper
MA [mac address] locally administered MAC address
KS keyboard/mouse statistics
NF [rsize] set block size from 128 to 8192 bytes
NV nvram utility
PI [timeout] [local-IP host-IP] [gateway-IP] [subnet mask] ping host
RS reset system
SI [0/1] set serial i/o mode
SB [enable/disable] subnet broadcast TFTP
SE nvram setup
SM show memory configuration
ST stack trace
TI [num] set warning timeout in 10 seconds intervals
TM [mtu] set TRN MTU
TR [4 or 16] set TRN speed
UN [file][local-IP host-IP][gateway-IP][subnet mask] upload via nfs
UP [file][local-IP host-IP][gateway-IP][subnet mask] upload via tftp
ZK zero keyboard/mouse statistics
ZS zero boot statistics
```

*Figure 339. Boot Monitor Commands*

---

## 19.9 Getting Additional File Diagnostics

If you are in a situation where you have a particularly difficult problem with the file system, reading files for example, there is an extended diagnostic switch that can be set to trigger the logging of additional messages to the message log.

This is done by setting the parameter file-extended-diagnostics to true. The default is false and this value is set in NVRAM.

If you have access to the Setup pull-down menu on the console, you can also set it by clicking on **Setup=>Change Setup Parameters=>File Service**, click on the **Extended Diagnostics** button and click on **Apply**. The effect is immediate.

Here is a short example of the additional messages that get logged when this option is turned on.

```
%NETFILE-I-OPENATTEMPT, attempting open for /nstation/mods/Login/MRI2924/Login
%NETFILE-I-MATCHATTEMPT, attempting TFTP access of /nstation/mods/Login/MRI2924/
Login on 9.24.104.240 for /nstation/mods/Login/MRI2924/Login
%NETFILE-I-OPENSUCCESS, open succeeded for /nstation/mods/Login/MRI2924/Login
%FILE-I-READ, reading file: /nstation/mods/Login/MRI2924/Login
%NETFILE-I-OPENATTEMPT, attempting open for /nstation/fonts/pcf/misc/7x14B.pcf
%NETFILE-I-MATCHATTEMPT, attempting TFTP access of /nstation/fonts/pcf/misc/7x14
B.pcf on 9.24.104.240 for /nstation/fonts/pcf/misc/7x14B.pcf
+ 0:00:00:32
%NETFILE-I-OPENSUCCESS, open succeeded for /nstation/fonts/pcf/misc/7x14B.pcf
%FILE-I-READ, reading font file: /nstation/fonts/pcf/misc/7x14B.pcf
%NETFILE-I-OPENATTEMPT, attempting open for /nstation/fonts/pcf/misc/9x15B.pcf
%NETFILE-I-MATCHATTEMPT, attempting TFTP access of /nstation/fonts/pcf/misc/9x15
B.pcf on 9.24.104.240 for /nstation/fonts/pcf/misc/9x15B.pcf
%NETFILE-I-OPENSUCCESS, open succeeded for /nstation/fonts/pcf/misc/9x15B.pcf
%FILE-I-READ, reading font file: /nstation/fonts/pcf/misc/9x15B.pcf
%NETFILE-I-PERMCHKATTEMPT, attempting permission check for /usr/lib/X11/bitmaps/
Login
%NETFILE-W-MATCHFAIL, TFTP permission check attempt for /usr/lib/X11/bitmaps/Log
in returns: Operation not supported on socket
%NETFILE-W-MATCHFAIL, TFTP permission check attempt for /usr/lib/X11/bitmaps/Log
in returns: Operation not supported on socket
%NETFILE-E-OUTOFMATCHES, operation failed, no more matches for /usr/lib/X11/bitm
aps/Login
%NETFILE-I-STATATTEMPT, attempting stat for /usr/lib/X11/bitmaps/Login
%NETFILE-W-MATCHFAIL, TFTP stat attempt for /usr/lib/X11/bitmaps/Login returns:
Operation not supported on socket
%NETFILE-W-MATCHFAIL, TFTP stat attempt for /usr/lib/X11/bitmaps/Login returns:
Operation not supported on socket
%NETFILE-E-OUTOFMATCHES, operation failed, no more matches for /usr/lib/X11/bitm
aps/Login
```

Figure 340. Message Log with File Extended Diagnostics Enabled

You can then turn off the extended diagnostics by accessing the value in the same way and clicking it off. Remember that this is a value that is kept in NVRAM and therefore, rebooting does not necessarily turn extended diagnostic off, unless there is a specific parameter set in the configuration files on the server to turn extended diagnostic off.

The number of messages issued when extended diagnostics is turned on is very large, so it is a good thing to remember to turn it off when it is not required.

---

## 19.10 Uploading Dump Files

When the Network Station encounters a severe problem, the user may see a window, called a Panic screen, with a cryptic message about the location of the error. If service personnel then require a dump of the Network Station memory in order to do problem determination, there are two boot monitor commands that allow a dump file (essentially a map of the memory) to be uploaded to the boot server.

The commands are:

- UP - to upload using TFTP
- UN - to upload using NFS

### 19.10.1 Using TFTP to Upload a DUMP File

#### Memory greater than 32M

Please note that TFTP cannot upload Panic dumps from Network Stations with memory greater than or equal to 32M; in these cases therefore, please use NFS as the upload method.

Here is a suggested procedure to upload via TFTP:

- On the boot server:
  1. Create a directory called \nstation\service.
  2. Create a dummy file called yyyyyyyy.dmp where yyyyyyyy is the last eight digits of the MAC address of the Network Station.

**Note:** This file must exist before you upload, otherwise you will get an access denied message.
  3. Update the TFTP configuration to allow write operations and save the file, which causes the service to be restarted.
- On the Network Station, after the Panic screen:
  1. Issue the UP boot monitor command.

We had to use the format UP /nstation/ to which the boot monitor added /service/yyyyyyyy.dmp.
  2. The adapter is opened, the ring entered, and a progress indicator bar appears (similar to the progress bar you get during a kernel load). Press ESC if you need to interrupt the transfer.
- On the server, after the upload, remember to reset the TFTP service to read only.

### 19.10.2 Using NFS to Upload a DUMP File

If you prefer to upload using NFS, which is the recommended method, the procedure is as follows

- On the boot server:

1. A directory called `x:\nstation\prodbase\service` already exists and is configured in NFS with an alias of `/netstation/prodbase/service/`, and with read/write permission, as illustrated in the next figure:

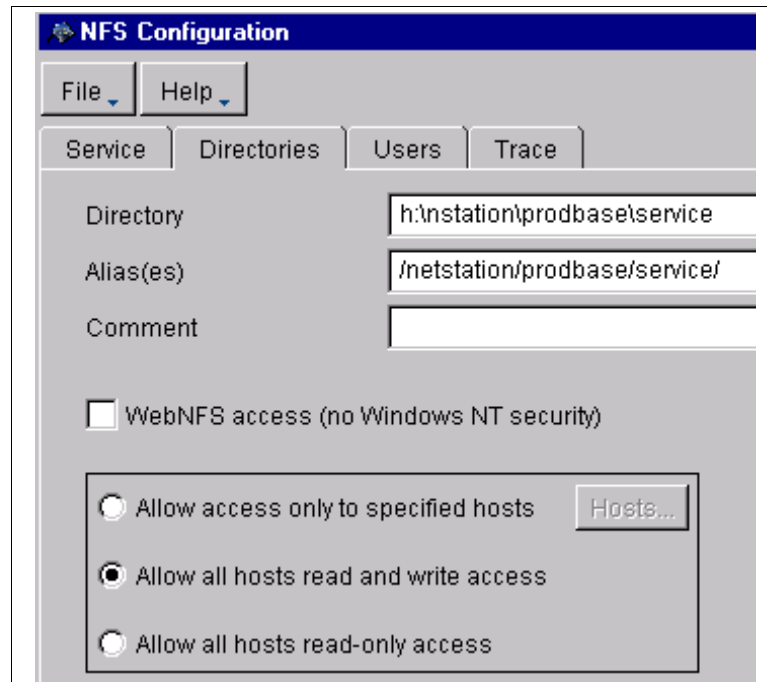


Figure 341. NFS Service Directory

2. Create a dummy file called `yyyyyyyy.dmp`, where `yyyyyyyy` is the last eight digits of the MAC address of the Network Station and save it in the `\nstation\prodbase\service` directory, because a file must already exist before it can be replaced.
- On the Network Station, after the Panic screen:
    1. Issue the UN boot monitor command.  
If the file does not already exist on the host, you get the message:  

```
NS0784 NFS failed file 'xxxxx.xxx' not found.
```

  
If you need to interrupt the transfer, press the ESC key. You can then re-enter a command on the boot monitor command line.
    2. The adapter is opened, the ring is entered and a progress indicator bar appears indicating the upload is happening.

**Note 1:** According to the format of the UN command, you are supposed to be able to specify your own file name, in which case you must also specify the path. We somehow never were able to make it work with a file name other than the default (last eight digits of the MAC address).

**Note 2:** In our tests, we did not have to alter any NT permissions settings or to check the WebNFS Access check box in order to make this work.

---

## 19.11 Resetting NVRAM Defaults

There might be cases where you need to reset all the NVRAM settings to the defaults, thereby eliminating any changes you might have made.

To reset the defaults:

1. Get a boot monitor command prompt.  
To do this, use the L-Alt+Caps Lock+Pause key sequence if your Network Station is in the running mode. Otherwise, use the L-Alt+L-Shift+L-Ctrl+F1 if in the setup utility mode.
2. Issue the `NV` command to run the NVRAM utility.
3. Type `L` to load the Network Station's defaults.
4. Type `S` to save these default parameters; confirm by clicking **Yes**.
5. Type `Q` to quit and return to the boot monitor.
6. Use F1 to get back to the Setup utility.

---

## 19.12 Resetting the IBM Network Station Password

The administrator can set a password on the Network Station to prevent users from changing any of the data in the NVRAM that is necessary to boot the Network Station.

There might be cases where you, as the administrator, forget what password was set for a particular station.

You might also get the case where the station was booted from a boot server that is not yours, and that server's configuration files included a password that you are not aware of.

Whatever the case, this calls for taking physical action to remove the password from the workstation. The procedure for doing this is:

1. Power off the Network Station.
2. Open the cover.
3. Locate the TP1 and TP2 test points.
  - For a Model 100 or 300  
If you hold the station such that the PCMCIA slot is to your left, the TP1 and TP2 test points are located next to the bottom right-hand corner of the PCMCIA adapter slot, between the PCMCIA and a hex screw securing the board to the cover, as illustrated in the next figure.

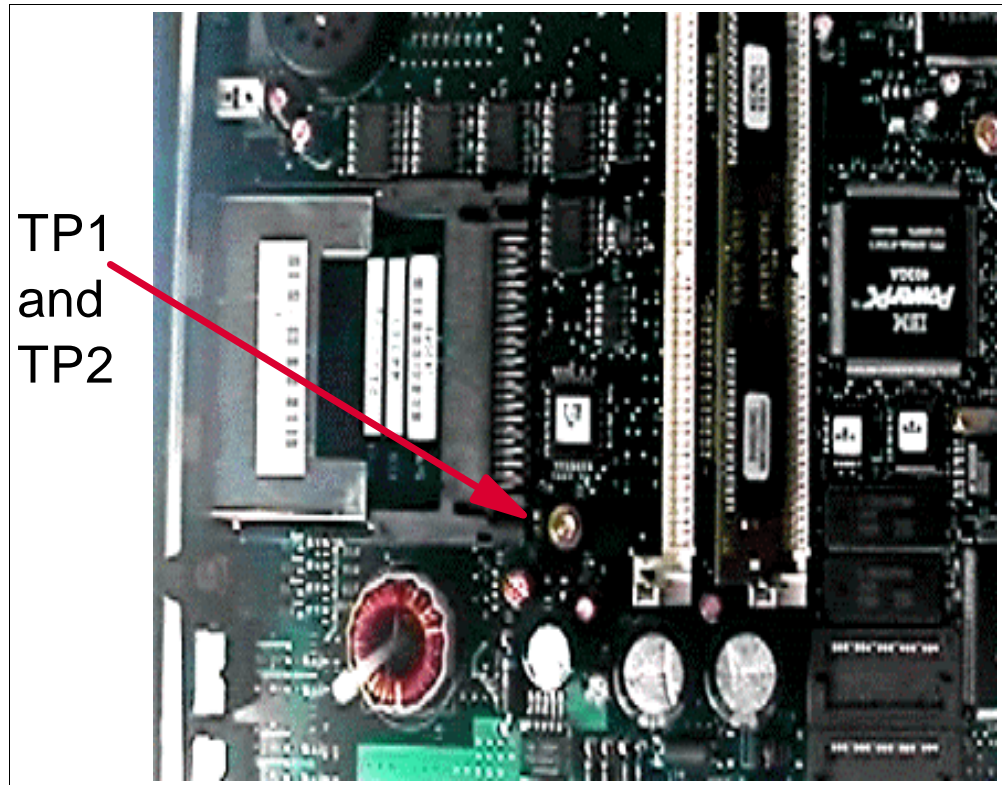


Figure 342. Resetting Password

- For a model 1000, if you hold the IBM Network Station facing you, when opened up, with the back of the station to your left and the front to your right, the TP1 and TP2 test points are located at the top of the unit, about 25% of the way towards the rear of the unit when you start from the front.  
There are in fact the words Reset Password inscribed on the board right below the test points.
- 4. *Carefully* shunt the TP1 and TP2 test points with a flat head screwdriver, and while holding tightly, power on the station.
- 5. A red message “NS0210 NVRAM initialize jumper detected” after 2-3 seconds indicates success.
- 6. Power off, re-install the cover and you are ready to proceed.

## 19.13 Avoiding Reboots

Whenever you are testing at the Network Station, or doing problem determination, and you need to change the settings of one or more parameters, there is not always a need to reboot in order to make those changes effective, and you can save yourself some valuable time by avoiding unnecessary reboots. Here are a few tips on the matter:

- First, use the Console Setup facilities to change parameters in a temporary way.
- Once the change is made, if the parameter is identified as an immediate effect parameter, then it becomes effective immediately.

- If you then want to apply it in the configuration files on the server to make sure that it is coded properly, make the change, and then use the Defaults button on one of the Setup panels, or the Restore Defaults on the File pull-down of one of the Setup panels. This causes the kernel to read its configuration files from the server. If you have your Setup utility panel opened, you can see the changes take effect immediately.
- If the parameter you changed is in one of the startup files, then you need to do a log out, which causes all the configuration files to be reloaded but also the startup files to be processed after the new user login.
- Finally, if you make a change to a parameter that is effective only at boot time, you then do need to reboot in order to test out that parameter. You can cause a reboot by selecting the **Reboot** item on the Console pull-down, or you can use the control key sequences we discussed earlier.

---

## 19.14 Rebooting IBM Network Stations Remotely

A new utility called nsreboot is available with the NSM Service Update 2.

This utility and instructions on how to use it are located in the x:\ntnsm\en\utility directory on the CD-ROM.

In summary, you can cause a remote IBM Network Station to reboot by issuing commands from a remote PC.

The prerequisites are that there must be a configuration password set on the IBM Network Station. This can be done in NSM by selecting **Hardware=>Workstations=>System Defaults=>Configuration Password**.

You can then issue a command such as the following, where 5999 is the configuration port number (by default):

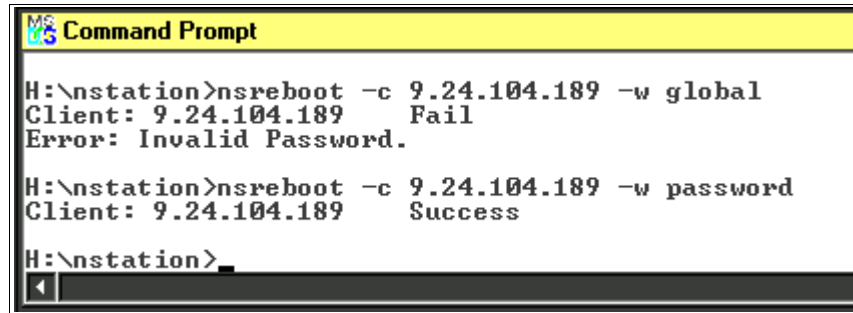
```
nsreboot -c station1 -w password1 -p 5999
```

The -p parameter is optional unless the configuration port number is other than 5999.

This can also be done for a list of stations by entering the different stations addresses and password in a file and specifying the file name on the nsreboot command, or range of IP addresses if all stations have a common password and common configuration port number.

Results are displayed on the console by indicating the success and failure of each attempt, as illustrated in the next figure, where the first attempt with a password of global fails, but the second attempt with a password of password succeeds.





