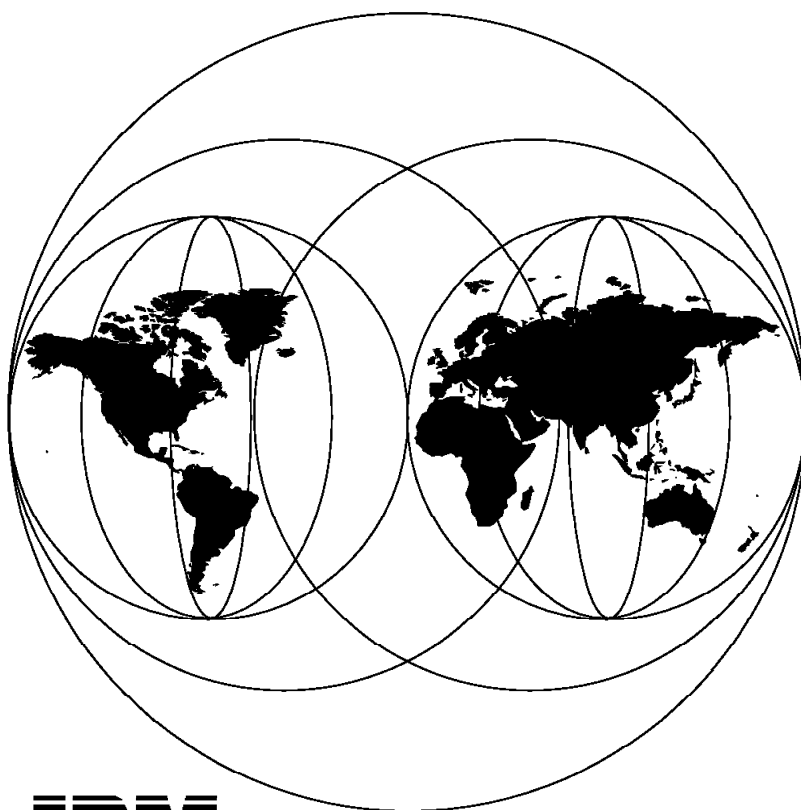


# **IBM Network Station Guide for Windows NT**

November 1997



**International Technical Support Organization  
Raleigh Center**





International Technical Support Organization

SG24-2127-00

## **IBM Network Station Guide for Windows NT**

November 1997

**Take Note!**

Before using this information and the product it supports, be sure to read the general information in Appendix E, "Special Notices" on page 221.

**First Edition (November 1997)**

This edition applies to the IBM Network Station Manager for Windows NT Server 4.0, Product No. 5639-B62.

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 1997. 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> . . . . .	vii
<b>Tables</b> . . . . .	xi
<b>Preface</b> . . . . .	xiii
The Team That Wrote This Redbook . . . . .	xiii
Comments Welcome . . . . .	xiv
<b>Chapter 1. Introduction</b> . . . . .	1
<b>Chapter 2. Overview</b> . . . . .	3
2.1 What Is an IBM Network Station? . . . . .	3
2.2 Role of the Boot Server . . . . .	3
2.3 IBM Network Station Components . . . . .	5
2.4 The Boot Process . . . . .	5
2.5 Using DHCP . . . . .	6
2.6 Server Components . . . . .	7
2.7 The IBM Network Station Manager . . . . .	7
2.8 What Is WinCenter? . . . . .	8
2.8.1 Can a WinCenter Server also Be a Boot Server for Network Stations? . . . . .	9
2.8.2 What about Using the IBM Network Station Manager on a WinCenter Server? . . . . .	9
2.8.3 What about Plans for WinCenter on a Windows NT 4.0 Platform? . . . . .	9
2.9 Summary . . . . .	9
<b>Chapter 3. Windows NT Server Installation</b> . . . . .	11
3.1 Prerequisites . . . . .	11
3.2 Performing a "Clean" Installation of Windows NT Server 4.0 . . . . .	12
3.3 Downloading Products from the World Wide Web . . . . .	13
3.3.1 Create a Target Download Directory . . . . .	13
3.3.2 Download Necessary Software Products from the World Wide Web . . . . .	13
3.4 Installing the Java Development Kit . . . . .	17
3.5 Installing the IBM DHCP Protocol Driver . . . . .	18
3.6 Installing the IBM Network Station Manager . . . . .	18
3.7 Installing the IBM Network Station Browser . . . . .	19
3.8 Installing the NAVIO Browser . . . . .	19
3.9 Installing IBM TCP/IP Services . . . . .	20
3.10 Creating Network Station User Accounts . . . . .	22
3.11 Starting the IBM Network Station Manager for Windows NT Server 4.0 . . . . .	23
3.12 Installation Results . . . . .	25
3.13 Uninstalling the Product Components . . . . .	29
3.14 Disabling and Removing the IBM DHCP Driver . . . . .	31
<b>Chapter 4. IBM Network Station Installation and Configuration</b> . . . . .	33
4.1 Physical Installation . . . . .	33
4.2 Setup/Configuration Methods . . . . .	33
4.3 Configuration of the Network Station . . . . .	33
4.3.1 Setting Up for a Boot from NVRAM . . . . .	35
4.3.2 Logging On . . . . .	38
4.3.3 Setting Up for a Boot Using DHCP . . . . .	38