```
H:\nstation>nsreboot -c 9.24.104.189 -w global
Client: 9.24.104.189    Fail
Error: Invalid Password.

H:\nstation>nsreboot -c 9.24.104.189 -w password
Client: 9.24.104.189    Success

H:\nstation>
```

Figure 343. NSREBOOT Command Sample Output

See the x:\ntnsm\en\utility\nsreboot.txt file on the CD for details.

In you specify *public* as the password, which is the default read-only password for the configuration port, you get an indication back of SUCCESS but actually nothing happens.

If you have both a global unit password and a specific read-write configuration password in effect, either will work. Remember as well that passwords are case-sensitive.

**Note:** The nsreboot utility is currently available on Windows NT only. However, a remote reboot of a station can also be caused by using a telnet session to port 5999 and issuing the following commands:

```
set unit-administrative-status = unit-reset
apply
```

As the apply is issued, it causes the station to reboot. This method can therefore be used on any platform.

---

## 19.15 Getting Additional Messages with Java

When working with Java applications, the way to get additional information logged to the message log is to use the -verbose option on the java command.

---

## 19.16 Service Information Tool

There is a service tool called ntnsmver, located in nstation\servbase\bin, which can be executed to provide service personnel with a great amount of information on the status of the installed server.

The tool has eight main categories of information that it gathers, such as:

- Web server environment variables
- Hard disk information
- Registry settings
- List of running services
- Network port status
- TCP/IP information
- User information
- Binary file information

The utility can be executed in two ways:

1. Locally, on the server itself, by entering the following on a command line to direct the output to a file that can then be sent to service personnel:

```
ntnsmver > output_file
```

2. Remotely using a Web browser by IBM Service personnel using a browser to access the same information in an interactive fashion by using the following URL:

`http://server_location/networkstation/cgi/service`

An administrative user ID and password is required. The output is illustrated in the next figure. Any of the categories can be selected directly to view the relevant information.



Figure 344. Executing ntnsmver through a Web Browser

The amount of text lines produced can easily be upwards of 800 lines, so it may take a while to load if you are on a slow link.

## 19.17 Lotus Domino Go Webserver Logging/Reporting

Access logging and error logging on the Lotus Domino Go Webserver is controlled through the interactive configuration interface.

On the Configuration and Administration Forms panel, select the **Logging and Reporting** section, which displays as illustrated in the next figure.

Log files are stored in `x:\www\Logs`.

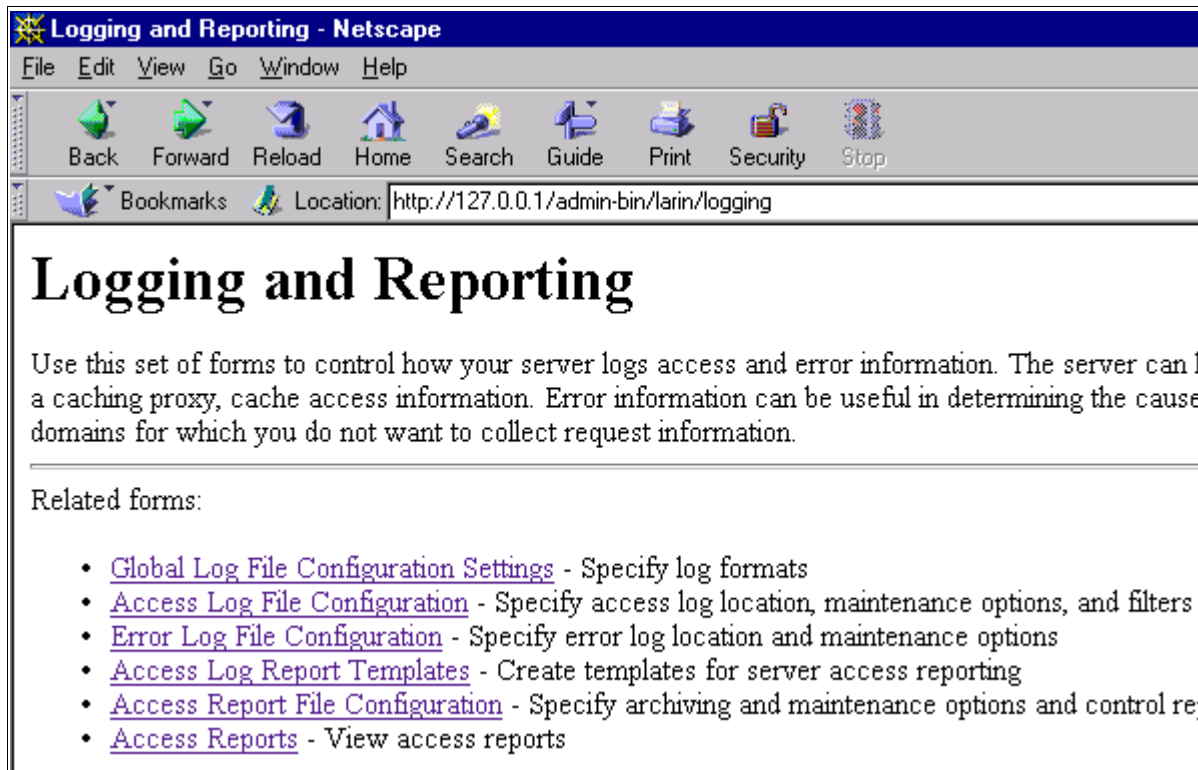


Figure 345. Lotus Domino Go Webserver Logging and Reporting

## 19.18 DHCP Server Logging/Tracing

The DHCP server log file is essential in doing problem determination when using DHCP. This log file, when enabled with the TRACE options, displays all the processing details from the receipt of a DHCP discover broadcast frame, to looking up the DHCP configuration file searching for a matching client, to issuing a DHCP offer to a valid client.

From this log, the administrator can determine exactly what happened after the receipt of a request, or even if the request was ever received from a client.

The option that produces the greatest number of log entries is the Trace messages option, but it is also the most useful when trying to identify the cause of a problem because of the details it provides.

DHCP logging is configured by selecting **DHCP Server** on the main window, then **Configure=>Modify selected object**.

By default, logging is configured to take place with a few categories of events pre-selected, as well as the number of log files, size and name, as illustrated in the next figure:

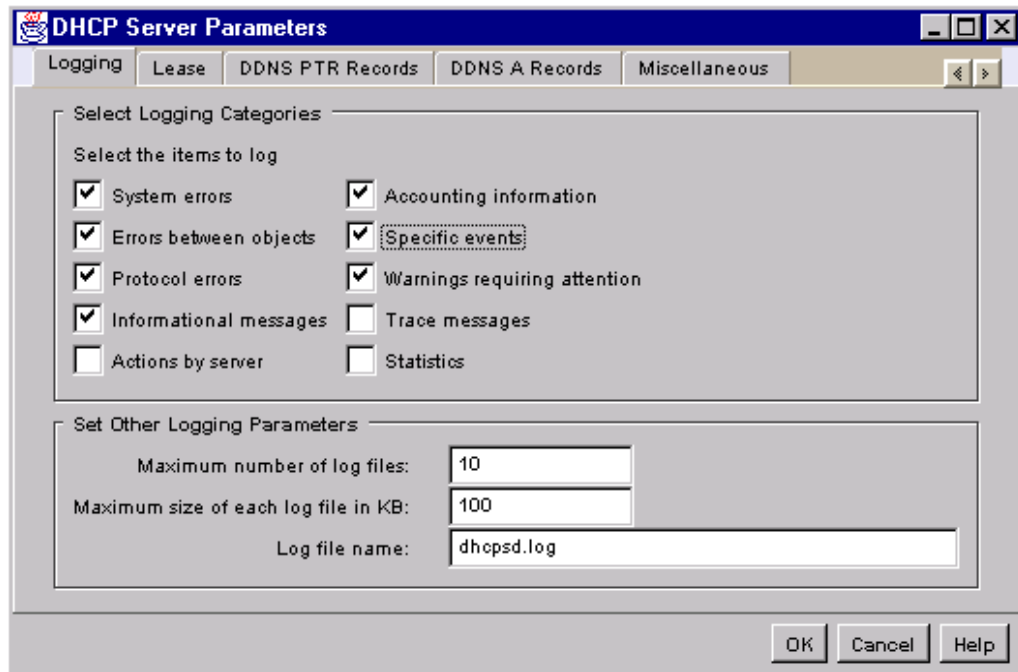


Figure 346. DHCP Server - Logging Parameters

To enable logging by the server, all of the following must be specified:

- Number of DHCP log files
  - If the value for Maximum number of log files is 0, no logging occurs.
  - All older files are renamed by incrementing the previously appended integer filetype by 1. For example, DHCPSPD.003 is an older log file than DHCPSPD.001.
- Size of each log file
 

Maximum log file size in kilobytes. The minimum size is 1 KB.
- Name of the log file

If you do not specify a path, the log file will be stored in `\winnt\system32\dhcpsd.log`. If you find this too cumbersome, you can change the location of the log files in two ways:

1. In the previous version, you were allowed to put a complete path here, such as `d:\work\dhcpsd.log`; however, this version only allows `\path\` to precede the file name. (A drive:`\` cannot be specified.) For example, if you specify `\dhcplogs\dhcpsd.log`, you must first create a directory called `dhcplogs` on the same drive where `\winnt\system32` is.
2. You can manually alter the logging entry on the `dhcpsd.cfg` file, and specify a path such as `d:\work\dhcpsd.log`. This will work and the DHCP server will start and actually use that path. However, every time you start the DHCP configuration interface, the logging statement triggers an error message, illustrated in the next figure, which can be ignored by clicking on **Continue**.

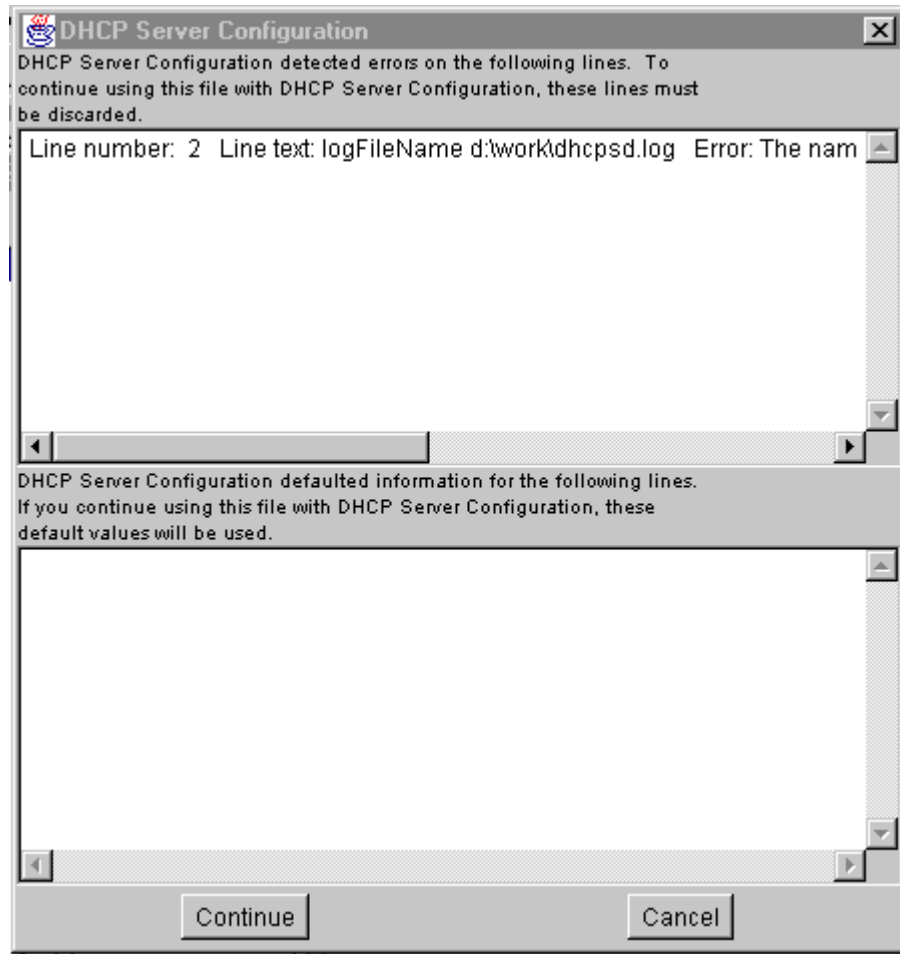


Figure 347. Error Message - Log File Name

#### 19.18.0.1 Tracing

The amount of information logged is dependent on the number of categories that you select.

If you want to get the tracing information, there are two ways of doing this:

1. Open the configuration file and modify the logging selections to include the TRACE category, along with all the other categories. Save the file and re-initialize the server to start logging all entries.
2. Use the **Start Trace** button on the DHCP Server Administration panel (see Figure 173., "DHCP Server Administration - Server" on page 193), which dynamically includes the TRACE category to the log and therefore is a much easier method. Then simply click the **Stop trace** button after you have captured the events that you need in order to get back to normal logging.

In a test environment, if you do not need to keep the log and you want a clean log to start with in order to facilitate your search in the log for particular events, you can simply erase the dhcpcsd.log file, then re-initialize the server and start the trace.

Shown below is an extract from a sample DHCP log files to illustrate the types of messages that are logged when all options are selected. We have extracted only certain key entries to show how a received request can be tracked in terms of its processing by the DHCP server.

This particular trace, taken with the previous version, shows a normal flow where a client with a MAC address of 0000e568bfad is given an offer for address 9.24.104.189.

```

07/22/97 10:42:45 START: .....log_initialize: *****
07/22/97 10:42:45 START: .....log_initialize: *      NEW LOG FOLLOWS      *
07/22/97 10:42:45 START: .....log_initialize: * | | | | | | | | | | *
07/22/97 10:42:45 START: .....log_initialize: * V V V V V V V V V V V *
07/22/97 10:42:45 START: .....log_initialize: *****
07/22/97 10:42:45 SYSERR: .....log_initialize: Logging ENABLED
07/22/97 10:42:45 OBJERR: .....log_initialize: Logging ENABLED
07/22/97 10:42:45 PROTERR:.....log_initialize: Logging ENABLED
07/22/97 10:42:45 WARNING:.....log_initialize: Logging ENABLED
07/22/97 10:42:45 EVENT: .....log_initialize: Logging ENABLED
07/22/97 10:42:45 ACTION: .....log_initialize: Logging ENABLED
07/22/97 10:42:45 INFO: .....log_initialize: Logging ENABLED
07/22/97 10:42:45 ACNTING:.....log_initialize: Logging ENABLED
07/22/97 10:42:45 STAT:.....log_initialize: Logging ENABLED
07/22/97 10:42:45 TRACE: .....log_initialize: Logging ENABLED
.....
07/22/97 10:42:46 INFO: .....etc\\dhcps.crb: previous map files not removed; try to
accommodate within new config
07/22/97 10:42:46 TRACE: .....locateAddressRecord: function Entered
07/22/97 10:42:46 TRACE: .....etc\\dhcps.crb: previous address 9.24.104.185 has been adopted
07/22/97 10:42:46 TRACE: .....locateAddressRecord: function Entered
.....
07/22/97 10:50:42 TRACE: ....receiveMailbox: DHCP comm descriptor selected
07/22/97 10:50:42 TRACE: ..main: size of incoming packet is 548
07/22/97 10:50:42 TRACE: ....process_bootrequest: function entered
.....
07/22/97 10:50:42 TRACE: .....legibleRequest: DHCP msg type DHCPDISCOVER
07/22/97 10:50:42 TRACE: ....process_bootrequest: request is self-consistent
.....
07/22/97 10:50:42 TRACE: .....processDISCOVER: function entered
07/22/97 10:50:42 TRACE: .....locateExchange: function entered
07/22/97 10:50:42 TRACE: .....locateExchange: client id matches an active exchange
.....
07/22/97 10:50:42 TRACE: .....locateClientRecord: function Entered
07/22/97 10:50:42 TRACE: .....locateClientRecord: located client 6-0x0000e568bfad in
client records
.....
07/22/97 10:50:42 TRACE: .....processDISCOVER: AM_STATUS_RESERVED
.....
07/22/97 10:50:43 TRACE: ....generate_bootreply: function entered
07/22/97 10:50:43 INFO: ....generate_bootreply: generating a DHCP OFFER reply
.....
07/22/97 10:53:32 TRACE: .....legibleRequest: function entered
07/22/97 10:53:32 TRACE: .....legibleRequest: DHCP msg type DHCPREQUEST
.....
07/22/97 10:53:32 TRACE: processREQUEST: OFFER was selected by client 6-0x0000e568bfad
.....
07/22/97 10:53:32 TRACE: processREQUEST: address 9.24.104.189 has been bound to 6-0x0000e568bfad
.....
07/22/97 10:53:33 TRACE: ....generate_bootreply: function entered
07/22/97 10:53:33 INFO: ....generate_bootreply: generating a DHCPACK reply

```

Figure 348. DHCP Server Sample Message Log

---

## 19.19 Windows NT Network Monitor

The Network Monitor tool is a standard tool available on the Windows NT Server system; it only needs to be selected for install in order to be used.

This tool provides the ability to capture and display LAN frames as they are received by the network adapter, and it is very easy to use.

There are three ways of using this tool:

1. By capturing only the frames *incoming* from the network to the server. This only requires that the Network Monitor tool be installed as part of the NT Server installation and a standard LAN adapter be used.

This does not allow the user to capture outgoing frames, that is frames originating on the server, but does allow you to capture all the frames whose destination is the server.

2. By using a network adapter that can be set to promiscuous copy mode, all frames originating on the server to any destination can also be captured. This then allows the administrator to see all frames, either received by the server or sent by the server. This is extremely useful for doing problem determination of a DHCP server.

### Adapters Supporting Promiscuous Copy Mode

Note that not all adapters can be set to promiscuous copy mode. For a list of IBM adapters that support this mode, go to the Web site:

<http://www.networking.ibm.com/support>

and use the search facility using the word promiscuous. This should return a page entitled IBM Promiscuous Copy Support where you will find a list of all the adapters and whether they support this mode or not.

Once you have an adapter that supports the promiscuous copy mode, it might be necessary to make some entries in the NT registry in order for the adapter to function in this mode. See the following Web site for instructions on how to do this:

<http://www.microsoft.com/kb/articles/q152/6/43.htm>

We have also reproduced these instructions below for your convenience:

1. Run the Registry Editor (regedt32.exe).
2. From the HKEY\_LOCAL\_MACHINE subtree, find the key:  
    \SYSTEM\CurrentControlSet\Services\bh\Parameters.
3. On the Edit menu, choose **Add Key**, Key Name = ForcePmode, Class = (leave blank).
4. Then select the key you just created, and choose **Add Value** on the Edit menu.
5. Add the following: Value Name= EPRO1 as an example. (Our value was Streamer.)