<b>Chapter 5. IBM Network Station Customization Files</b>	41
5.1 Configuration Files	41
5.1.1 Global Level Configuration Files	41
5.1.2 Workstation Level Configuration Files	44
5.1.3 User Level Configuration Files	45
5.1.4 The Three Levels of Configuration Files	46
5.1.5 Configuration Files Used at Boot and Log Out - Read Order	46
5.2 Startup Files	48
5.2.1 Startup Files Used at Login - Read Order	48
5.2.2 The Menu Bar Items and Startup Programs	50
5.3 Application Preference Files	52
 <b>Chapter 6. Understanding Dynamic Host Configuration Protocol (DHCP)</b>	 55
6.1 Booting the Network Station	55
6.2 Network Protocols	55
6.3 DHCP vs BOOTP	56
6.3.1 Dynamic IP Address Allocation	56
6.3.2 Helpful Documentation	57
6.4 Boot Sequence - How Information Is Obtained via DHCP	58
6.5 The DHCP Server Configuration Program	60
6.5.1 Configuring Your Environment	61
6.6 A Sample DHCP Configuration	64
6.7 Server Parameters	65
6.7.1 Global Definitions	66
6.7.2 Subnet Definition	69
6.7.3 Client Definition	70
6.7.4 Problem Solving/Logging	75
6.8 Administration of a Running DHCP Server	76
 <b>Chapter 7. IBM Network Station Manager</b>	 79
7.1 Hardware Settings	81
7.1.1 Files Created by NSM for Hardware Settings	86
7.2 Desktop Manager Setting	87
7.2.1 Files Created by NSM for Desktop Manager Settings	89
 <b>Chapter 8. Network Station Applications and User Services</b>	 91
8.1 The Menu Bar	91
8.1.1 Creating a New Menu Bar Item	93
8.1.2 Autostarting an Application	93
8.1.3 MENU Item for Remote Applications (X Session)	94
8.1.4 Starting a Java Applet	94
8.1.5 Starting a Java Application	95
8.2 The Network Station Console	96
8.2.1 Statistics	96
8.2.2 Setup	99
8.2.3 Utilities	102
8.2.4 Window Manager	103
8.2.5 Terminals	103
8.2.6 Login	104
8.2.7 Console	104
8.2.8 Messages	104
 <b>Chapter 9. Network Station Emulators</b>	 105
9.1 Configuring the IBM Network Station 3270 Emulator using NSM	105
9.1.1 Files Created by NSM for 3270 Settings	107