The value should be the same as the name in the  
    \SYSTEM\CurrentControlSet\Services\bh\Linkage key, under the Bind



Value with the leading "\Device\" stripped off, Data Type = REG\_DWORD and Data = 1.

6. Choose **OK** and quit the Registry Editor.

The figures below illustrate how these entries appear on our test system, which uses an IBM TRN Streamer adapter.

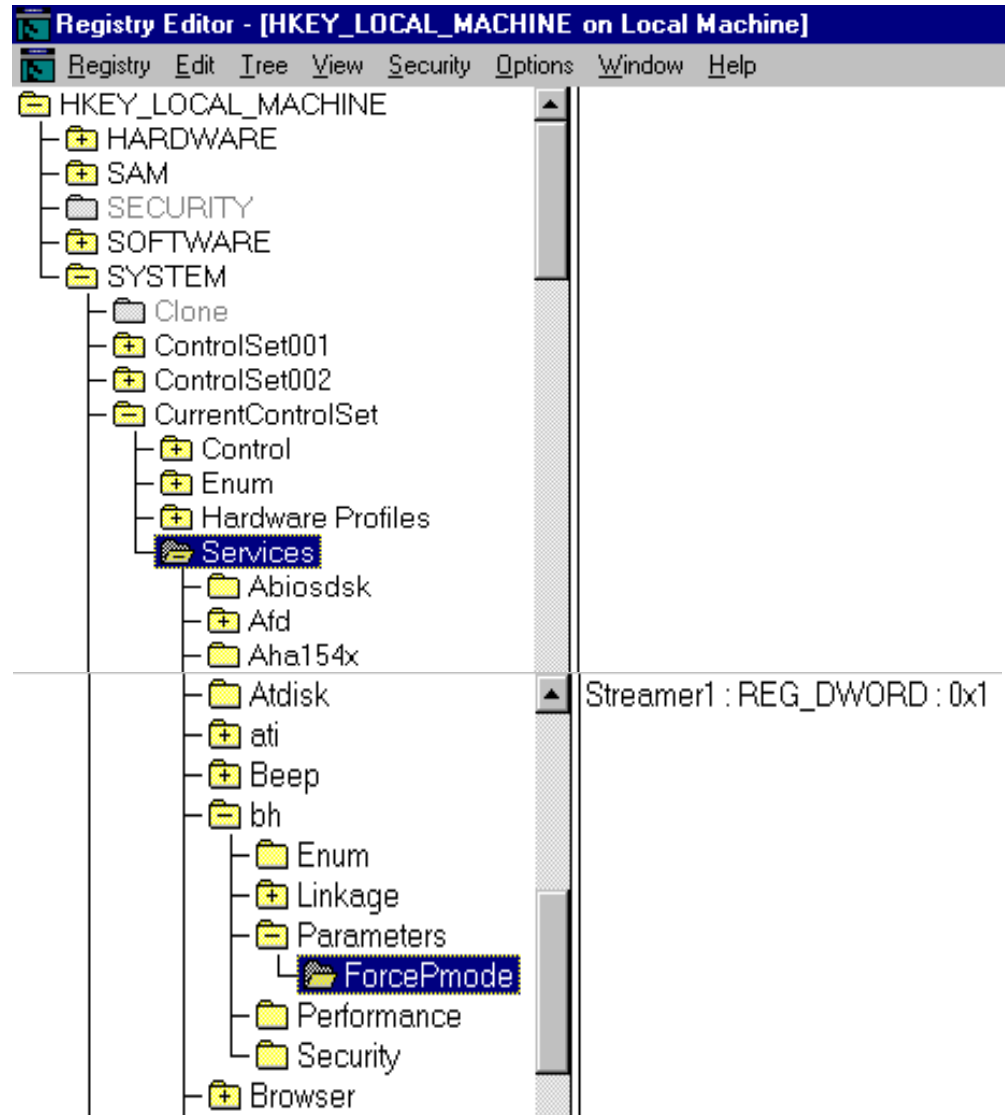


Figure 349. The ForcePmode Registry Entry

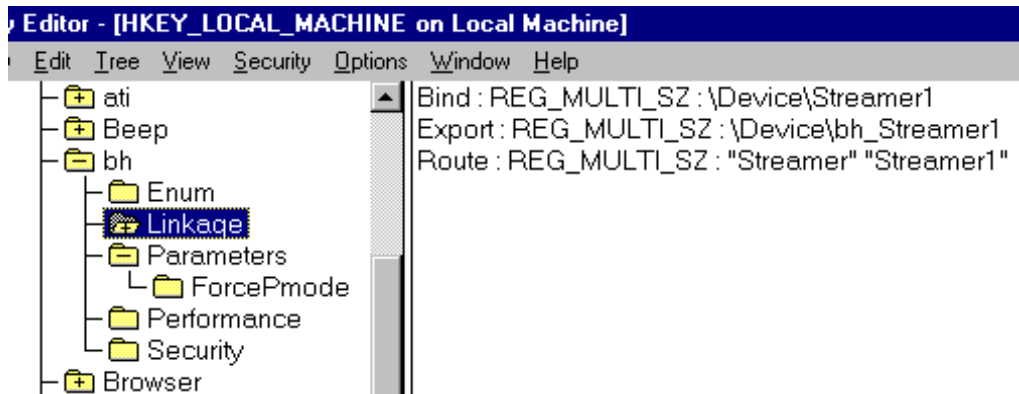


Figure 350. The Linkage Registry Entries

3. By using the version of the Network Monitor that comes with the Microsoft Systems Management Server utilities.

With the standard network monitor tool, one can only display the frames *originating from* or *received by* the adapter where the Network Monitor tool resides.

If one needs to display *all* frames, that is frames originating from any adapter on the LAN or destined to any adapter on the LAN, then one should use the version of the Network Monitor tool available with SMS. In fact, a message to that effect is displayed by the standard tool if the user tries to set filters to capture frames from addresses other than his or her own.

### 19.19.1 Installing the Network Monitor Tool

To install the Network Monitor tool, click on **Start=>Settings=>Control Panel=>Network=>Services**. Click on **Add**, select **Network Monitor Tools and Agent**, as shown in the figure below, and click on **OK**. You will need the Windows NT Server 4.0 CD in order to add this component.

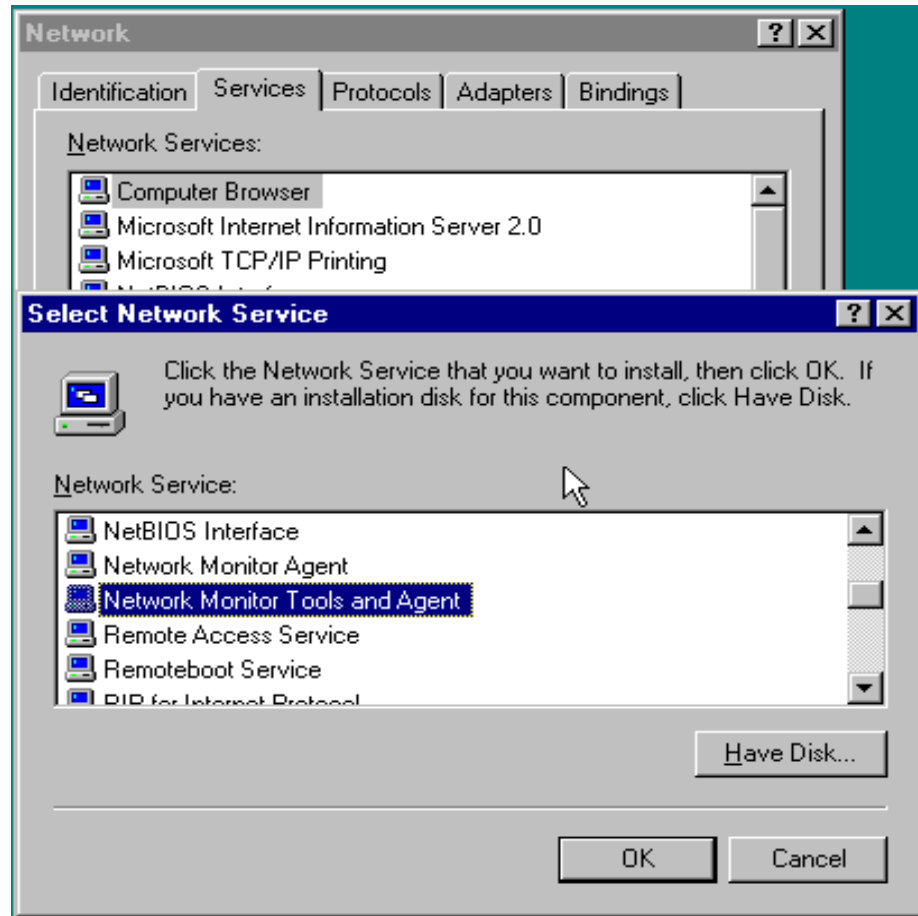


Figure 351. Network Monitor Tool Installation

### 19.19.2 Using the Network Monitor Tool

There are two major steps in using the Network Monitor tool:

1. Capturing the data

This is done by simply starting the Network Monitor tool. By default, the tool captures all frames, for all protocols and for all LAN addresses. Start the tool by clicking **Capture**, then **Start**.

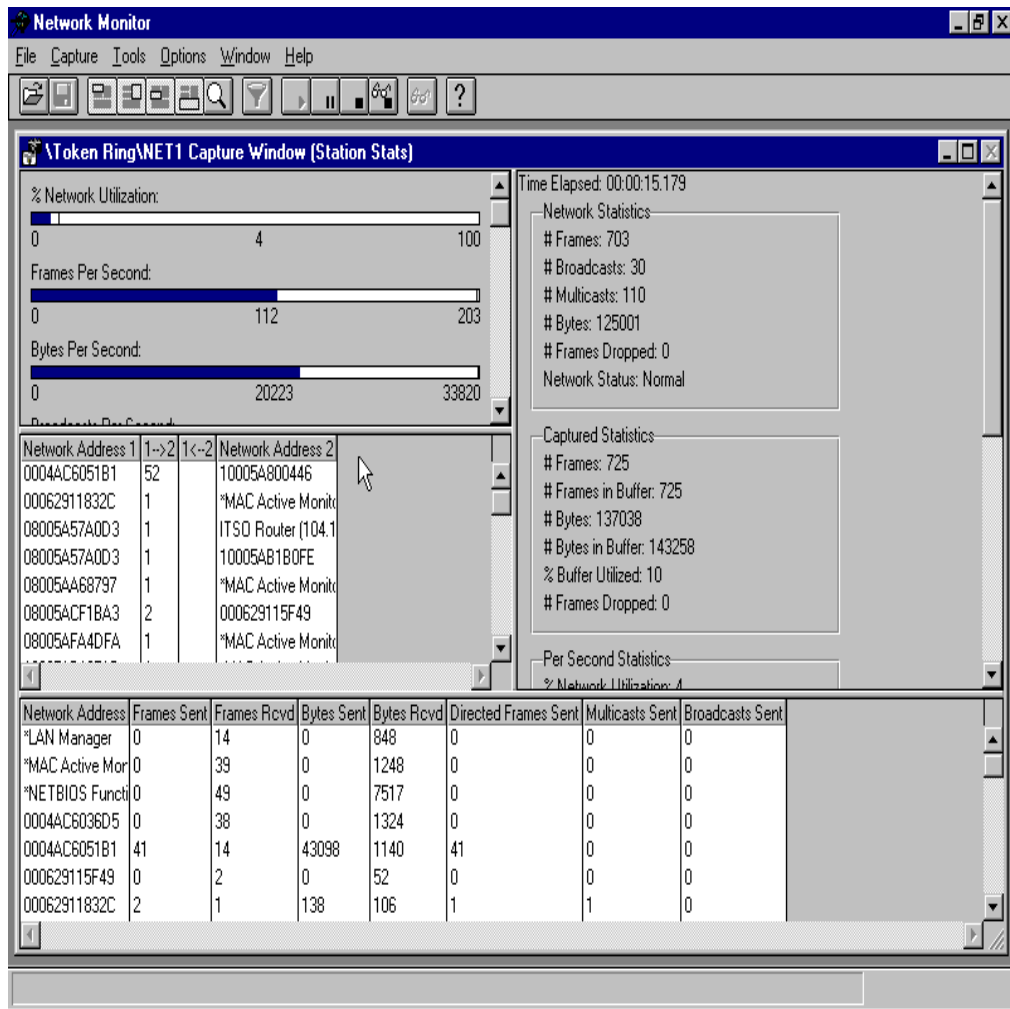


Figure 352. Network Monitor Tool - Main Panel while Capturing Data

This panel is partitioned into many specific areas. While the capture is going on, the area on the right shows running statistics on the number of frames on the network, the total number captured, etc. This area scrolls down for additional categories as well.

On the top left-hand corner are bars indicating percent of network utilization, frames per second, bytes per second, etc. This is also an area that can be scrolled to show additional statistics.

In the bottom left-hand corner are two areas showing a summary of the number of frames to and from specific addresses, with additional information on a per address basis in the bottom part of the display.

If there is a need to minimize the amount of data captured, the user can set capture filters in order to do a selective capture. The panel below illustrates the Capture Filter panel.

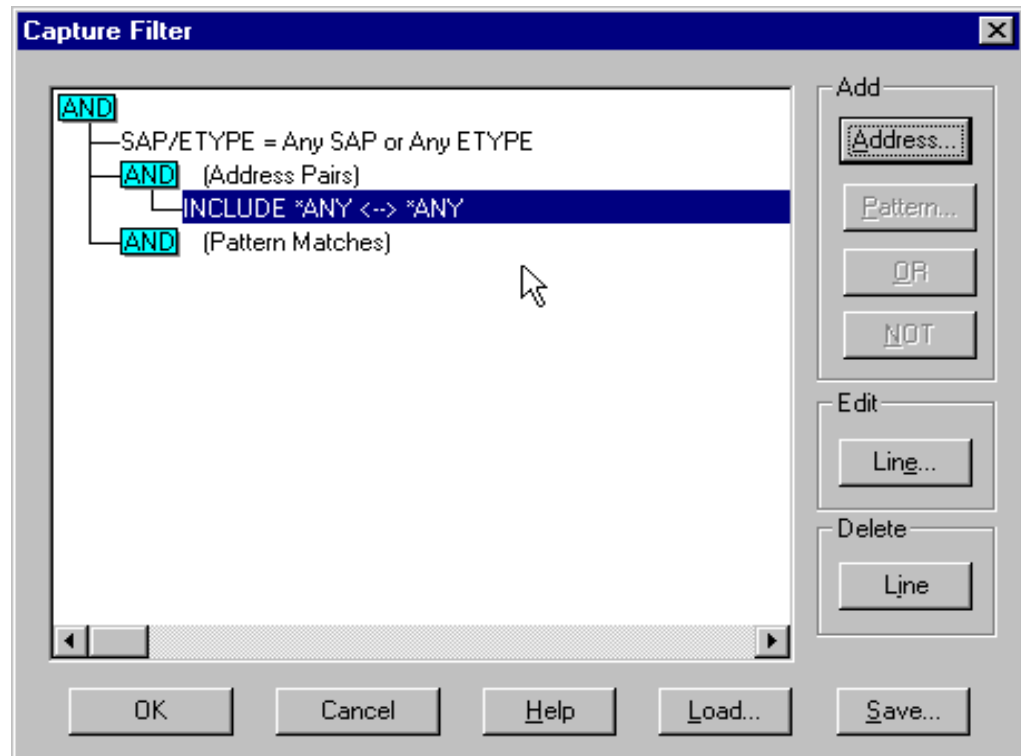


Figure 353. Network Monitor Tool - Capture Filters

Clicking on **INCLUDE ANY <==> ANY** brings up the panel below where you can include or exclude certain addresses. Notice that you can set to capture frames going from station 1 to station 2, or from station 2 to station 1, or from both directions by setting the arrow in the pane labeled Direction in the center of the panel.

Unless you have some disk space problems, it is probably easier to capture all frames and then use filters at display time to selectively look at the data.

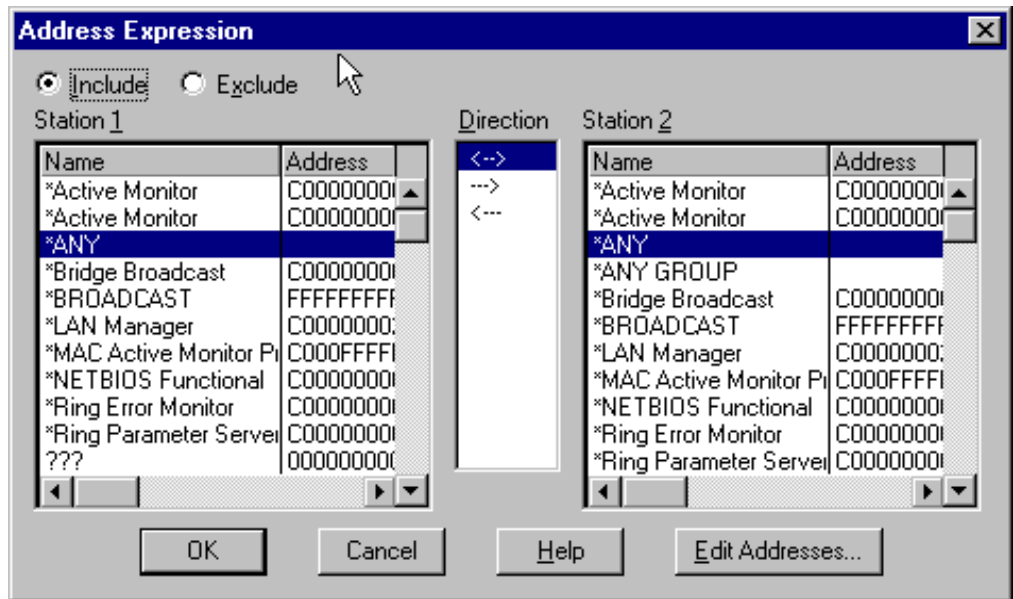


Figure 354. Network Monitor Tool - Filtering on Addresses

## 2. Displaying the captured data

Once the capture is stopped, the user can then display all the frames that have been captured. Below is the panel showing all the frames captured when no display filters have been applied. This display can be scrolled of course, since there can be hundreds and thousands of messages in the capture file.

Network Monitor - [C:\SMSADMIN\NETMON\X86\CAPTURES\DHCPACK0K.cap (Summary)]					
File Edit Display Tools Options Window Help					
Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
23	44.025	INS 1	*BROADCAST	DHCP	Discover (xid=BA010000)
24	44.056	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
25	46.097	INS 1	*BROADCAST	DHCP	Discover (xid=BA010000)
26	46.128	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
27	46.492	ITS0 Router (	INS 1	ICMP	Echo, From 09.90.72.162 To 09.24.104.189
28	46.493	ITS0 Router (	INS 1	ARP_RARP	ARP: Request, Target IP: 9.24.104.189
29	46.504	INS 1	???	ICMP	Echo Reply, To 09.90.72.162 From 09.24.104.189
30	46.510	INS 1	ITS0 Router (	ARP_RARP	ARP: Reply, Target IP: 9.24.104.1 Target Hdw Addr: 40005200501
31	47.115	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
32	47.476	ITS0 Router (	INS 1	ICMP	Echo, From 09.90.72.162 To 09.24.104.189
33	47.485	INS 1	???	ICMP	Echo Reply, To 09.90.72.162 From 09.24.104.189
34	48.169	INS 1	*BROADCAST	DHCP	Discover (xid=BA010000)
35	48.201	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
36	48.257	INS 1	ITS0 Router (	ARP_RARP	ARP: Reply, Target IP: 9.24.104.1 Target Hdw Addr: 40005200501
37	48.718	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
38	50.246	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
39	50.255	INS 1	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.104.189
40	50.767	INS 1	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.104.189
41	50.928	NT Boot Serve	*MAC Active M	TMAC	Standby Monitor Present
42	50.990	INS 1	*MAC Active M	TMAC	Standby Monitor Present
43	51.199	10005A998E4E	INS 1	TMAC	Request Ring Station Attachments
44	51.199	INS 1	10005A998E4E	TMAC	Report Ring Station Attachments
45	51.284	INS 1	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 9.24.104.240
46	51.285	NT Boot Serve	INS 1	ARP_RARP	ARP: Reply, Target IP: 9.24.104.189 Target Hdw Addr: 0000E568E
47	51.298	INS 1	*BROADCAST	DHCP	Request (xid=BA010000)
48	51.330	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
49	51.834	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
50	53.554	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
51	55.193	NT Boot Serve	OPTICL005052	LLC	RR DSAP=0xF0 SSAP=0xF0 C N(R) = 0x4B POLL
52	55.193	OPTICL005052	NT Boot Serve	LLC	RR DSAP=0xF0 SSAP=0xF1 R N(R) = 0x04 FINAL
53	55.228	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
54	56.834	NT Boot Serve	INS 1	DHCP	ACK (xid=BA010000)

Figure 355. Network Monitor Tool - Display Panel

This is, in most cases, too much data to look at, so it is best to first apply display filters in order to have the tool select only certain records for display.

The display filters can be set to:

- Display only certain types of frames.

For example, you can elect to display only DHCP frames. Below is the panel showing the display filter setup. In this example, we have set the filter to display only DHCP frames.

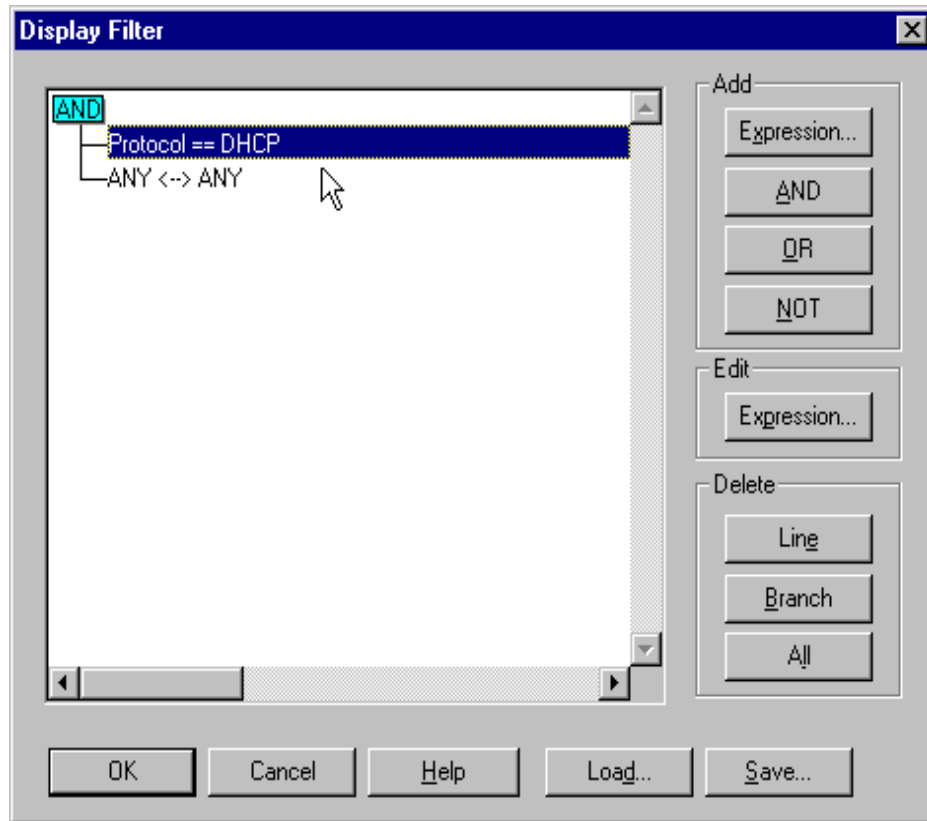


Figure 356. Network Monitor Tool - Display Filters

In the panel above, the Protocol == DHCP line normally displays Any Protocol before you make a change to it. A double-click on that line brings up the panel below, where we used the **Disable All** button to remove all the protocols and then added back only the DHCP protocol.



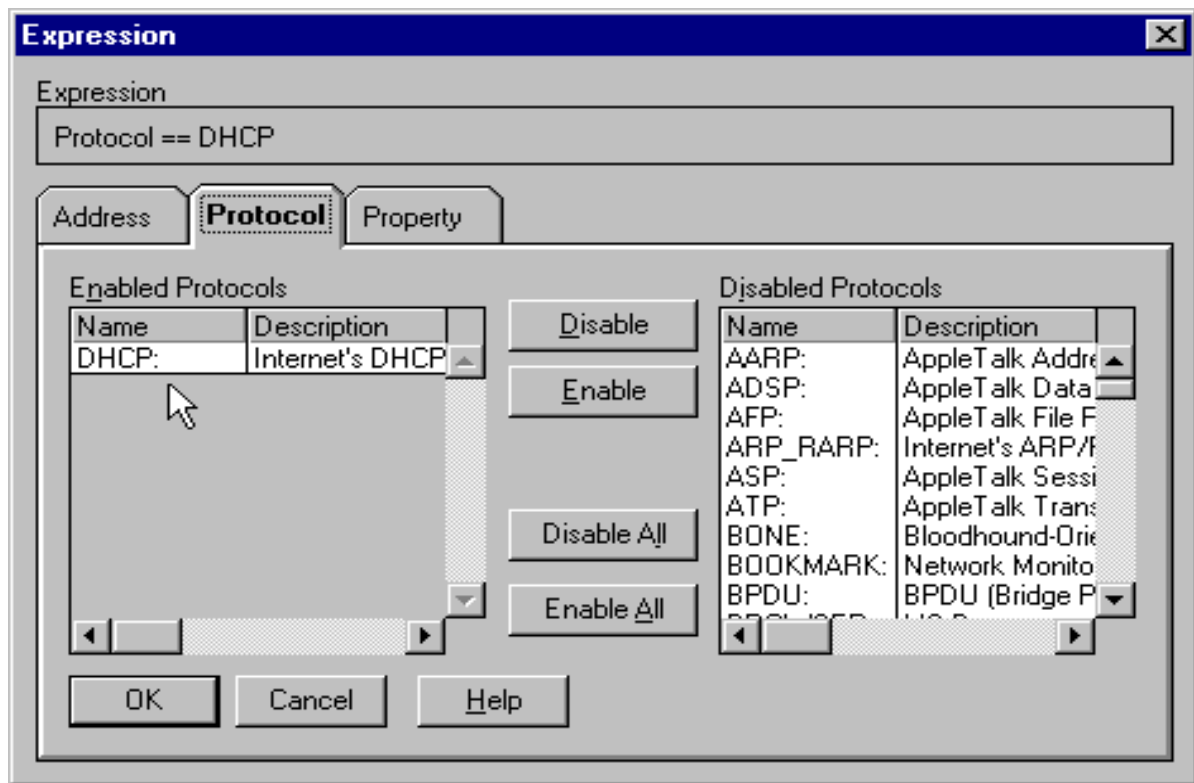


Figure 357. Network Monitor Tool - Selecting the DHCP Frames Only

- Display only frames originating from, or destined to, specific addresses, and these addresses can be expressed as MAC addresses, or IP addresses, etc.

The user can enter names to represent addresses in order to make the display more readable and work with meaningful names as opposed to addresses.

**Note:** If using the standard tool, only frames to and from the local adapter can be displayed.

Shown below is the display resulting from applying the filter above. The number of frames displayed has been significantly reduced and can therefore be more easily analyzed.

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
23	44.025	INS 1	*BROADCAST	DHCP	Discover (xid=BA010000)
24	44.056	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
25	46.097	INS 1	*BROADCAST	DHCP	Discover (xid=BA010000)
26	46.128	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
31	47.115	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
34	48.169	INS 1	*BROADCAST	DHCP	Discover (xid=BA010000)
35	48.201	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
37	48.718	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
38	50.246	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
47	51.298	INS 1	*BROADCAST	DHCP	Request (xid=BA010000)
48	51.330	AS/400 C	INS 1	DHCP	BOOTP/DHCP Packet (xid=BA010000)
49	51.834	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
50	53.554	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
53	55.228	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)
54	56.834	NT Boot Serve	INS 1	DHCP	ACK (xid=BA010000)
64	59.034	NT Boot Serve	INS 1	DHCP	ACK (xid=BA010000)

Figure 358. Network Monitor Tool - Display of DHCP Frames Only

### 3. Displaying the details

Each line displayed can be expanded into a significant amount of details by a double-click on the line.

Each group displayed can then be expanded by a click on the + sign, yielding details down to the bit level in some cases. Also displayed is a hex representation of the data.

In the case of the DHCP frames here for example, all the DHCP options can be displayed.

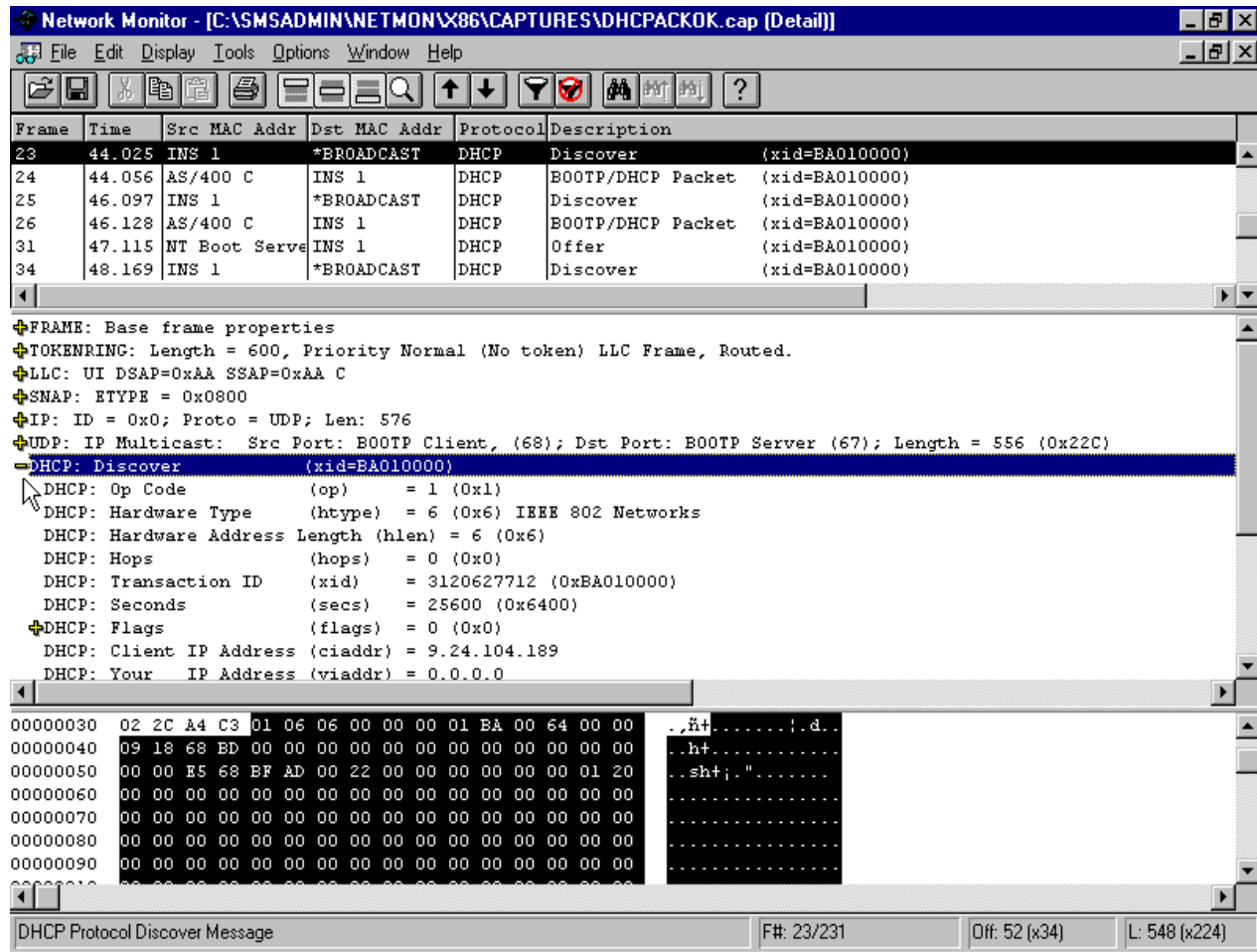


Figure 359. Network Monitor Tool - Displaying the Details of Each Frame

#### 4. Printing the captured data

Selected frames can be printed, or a range of frames can be printed, or you can specify that the same filters used for the display should apply to the printed output. You can reduce the details by choosing to not expand each of the groups within the frame, or to expand all if you want all the details.

Below is an illustration of the print filters that can be used:

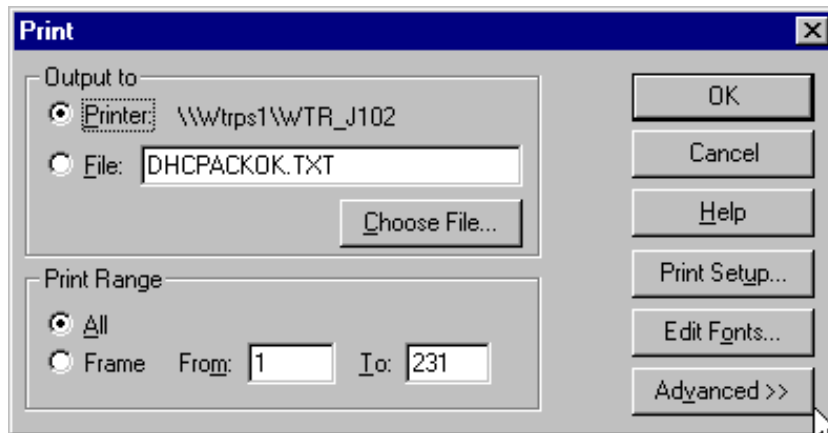


Figure 360. Network Monitor Tool - Printing Selected Frames

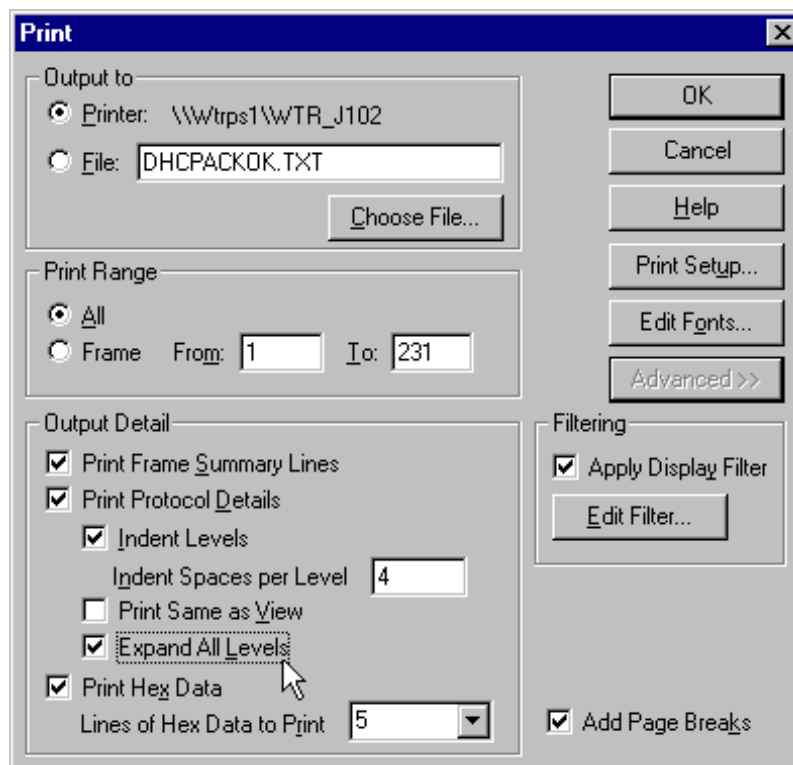


Figure 361. Network Monitor Tool - Printing Selected Frames - Advanced Options

## 5. Sample printed output

Below is an extract from a sample printed output showing a few DHCP frames that have been printed by requesting to expand all groups.