9.2 Starting the IBM Network Station Emulators . . . . .	108
9.2.1 Files Created by NSM for Startup Terminal Emulators . . . . .	111
9.3 Using the IBM Network Station 3270 Emulator . . . . .	112
9.3.1 Copy and Paste . . . . .	113
9.4 Configuring the IBM Network Station 5250 Emulator . . . . .	113
9.4.1 Files Created by NSM for 5250 Emulator Settings . . . . .	116
9.5 Using the IBM Network Station 5250 Emulator . . . . .	117
9.5.1 Copy and Paste . . . . .	118
<b>Chapter 10. Network Station Browsers . . . . .</b>	<b>119</b>
10.1 Configuring for Using the Browsers . . . . .	119
10.1.1 Files Created by NSM for Network Settings . . . . .	123
10.2 Configuring the IBM Network Station Browser Using the NSM . . . . .	124
10.2.1 Files Created by NSM for IBM Network Station Browser Settings . . . . .	126
10.3 The Java Applet Viewer . . . . .	127
10.3.1 Configuring the Java Applet Viewer . . . . .	128
10.3.2 Files Created by NSM for Java Applet Viewer Setting . . . . .	129
10.4 Starting the IBM Network Station Browser . . . . .	129
10.4.1 Files Created by NSM for the Browsers Startup Settings . . . . .	131
10.5 Using the IBM Network Station Browser . . . . .	132
10.5.1 Hot List . . . . .	135
10.5.2 Saving Files . . . . .	135
10.5.3 Starting Multiple Network Station Browser Windows . . . . .	135
10.5.4 Files Created by the IBM Network Station Browser Operations . . . . .	135
10.6 Configuring the Navio NC Navigator in NSM . . . . .	137
10.6.1 Files Created by NSM for Navio NC Navigator Settings . . . . .	139
10.7 Using the NAVIO NC Navigator . . . . .	140
10.7.1 Setting User Preferences . . . . .	140
10.7.2 Bookmarks . . . . .	142
10.7.3 Saving Files . . . . .	142
10.7.4 Starting Multiple Navio NC Navigator Windows . . . . .	142
10.7.5 Files Created from Navio NC Navigator User Settings . . . . .	143
<b>Chapter 11. IBM Network Station and Windows NT Security . . . . .</b>	<b>147</b>
11.1 Network Station Security . . . . .	147
11.1.1 Setup Utility Panels . . . . .	147
11.1.2 File Service - Local File System . . . . .	149
11.1.3 Access Control . . . . .	151
11.2 Windows NT Server Security . . . . .	153
11.2.1 Directory and File Access . . . . .	153
11.2.2 Network Station Manager Groups . . . . .	157
<b>Chapter 12. Problem Determination - Tools, Tips and Techniques . . . . .</b>	<b>159</b>
12.1 The IBM Network Station Message Log . . . . .	159
12.1.1 On-Screen Messages during the Boot Process . . . . .	159
12.1.2 Messages on the IBM Network Station Console . . . . .	160
12.1.3 Message Log via TELNET from the IBM Network Station . . . . .	161
12.1.4 Message Log from a Remote Host Using TELNET . . . . .	163
12.1.5 Sample Message Log . . . . .	164
12.2 The Network Station Console . . . . .	166
12.3 NT's Event Viewer . . . . .	166
12.4 DHCP Server Log Files . . . . .	169
12.5 Web Server Log Files . . . . .	171
12.6 Windows NT Network Monitor . . . . .	173
12.6.1 Installing the Network Monitor Tool . . . . .	174

12.6.2 Using the Network Monitor Tool . . . . .	175
12.7 Launching Commands from a Remote Host . . . . .	188
12.7.1 Commands . . . . .	189
12.7.2 Help on Commands . . . . .	191
12.8 Using the Config Daemon from a Remote Location . . . . .	193
12.9 Accessing the Setup Panels from Another Network Station . . . . .	196
12.10 Using the Boot Monitor Commands . . . . .	196
12.11 Getting Additional File Diagnostics . . . . .	197
12.12 Uploading Dump Files . . . . .	198
12.12.1 Using TFTP to Upload a DUMP File . . . . .	199
12.12.2 Using NFS to Upload a DUMP File . . . . .	199
12.12.3 Which Method Should You Use for the Upload? . . . . .	200
12.13 Resetting NVRAM Defaults . . . . .	200
12.14 Resetting the IBM Network Station Password . . . . .	200
12.15 Avoiding Reboots . . . . .	201
12.16 Getting Additional Messages with Java . . . . .	202
 <b>Appendix A. Sample Configuration Files . . . . .</b>	 203
 <b>Appendix B. Boot Monitor Commands . . . . .</b>	 213
 <b>Appendix C. Useful Control Key Sequences . . . . .</b>	 215
 <b>Appendix D. Configuration