```

*****
Frame   Time   Src MAC Addr   Dst MAC Addr   Protocol   Description
23      44.025  INS 1          *BROADCAST     DHCP       Discover

FRAME: Base frame properties
FRAME: Time of capture = Jul 23, 1997 16:0:35.559
FRAME: Time delta from previous physical frame: 20 milliseconds
FRAME: Frame number: 23
FRAME: Total frame length: 600 bytes
FRAME: Capture frame length: 600 bytes
FRAME: Frame data: Number of data bytes remaining = 600 (0x0258)
TOKENRING: Length = 600, Priority Normal (No token) LLC Frame, Routed.
TOKENRING: Access control = 24 (0x18) Repeated, Frame, Priority: Normal (No token)
    TOKENRING: ....000   Reservation bits: Reservation = Normal, No token needed.
    TOKENRING: ....1...   Monitor bit = Frame has been repeated by Active Monitor.
    TOKENRING: ...1....   Token bit = Frame
    TOKENRING: 000.....   Priority bits: Priority = Normal, No token needed.
TOKENRING: Frame control = 64 (0x40), LLC Frame
    TOKENRING: ....0000   Control bits = Normal Buffered
    TOKENRING: 01.....   Frame type = LLC Frame
TOKENRING: Destination address : FFFFFFFFFFFFFFFF
    TOKENRING: Destination Address I/G Bit           = Group address
    TOKENRING: Destination Address U/L bit           = Locally administered address
    TOKENRING: Destination Address Functional bit     = Group address
TOKENRING: Source address      : 8000E568BFAD
    TOKENRING: Source Address Routing bit = Routing information present
    TOKENRING: Source Address U/L bit     = Universally administered address
TOKENRING: Frame length : 600 (0x0258)
TOKENRING: Routing control 1 = 0x82, length 2, All Routes Broadcast
    TOKENRING: ...00010   Routing length = 2 bytes.
    TOKENRING: 100.....   Broadcast indicator = All Routes Broadcast B'100'
TOKENRING: Routing control 2 = 0x70, Backward, All-routes broadcast.
    TOKENRING: Direction indicator = Forward (left-to-right) direction.
    TOKENRING: Largest frame = All-routes broadcast.
TOKENRING: Tokenring data: Number of data bytes remaining = 584 (0x0248)
LLC: UI DSAP=0xAA SSAP=0xAA C
LLC: DSAP = 0xAA : INDIVIDUAL : Sub-Network Access Protocol (SNAP)
LLC: SSAP = 0xAA: COMMAND : Sub-Network Access Protocol (SNAP)
LLC: Frame Category: Unnumbered Frame
LLC: Command = UI
LLC: LLC Data: Number of data bytes remaining = 581 (0x0245)
SNAP: ETYPE = 0x0800
SNAP: Snap Organization code = 00 00 00
SNAP: Snap etype : 0x0800
SNAP: Snap Data: Number of data bytes remaining = 576 (0x0240)
IP: ID = 0x0; Proto = UDP; Len: 576
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
    IP: Precedence = Routine
    IP: ...0.... = Normal Delay
    IP: ....0... = Normal Throughput
    IP: .....0.. = Normal Reliability

```

Figure 362. Frame 23 - A DHCPDISCOVER Frame - Page 1

```

IP: Total Length = 576 (0x240)
  IP: Identification = 0 (0x0)
  IP: Flags Summary = 0 (0x0)
    IP: .....0 = Last fragment in datagram
    IP: .....0. = May fragment datagram if necessary
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 255 (0xFF)
  IP: Protocol = UDP - User Datagram
  IP: Checksum = 0xB9AD
  IP: Source Address = 0.0.0.0
  IP: Destination Address = 255.255.255.255
  IP: Data: Number of data bytes remaining = 556 (0x022C)
UDP: IP Multicast: Src Port: BOOTP Client, (68); Dst Port: BOOTP Server (67); Length = 556
(0x22C)
  UDP: Source Port = BOOTP Client
  UDP: Destination Port = BOOTP Server
  UDP: Total length = 556 (0x22C) bytes
  UDP: UDP Checksum = 0xA4C3
  UDP: Data: Number of data bytes remaining = 548 (0x0224)
DHCP: Discover (xid=BA010000)
  DHCP: Op Code (op) = 1 (0x1)
  DHCP: Hardware Type (htype) = 6 (0x6) IEEE 802 Networks
  DHCP: Hardware Address Length (hlen) = 6 (0x6)
  DHCP: Hops (hops) = 0 (0x0)
  DHCP: Transaction ID (xid) = 3120627712 (0xBA010000)
  DHCP: Seconds (secs) = 25600 (0x6400)
  DHCP: Flags (flags) = 0 (0x0)
    DHCP: 0..... = No Broadcast
  DHCP: Client IP Address (ciaddr) = 9.24.104.189
  DHCP: Your IP Address (yiaddr) = 0.0.0.0
  DHCP: Server IP Address (siaddr) = 0.0.0.0
  DHCP: Relay IP Address (giaddr) = 0.0.0.0
  DHCP: Client Hardware Address (chaddr) = 0 0 E5 68 BF AD 0 22 0 0 0 0 0 0 1 20
  DHCP: Server Host Name (sname) = <Blank>
  DHCP: Boot File Name (file) = <Blank>
  DHCP: Magic Cookie = [OK]
  DHCP: Option Field (options)
    DHCP: DHCP Message Type = DHCP Discover
    DHCP: Maximum DHCP Message Size = (Length: 2) 02 40
    DHCP: Requested Address = 9.24.104.189
    DHCP: Unrecognized Option = 77 (0x4D)
    DHCP: Client Class information = (Length: 19) 49 42 4d 20 4e 65 74 77 6f 72 6b 20 53 74 61
74 ...
    DHCP: End of this option field
  DHCP: Malformed Packet , Field "Option" is invalid

00000: 18 40 FF FF FF FF FF 80 00 E5 68 BF AD 82 70 .@.....h...p
00010: AA AA 03 00 00 00 08 00 45 00 02 40 00 00 00 00 .....E..@....
00020: FF 11 B9 AD 00 00 00 00 FF FF FF FF 00 44 00 43 .....D.C
00030: 02 2C A4 C3 01 06 06 00 00 00 01 BA 00 64 00 00 .,.....d..
00040: 09 18 68 BD 00 00 00 00 00 00 00 00 00 00 00 00 ..h.....

```

Figure 363. Frame 23 - A DHCPDISCOVER Frame - Page 2

```

*****
Frame   Time      Src MAC Addr  Dst MAC Addr  Protocol  Description
31      47.115    NT Boot Server  INS 1         DHCP      Offer

FRAME: Base frame properties
FRAME: Time of capture = Jul 23, 1997 16:0:38.649
FRAME: Time delta from previous physical frame: 605 milliseconds
FRAME: Frame number: 31
FRAME: Total frame length: 626 bytes
FRAME: Capture frame length: 626 bytes
FRAME: Frame data: Number of data bytes remaining = 626 (0x0272)
TOKENRING: Length = 626, Priority Normal (No token) LLC Frame
TOKENRING: Access control = 24 (0x18) Repeated, Frame, Priority: Normal (No token)
TOKENRING: .....000   Reservation bits: Reservation = Normal, No token needed.
TOKENRING: ....1...   Monitor bit = Frame has been repeated by Active Monitor.
TOKENRING: ...1....   Token bit = Frame
TOKENRING: 000.....   Priority bits: Priority = Normal, No token needed.
TOKENRING: Frame control = 64 (0x40), LLC Frame
TOKENRING: ....0000   Control bits = Normal Buffered
TOKENRING: 01.....   Frame type = LLC Frame
TOKENRING: Destination address : 8000E568BFAD
TOKENRING: Destination Address I/G Bit           = Group address
TOKENRING: Destination Address U/L bit           = Universally administered address
TOKENRING: Destination Address Functional bit = Group address
TOKENRING: Source address      : 400052005210
TOKENRING: Source Address Routing bit = No routing information present
TOKENRING: Source Address U/L bit      = Locally administered address
TOKENRING: Frame length : 626 (0x0272)
TOKENRING: Tokenring data: Number of data bytes remaining = 612 (0x0264)
LLC: UI DSAP=0xAA SSAP=0xAA C
LLC: DSAP = 0xAA : INDIVIDUAL : Sub-Network Access Protocol (SNAP)
LLC: SSAP = 0xAA: COMMAND : Sub-Network Access Protocol (SNAP)
LLC: Frame Category: Unnumbered Frame
LLC: Command = UI
LLC: LLC Data: Number of data bytes remaining = 609 (0x0261)
SNAP: ETYPE = 0x0800
SNAP: Snap Organization code = 00 00 00
SNAP: Snap etype : 0x0800
SNAP: Snap Data: Number of data bytes remaining = 604 (0x025C)
IP: ID = 0xC92C; Proto = UDP; Len: 604
IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type = 0 (0x0)
IP: Precedence = Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability
IP: Total Length = 604 (0x25C)
IP: Identification = 51500 (0xC92C)

```

Figure 364. Frame 31 - A DHCP OFFER Frame - Page 1

```

IP: Flags Summary = 0 (0x0)
    IP: .....0 = Last fragment in datagram
    IP: .....0. = May fragment datagram if necessary
IP: Fragment Offset = 0 (0x0) bytes
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 0x8B87
IP: Source Address = 9.24.104.240
IP: Destination Address = 9.24.104.189
IP: Data: Number of data bytes remaining = 584 (0x0248)
UDP: Src Port: BOOTP Server, (67); Dst Port: BOOTP Client (68); Length = 584 (0x248)
UDP: Source Port = BOOTP Server
UDP: Destination Port = BOOTP Client
UDP: Total length = 584 (0x248) bytes
UDP: UDP Checksum = 0xEB57
UDP: Data: Number of data bytes remaining = 576 (0x0240)
DHCP: Offer (xid=BA010000)
    DHCP: Op Code (op) = 2 (0x2)
    DHCP: Hardware Type (htype) = 6 (0x6) IEEE 802 Networks
    DHCP: Hardware Address Length (hlen) = 6 (0x6)
    DHCP: Hops (hops) = 0 (0x0)
    DHCP: Transaction ID (xid) = 3120627712 (0xBA010000)
    DHCP: Seconds (secs) = 0 (0x0)
    DHCP: Flags (flags) = 0 (0x0)
    DHCP: 0..... = No Broadcast
    DHCP: Client IP Address (ciaddr) = 0.0.0.0
    DHCP: Your IP Address (yiaddr) = 9.24.104.189
    DHCP: Server IP Address (siaddr) = 0.0.0.0
    DHCP: Relay IP Address (giaddr) = 0.0.0.0
    DHCP: Client Hardware Address (chaddr) = 0 0 E5 68 BF AD 0 22 0 0 0 0 0 0 1 20
    DHCP: Server Host Name (sname) = < Blank>
    DHCP: Boot File Name (file) = /nstation/kernel
    DHCP: Magic Cookie = [OK]
    DHCP: Option Field (options)
        DHCP: DHCP Message Type = DHCP Offer
        DHCP: Server Identifier = 9.24.104.240
        DHCP: Renewal Time Value (T1) = 11:56:28
        DHCP: Rebinding Time Value (T2) = 20:53:49
        DHCP: Subnet Mask = 255.255.255.0
        DHCP: Time Offset = (Length: 4) 00 00 00 01
        DHCP: Router = 9.24.104.1
        DHCP: Time Server = (Length: 4) 09 18 68 f0
        DHCP: Domain Name Server = 9.24.104.108
        DHCP: Domain Name = (Length: 16) 69 74 73 6f 2e 72 61 6c 2e 69 62 6d 2e 63 6f 6d
        DHCP: Broadcast Address = 255.255.255.255
        DHCP: IP Address Lease Time = 23:52:56
        DHCP: End of this option field

00000: 18 40 80 00 E5 68 BF AD 40 00 52 00 52 10 AA AA .@...h..@.R.R...
00010: 03 00 00 00 08 00 45 00 02 5C C9 2C 00 00 80 11 .....E..\.,....
00020: 8B 87 09 18 68 F0 09 18 68 BD 00 43 00 44 02 48 ...h...h..C.D.H
00030: EB 57 02 06 06 00 00 00 01 BA 00 00 00 00 00 00 .W.....
00040: 00 00 09 18 68 BD 00 00 00 00 00 00 00 00 00 00 ....h.....

```

Figure 365. Frame 31 - A DHCP OFFER Frame - Page 2



---

## Appendix A. Useful Control Key Sequences

Listed here are some of the control key sequences that can be used on the IBM Network Station.

These keys are sometimes not easy to remember, unless you use them frequently, but they can be useful to save time when doing testing and problem determination.

Key Sequence	Context When Issued	Action	Comments
ESC	Boot time	Stops downloading kernel and invokes Setup Utility main menu	
L-Alt + L-Ctrl + L-Shift + F1	Setup Utility	Enters the boot monitor program	101/102 keyboards only
L-Alt + L-Shift + F1	Setup Utility	Enter the boot monitor program	5250/3270 keyboards only
F1	Boot Monitor	Enter Setup Utility	
L-Alt + Caps Lock + Pause	Window Manager	Enter boot monitor	All applications terminate
L-Alt + L-Shift + Right mouse	Window Manager	Displays local client list	Not operational if window manager not active
L-Alt + Tab	Window Manager	Switches between active windows	Configurable thru pref-console-key-sequence
L-Alt + L-Shift + Home	Window Manager	Toggles console on and off	

Table 12. Useful IBM Network Station Control Key Sequences



---

## Appendix B. Boot Monitor Commands

Below is the list of boot monitor commands.

This list can also be obtained by entering a ? on the boot monitor command prompt.

**BL** [file] boot locally  
**BN** [file] [local-IP host-IP] [gateway-IP] [subnet mask] boot via nfs  
**BR** [retries] booting retries  
**BT** [file] [local-IP host-IP] [gateway-IP] [subnet mask] boot via tftp  
**DA** display addresses  
**DM** [addr] [len] display memory  
**DR** display registers  
**DS** display booting statistics  
**EX** extended tests  
**KM** keyboard mapper  
**MA** [mac address] locally administered MAC address  
**KS** keyboard/mouse statistics  
**NF** [rsize] set block size from 128 to 8192 bytes  
**NV** nvram utility  
**PI** [timeout] [local-IP host-IP] [gateway-IP] [subnet mask] ping host  
**RS** reset system  
**SI** [0/1] set serial i/o mode  
**SB** [enable/disable] subnet broadcast TFTP  
**SE** nvram setup  
**SM** show memory configuration  
**ST** stack trace  
**TI** [num] set warning timeout in 10 seconds intervals  
**TM** [mtu] set TRN MTU  
**TR** [4 or 16] set TRN speed  
**UN** [file][local-IP host-IP][gateway-IP][subnet mask] upload via nfs  
**UP** [file][local-IP host-IP][gateway-IP][subnet mask] upload via tftp  
**ZK** zero keyboard/mouse statistics  
**ZS** zero boot statistics



---

## Appendix C. Special Notices

This publication is intended to help the reader understand the new features and functions available with Release 3 of the IBM Network Station Manager and the differences with the previous release. The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM Network Station Manager. See the PUBLICATIONS section of the IBM Programming Announcement for the IBM Network Station Manager Release 3 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.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

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:

IBM ®	AIX
AS/400	MVS/ESA
OS/390	OS/400
RS/6000	S/390
System/390	VM/ESA

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

---

## Appendix D. Related Publications

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

---

### D.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How To Get ITSO Redbooks" on page 427.

- *IBM Network Station Guide for Windows NT, SG24-2127*
- *S/390 - IBM Network Station - Getting Started, SG24-4954*
- *S/390 - IBM Network Station - End User Information, SG24-4955*
- *AS/400 - IBM Network Station - Getting Started, SG24-2153*
- *IBM Network Station - RS/6000 Notebook, SG24-2016*
- *IBM Network Station Printing Guide, SG24-5212*
- *Network Computing Framework Component Guide, SG24-2119*
- *Internet Security in the Network Computing Framework, SG24-5220*
- *Java Thin-Client Programming for a Network Computing Environment, SG24-5115*
- *Beyond DHCP - IBM's Guide to Network Communications with TCP/IP, SG24-5280*

---

### D.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
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

---

### D.3 Other Publications

These publications are also relevant as further information sources:

- *IBM Network Station Manager Installation and Use, SC41-0664*
  - Microsoft Windows NT Server, Terminal Server Edition, Administrator's Guide
- This publication is shipped with the WTSE product.

- *Microsoft Windows NT Server, Terminal Server Edition, Start Here*  
This is Basics and Installation. Shipped with the WTSE product.
- *Citrix MetaFrame Administrator's Guide*  
This publication is shipped with the MetaFrame product.
- *Citrix MetaFrame ICA Client User's Guide*  
This publication is shipped with the MetaFrame product.
- *UNIX Integration Services Administrator's Guide*  
This publication, from Citrix Systems Inc., is shipped with the UNIX Integration Services product.

---

## D.4 Web Sites

These Web sites are also relevant as further information sources:

- [www.ibm.com/nc/pubs](http://www.ibm.com/nc/pubs)  
The Advanced User Information at this site provides information on full-screen solutions, configuration files and migration.  
This site also points to other IBM Network Station-related publications.
- [service.boulder.ibm.com](http://service.boulder.ibm.com)  
This is the site from where the IBM Network Station Manager code can be obtained.
- [www.pc.ibm.com/networkstation/](http://www.pc.ibm.com/networkstation/)  
This is the IBM home of the IBM Network Station.
- [ftp.software.ibm.com/as400/pubs/netstat/config/](http://ftp.software.ibm.com/as400/pubs/netstat/config/)  
Copies of the original R 2.5 configuration files.
- <http://www.microsoft.com/NTServer/Basics/TechPapers/default.asp>  
Microsoft White papers on Windows NT Server.
- [www.citrix.com](http://www.citrix.com)  
This Citrix Systems Inc. Web site has a lot of information on WinFrame, MetaFrame and related subjects.
- [www.ncd.com](http://www.ncd.com)  
This NCD Inc. Web site has information on WinCenter-related products.



---

## List of Abbreviations

<b>API</b>	Application Programming Interface	<b>TCP</b>	Transmission Control Protocol
<b>CDE</b>	Common Desktop Environment	<b>TFTP</b>	Trivial File Transfer Protocol
<b>DDNS</b>	Dynamic Domain Name Server	<b>UIS</b>	UNIX Integration Services
<b>DHCP</b>	Dynamic Host Configuration Protocol	<b>URL</b>	Universal Resource Locator
<b>DNS</b>	Domain Name Server	<b>WTS</b>	Windows Terminal Server
<b>FTP</b>	File Transfer Protocol	<b>WTSE</b>	Windows Terminal Server Edition
<b>ICA</b>	Independent Computing Architecture	<b>XDMCP</b>	X Display Manager Control Protocol
<b>GMT</b>	Greenwich Mean Time		
<b>HACL</b>	Host Access Class Library		
<b>HLLAPI</b>	High Level Language API		
<b>HOD</b>	Host On-Demand		
<b>HTML</b>	Hyper Text Markup Language		
<b>HTTP</b>	Hyper Text Transfer Protocol		
<b>IBM</b>	International Business Machines Corporation		
<b>ITSO</b>	International Technical Support Organization		
<b>IP</b>	Internet Protocol		
<b>JDK</b>	Java Development Kit		
<b>JIT</b>	Just In Time Compiler		
<b>JRE</b>	Java Runtime Environment		
<b>LPD</b>	Line Printer Daemon		
<b>LPR</b>	Line Printer Requester		
<b>LPRD</b>	Line Printer Requester Daemon		
<b>MAC</b>	Media Access Control		
<b>NFS</b>	Network File System		
<b>NSLD</b>	Network Station Login Daemon		
<b>NSM</b>	Network Station Manager		
<b>OIA</b>	Operator Information Area		
<b>PCMCIA</b>	Personal Computer Memory Card Industry Association		
<b>POP</b>	Post Office Protocol		
<b>POST</b>	Power On Self Test		
<b>RPC</b>	Remote Procedure Call		
<b>SMTP</b>	Simple Mail Transfer Protocol		



---

## 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 <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
```

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 Web Site 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](mailto: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.

---

### Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (<http://www.redbooks.ibm.com/redpieces.html>). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

---

## 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:

	<b>IBMMAIL</b>	<b>Internet</b>
In United States	usib6fpl at ibmmail	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 Allerød Denmark
--	--	--

- **Fax** – send orders to:

United States (toll free)	1-800-445-9269
Canada	1-800-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States) or (+1) 408 256 5422 (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](mailto:softwareshop@vnet.ibm.com)

- **On the World Wide Web**

Redbooks Web Site	<a href="http://www.redbooks.ibm.com">http://www.redbooks.ibm.com</a>
IBM Direct Publications Catalog	<a href="http://www.elink.ibm.link.ibm.com/pbl/pbl">http://www.elink.ibm.link.ibm.com/pbl/pbl</a>

- **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](mailto:announce@webster.ibm.link.ibm.com) with the keyword `subscribe` in the body of the note (leave the subject line blank).

---

### Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (<http://www.redbooks.ibm.com/redpieces.html>). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

## 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.**



# Index

-- parameter of icacInt 289

## Symbols

\$(PASSWORD) variable 289  
\$(USER) variable 289  
%client% variable 300  
%clientname% 288  
%display% variable 300  
%server% variable 300  
%systemroot% 314  
%username% 312

## Numerics

127.0.0.1 148  
128-bit version - NC Navigator 32  
3270 159  
3270 Full-Screen Example 217  
3270 light pen emulation 160  
3270 Menu Item 152  
3270 Sessions to AutoStart 153  
3270 terminal 215  
3489 emulation - 5250 159  
5250 159

## A

access - UIS 68  
access control 372  
access control list - printing 243  
Activate license 64  
activation code 64  
actlogin 60, 115  
Add Primary Domain 209  
Add/Remove Programs 327  
Adding users to eSuite 256  
additional products 23  
Address Records 200  
Adjust to local time 169  
Administration - Centralized 104  
Administration - DHCP 192  
Administration - ICA 64  
Administrator - eSuite 254  
ALS Groups UIS 68  
Alt-F4 292  
Anyprint 164  
Application compatibility issues 306  
Application Installation Scripts 308, 342  
Application Language 265  
Application notes 354  
Application Server - What is 109  
Apply Button - Console Panels 129  
Architecture - Network Station 12  
A-Records 200  
ASCII data streams 242  
authentication server 59  
Authentication Server - what is 108

AUTHENTICATION\_HOST variable 59  
authserv parameter - login 60  
automated install 55  
Automatically update DDNS A record 206  
Automatically update PTR records 207  
autorun.exe 22  
Autostarting an Application 153

## B

Backup Domain Controller 35  
base code server 57  
batch install 55  
benefits - DHCP server 106  
bookmarks - migration 163  
Boot File parameter - Setup 141  
Boot Monitor 13  
Boot Parameters - Setup 140  
Boot Phases 12  
Boot Sequence of Event 14  
Boot Server - what is 107  
Boot Server install 57  
Boot Using DHCP 145  
Boot Using NVRAM 139  
BOOTHOST variable 59  
Booting - Peer 6  
BOOTP server 106  
boot-tcpip-desired-server 195  
Browse printer 242  
browser 159

## C

calibrate - touchscreen 4  
CD contents 19  
CDE 132  
CD-ROM 19  
Centralized Administration 104  
change 327  
Change User Command  
    change user 307  
    change user /execute 307, 327  
    change user /install 53, 307  
    change user /query 330  
    format 325  
characters - DBCS 242  
Chooser Application - ICA 289  
Citrix 23  
Class - DHCP 185  
class name 156  
Classes - DHCP - IBM Network Station 191  
classpath 156  
Client - DHCP 185  
Client Connection Manager 284  
Client hardware type 190  
Client ID 190  
client licenses - X11 66  
CLIENTNAME variable 288  
close a session - Alt-F4 292

- code - how to obtain 19
- colors parameter 295
- command
  - dadmin 192
  - icacInt 288
  - rsh 293
  - term 162
  - UN 388
  - UP 388
  - wincenter 294
  - x11 293
- command execution - remote 376
- Commands - list 377
- compatibility entries 51
- compatibility flags 329, 346
- Components - network station 13
- compressed kernel 143
- config-console-display-password 374
- config-console-enforce-password-locally 374
- config-enforce-passwords-locally 374
- config-pref-enforce-passwords-locally 375
- config-pref-read-only-password 375
- config-pref-read-write-password 375
- config-read-only-password 375
- config-read-write-password 375
- Configuration 42
  - DHCP 183
  - NFS 171
  - printers 243
  - remote printers 245
  - TFTP 165
  - time server 169
  - UIS 67
- configuration file - Lotus Go Domino server 43
- Configuration host IP Address 140
- Configuration Parameters and DHCP Options 117
- configuration password 374
- Configuring the IBM Network Station 137
- Connect to New Unit 130
- Connection Manager. 284
- Connections 377
- console 370
- Console Access 374
- Control Key Sequences 417
- conversion - DBCS 242
- Copy Key Name - registry 351
- Copy/Cut/Paste - emulators 159
- C-Series card 6
- Ctl-Alt-Break 286
- Customize WorkPlace - eSuite 258
- Customizing eSuite Applications 257

## D

- dadmin command 192
- data stream - ASCII 242
- data streams 245
- DBCS conversion 242
- DDNS
  - configuration 202
  - Logging and tracing 211

- Server Administrator 208
- What is? 199
- default browser 25
- Default DHCP Configuration File 185
- Defaults button - Console panels 129
- defaults.r2 82
- Desktop
  - sample - eSuite 260
  - Shortcut - NSM 39
- desktop
  - settings 250
  - shortcut 25
- DHCP
  - Classes - IBM Network Station 191
  - IP Addressing Order 146
  - option 12 196
  - Options 115
  - Options for Separate Servers 116
  - record 181
  - server - benefits 106
  - Server - What is 106
  - Server Administration 191
  - server installation 29
  - server log file 395
  - server parameters 186
  - server reinitialization 192
- DHCP Options 181
- DHCP vs NVRAM 194
- DHCPACK 179
- DHCPDECLINE 179
- DHCPDISCOVER 178
- DHCPOFFER 178
- DHCPREQUEST 178
- dhcpsd.cfg 185
- Diag port 365
- diag-access-control-enabled 375
- Diagnostic Access 375
- Dialog - print 241
- Differences with release 2 install 20
- Directories
  - after uninstall 54
  - eNetwork On-Demand Server 52
  - NFS 172
  - on server 118
  - size after uninstall 54
  - Structure 50
- directory path - exported 118
- Disable registry mapping 348
- Disk Space Requirements 22
- display all parameters 385
- display parameter 294, 295
- DNS - configuring 249
- DNS - What is? 199
- Documentation
  - DHCP 193
  - eNetwork On-Demand Server 47, 193
  - MetaFrame 65
  - on-line 46
  - UIS 69
- domain - parameter of icacInt 289



- Domain Name Server 249
- download file sequence 234
- download web site 19
- D-series card 6
- dual server migration 73
- Dual Server Migration Example 77
- dual server migration example 77
- DUMP File Upload 388
- dynamic domain type 209

## E

- ECL option - emulators 161
- Editing
  - INI files 350
  - NFS directories 172
  - Registry Entries 350
- elements of migration 75
- emulators 159
- Emulators - what's new 159
- encoding kiosks.nsl 218
- eNetwork On-Demand
  - directories 52
  - server install 30
  - Server installation 30
  - servers 165
- Environment Variable - eSuite 252
- eSuite 247
  - desktop 250
  - environment variable 248
  - Main Administrator Configuration Panel 256
  - NT Service 248
  - proxy configuration 257
  - sample desktop 260
  - web browser 257
  - WorkPlace Administrator 254
- Event Viewer 370
- Events filter 372
- ewadmin command 254
- exec-access-control-enabled 376
- exec-access-control-list 373
- exec-disabled-commands 379
- exec-startup-command 60
- expired password 144
- exported directory path 118
- EXPORTS File - sample 121

## F

- fax size - 5250 159
- File Manager Password 375
- File Problems 310
- File Server - what is 109
- file service table 118
- file service table - displaying 121
- File Service Table - Sample 120
- Filter events 372
- First Boot Host IP Address 140
- First Configuration Directory 142
- flags - compatibility 329
- Flash Boot support 6

- flash card management 7
- flash memory card 6
- fonts - DBCS 242
- FTP 163
- full-screen solution example 217

## G

- Gateway IP Address 140
- GDDM graphics 159
- geometry parameter 296
- get all 385
- GetPrivateProfileString 328
- GetWindowsDirectory 326, 328
- Global options 185
- GMT offset 170
- GMT time 169
- GOPHER 163
- group - default settings 254
- group - NSM 253
- group - NT 253
- group - NT - creating 250
- Group Defaults 151

## H

- HACL 161
- hardware components - Network Station 9
- HLLAPI 161
- HOD 161
- home directory 108
  - creating 311
  - What is 311
- home drive
  - home drives 308
  - what is? 314
- home server 108
- Host Access Class Library 161
- hosts.nsm - sample file 204
- Hot Spot highlighting 160
- HTML 3.2 163
- httpd.cnf 42
- Hydra 277, 281

## I

- IBM Network Station browser 32
- IBM Network Station Manager 147
- IBMNSM class 191
- ICA Administration 64
- ICA Chooser Application 289
- ICA client 278, 287
- ICA client - Java 279
- ica-chooser-entries parameter 290
- icaclnt command 288
- ica-enable-chooser-editing parameter 291
- ICAUI command 290
- IIS 4.0 44
- initial file download 234
- Input Locales 267
- Input Method - Japanese language 274

## Install

- MetaFrame 62
- Terminal Server Edition 62

## install

- automated 55
  - Batch Mode 55
  - boot server only 57
  - DHCP server 29
  - Dialog Language 264
  - directories 50
  - eNetwork On-Demand Server 30
  - Language 263
  - language 22
  - Lotus Domino Go Webserver 25
  - Migration Selection 29
  - NC Navigator 31
  - NC Navigator Selection 31
  - Netscape Navigator 24
  - network station 137
  - response file 55
  - UIS 66
  - web server entries 42
  - Windows Terminal Server Edition 53
- Install Type Registry Entry 58
- installed products 34
- introduction - network station 7
- IP Address - network station 139
- IP Configuration of a Typical PC 195
- IP Configuration of an IBM Network Station 195
- IP host name 196
- IP routing table 384

## J

- Japanese Language Input Method 274
- Java 248
- Java - verbose option 393
- Java - What's new 164
- Java Applet - starting 155
- Java Application - starting 156
- Java support 159
- JavaScript 1.1 163
- JDK 1.1.5 - eSuite 248
- JIT 164
- JRE 164

## K

- kernel - compressed 143
- Kernel Environment Language 272
- key - shortcuts 417
- key combinations 417
- Key Sequences 417
- keyboard language 270
- Keyboard remapping 160
- Keyboard Settings 270
- keypads - emulators 159
- kiosk - web site for instructions 215
- kiosk mode - security considerations 219
- kiosk userid 217
- kiosks.nsl 215, 218

## L

- language - keyboard 270
- Language Settings 273
- lb parameter of icacInt 289
- Licensing - MetaFrame 63
- light pen emulation - 3270 160
- Limitations - Networking Applications 350
- LiveConnect 164
- Load Balancing 103
- load balancing - ICA parameter 289
- local file system 6
- local mount point 118
- local parallel printer 242
- Local Program Menu Item 154
- local serial printer 242
- local time 169
- locale - default system 266
- Locales - Input 267
- Lock password 124
- Lock Screen 123
- Log File - time server 171
- Log Out 123
- Logging
  - DDNS 211
  - Lotus GO 394
  - NFS 174
  - TFTP 167
  - time server 170
- Logging On 143
- LOGIN 378
- Login Chooser - X11 connection 298
- login panel - suppressing 215
- Login Panel Language 271
- Login Screen 144
- login server 108
- login-default-host 134
- logon screen 143
- Logon Scripts 308
- loopback address 148
- Lotus Domino Go Webserve
  - installation 25
- Lotus Domino Go Webserver
  - configuration file 42
  - default main page 48
  - error log 41
  - Logging/Reporting 394
  - reference documents 50
  - restart 43
  - starting 40
- Lotus eSuite WorkPlace 247
- Lotus eSuite Workplace Registry 248
- Lotus SmartSuite 97 333
- LPR capabilities 240
- LPR/LPD streaming 239

## M

- MAM 355
- Memory 377
- menu bar 123

- Message Log 363
- Messages - java 393
- MetaFrame 62, 281
  - applications 63
  - Documentation 65
  - installation 62
  - Licensing 63
  - Tools 63
- migrating user preference files 29
- Migration
  - overview 71
  - selection 29
- migration
  - directories 78
  - elements 75
  - instructions 71
  - methods 72
- models of Network Stations 10
- monitor resolution 139
- monochrome image printing - 5250 159
- multiple DHCP servers 194, 198
- Multiple Serial Port Adapter 4
- Multi-User Application Manager 355

## N

- name - parameter of icacnt 288
- National Language Support 263
- Native Applications - Network Station 11
- NC Navigator - what's new 163
- NC Navigator environment variable 32
- NC Navigator installation 31
- NCD 23
- Netscape Navigator installation 24
- Network Parameters -Setup utility 139
- Networking File System (NFS) Serve 171
- NFS 165
  - boot directory 141
  - Configuration 171
  - directories 172
  - Logging/tracing 174
  - Order 141
  - security 172
  - Users 173
- NMSUser group 148
- NNTP 163
- NS3270 378
- NS5250 378
- NSLOOKUP 210
- NSM Typical Configuration Examples 152
- NSMAdmin 36, 54
- NSMAdmin group 148
- nsmkiosk.exe 218
- nsmmigr.exe utility 76, 79, 90, 94
- NSMNFS\_USER 173
- NSMUser 36, 54
- nsreboot utility 392
- NT security and NFS 172
- NT services 35
- NTNSMRR2.EXE utility 75
- ntnsmver tool 393
- ntuser.dat 309, 320
- NVRAM 13
- NVRAM Reset 390
- NVRAM vs DHCP 194

## O

- object
  - system global 311
  - user global 311
- Object Problems 311
- offset - time 169
- OIA 159
- on-line documentation - DHCP 193
- on-line Help 46
- Options - DHCP 181

## P

- parallel printer 242
- parameters - get all 385
- Password
  - administrator 375
- password 144, 390
  - Administrator 375
  - configuration 374
  - console 374
  - console access 374
  - encoded 375
  - file manager 375
  - global unit 375
  - screen lock 375
- password - lock screen 124
- password - parameter of icacnt 289
- Password Change Panel 144
- PCMCIA - Series 1000 7
- PCMCIA adapter 6
- Peer Booting 6
- permanent IP address 196
- permissions 313
- physical installation 137
- PING 370
- playback files 159
- Plug-ins 164
- Policies 356
- POP3 163
- pop-up - emulators 159
- port
  - parallel 242
  - serial 242
- port 5998 365
- POST 137
- PREF 378
- pref-xserver-current-pointing-device 4
- prerequisites 20, 21
- presentation space - emulators 161
- primary domain 209
- Primary Domain Controller 35
- print
  - API 241
  - buffer sizes 243

- Capabilities Overview 240
- dialog 241
- server - what is 109
- streaming mode 243
- printer
  - drivers 245
  - list 242
  - queues 245
  - selector 241
- printers - remote 242
- Printers task 243
- Printing 239
- printing
  - access control list 243
  - API 241
  - buffer sizes 243
  - Configuration 243
  - data conversion 242
  - history 239
  - LPD capabilities 240
  - LPR capabilities 240
  - port 242
  - Release 3 Print Support 239
  - streaming 239
- prodbase 51
- Programmable Read Only Memory 13
- PROM 13
- Properties - ICA Chooser 291
- Proxies 163
- proxy configuration - eSuite 257
- PTR record 202

## Q

- QUICKSETUP 378

## R

- RAM 13
- rdisk.exe 351
- RDP 281
- Read from NVRAM 130
- reboot - remote 392
- Rebooting remotely 392
- Record/Playback 159
- Recording an install 55
- refresh 38
- regedit 351
- regedt32 351
- regini command 343
- Regional Settings 266
- Registry - eSuite 248
- Registry editor 351
- Registry Settings Problems 309
- re-initialize DHCP server 192
- Re-Installation 38
- Release 2 Boot Parameters 81
- Release 3.02 3
- remote
  - command execution 376
  - mount point 118

- printers 242
- Program Menu Item 153
- Remote Desktop Protocol 281
- Remote Desktop Protocol client 282
- Remote reboot 392
- Repair utility 351
- Reporting Lotus Go 394
- Resetting NVRAM 390
- resolution - display session - RDP 283
- resolution parameter 294
- response file 55
  - Changing the Install Drive 57
- Restart Button - Console panels 129
- Restore Defaults 130
- retargeting 71
- retargeting - general procedure 81
- Retargeting - NVRAM 80
- Return username 348
- Reverse Address 211
- Roam button 145
- Roaming 104
- routing table 384
- RSH 377
- RSH %clientname% 288
- RSH command 293
- rule line - 3270 159

## S

- sample DHCP record 181
- Sample Installation 22
- Sample Response File 56
- Save to File 130
- Save to NVRAM 130
- Screen Lock Password 375
- Second Boot Host IP Address 140
- second configuration directory 142
- security considerations - kiosk mode 219
- security log 372
- Select Printer 242
- Select User's Group 253
- Selector - printer 241
- Separate Servers - Objectives 102
- sequence of download files 234
- Sequences - key 417
- Serial Port Adapter - multiple 4
- serial printer 242
- SERIALD 241
- serial-interfaces-table 4, 5
- Server Components 17
- Server Directorie 118
- Server Options Pack 317
- Server Software 16
- Server Types - Definitions 106
- Service Information Tool 393
- Set Language Parameters 269
- set term-default-hosts 133
- SETUP 378
- Setup Tasks list 149
- setup utility 137
- Setup Utility Panel - Main 138

- setup.exe 57
- setup.exe /as 60
- setup.exe /asf 61
- setup.exe /bs 58
- setup.iss response file 55
- shared directory 314, 315
- shared drive - creating 315
- Shortcut - NSM desktop 39
- SHOW 377
- Show/Hide 123
- single server migration 72
- Single Server Migration Example 86
- Size of Installed Directories 22
- SmartSuite 97 333
- SMTP 163
- spooling 245
- Stand Alone Server attached to a domain 35
- Startup Language 268
- static IP address 177
- static name server 199
- Statistics 125
- STATS 377
- status line - emulator 159
- status panel - Lotus Domino Go 41
- streaming mode 243
- Subnet - DHCP 185
- SUBSTITUTE command 314
- switching input locales 267
- Synchronize user INI file 348
- SYSEDIT 350
- System Defaults 151
- system global object 311
- system locale 266

## T

- TCP/IP address 125
- tcpip-dns-default-domain 196
- tcpip-name-servers 196
- TELNET 365, 367, 378
- telnet session - local 154
- telnet session from browser 132, 160
- Templates 355
- TERM 378
- term Command 162
- term-default-host 133
- Terminal Configuration Server - what is 107
- Terminal Emulator 161
- Terminal Menu Item 155
- Terminal Server Client Creator. 282
- Terminal Server Edition. 281
- Terminal Server Home Directory 318
- TEST 377
- Test Network 370
- TFTP 165
  - boot directory 141
  - Configuration 165
  - Tracing and Logging 167
- Third Boot Host IP Address 140
- Time Server Configuration 169
- Time Server Log File 171

- Time Server Logging/Tracing 170
- Time Zone 251
- time-offset-from-gmt 170
- time-server 169
- title - parameter of icacInt 288
- tn3270 launch from browser 160
- TN3270E 159
- token-ring address 125
- Top/Bottom 123
- Touch Screen Support 3
- Tracing
  - DDNS 211
  - NFS 174
  - TFTP 167
  - time server 170
- Trivial File Transfer Protocol (TFTP) Server 165
- Types of Servers - Definitions 106
- TZ 251

## U

- UIS
  - Applications 67
  - Configuration 67
  - Documentation 69
  - Installation 66
  - licensed connection 197
- UN command 388
- uninstalling 53
  - eNetwork On-Demand Server 53
  - IBM Intermediate Support Driver 53
  - IBM Network Station Manager 53
  - Lotus Domino Go Webserver 53
  - NC Navigator 53
  - remaining files 54
- Unit Global Password 375
- unit name 234
- unit-administrative-status 393
- unit-global-password 376
- unit-initial-locale 272
- unit-query-for-name-at-boot = tcpip 234
- Unix Integration Services (UIS) 66, 197
- unlisted client 177
- unlisted client support 187
- UP command 388
- upload dump file 388
- user configuration server 108
- User Defaults 152
- User Editable Files 238
- user global object 311
- User Logon Scripts 308
- User Profile 316
  - copying 321
  - creating 320
  - local 323
  - mandatory 324
  - Permitted to use 322
  - roaming 323
  - User Profile Path 320
- userbase 51
- username - parameter of icacInt 289

- Using DHCP with IBM Network Stations 194
- Using Multiple DHCP Servers 198
- Using NCD's Unix Integration Services (UIS) 293
- Using X11 with DHCP 197

## V

- verbose 138
- verbose option 143, 363
- verbose option in java 393
- version 377
- View Boot Parameters 138
- View Network Parameters 138
- virtual directory - IIS 4.0 44
- VT320 161

## W

- wcprsh command 300
- web server entries 42
- web site - full screen solutions 215
- what is
  - application server 109
  - authentication server 108
  - boot server 107
  - DHCP server 106
  - file server 109
  - print server 109
  - terminal configuration server 107
  - WinCenter 280
  - WinFrame 279
- What is - flash memory 6
- What is - IBM Network Station 8
- What is - multiple serial adapter 4
- What is - touchscreen 3
- What needs migrating 75
- wildcards 218
- WinCenter 277, 355
- WinCenter - what is? 280
- wincenter command 294, 295
- WinCenter Connect - what is? 280
- Windows Applications Server 277
- Windows NT Regional Settings 266
- Windows Subdirectory 313
- Windows Terminal Server Edition 53, 277
- WinFrame 277
- WinFrame - What is? 279
- Winframe Server Options Pack 317
- WM command 378
- WorkPlace Administrator 254
- Workstation Defaults 151
- WritePrivateProfileString 326
- WTS 281

## X

- X Server Access 373
- X11 command 293
- X11 Command - Using 294
- X11 Command Options 294
- X11 Connections 293

- X11 protocol 280
- X11 protocol - enabling - UIS 69
- X-server 278
- xserver-access-control-enabled 374
- xserver-access-control-list 374
- xserver-initial-x-resources 379
- xserver-input-extension-device 4
- xserver-retain-x-settings 4
- X-station 280

---

## ITSO Redbook Evaluation

IBM Network Station Manager Release 3 Guide for Windows NT  
SG24-5221-00

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

- Use the online evaluation form found at <http://www.redbooks.ibm.com>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to [redbook@us.ibm.com](mailto:redbook@us.ibm.com)

**Please rate your overall satisfaction** with this book using the scale:  
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction \_\_\_\_\_

**Please answer the following questions:**

Was this redbook published in time for your needs? Yes\_\_\_ No\_\_\_

If no, please explain:

---

---

---

---

What other redbooks would you like to see published?

---

---

---

**Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)**

---

---

---

---

---

**SG24-5221-00**

**Printed in the U.S.A.**

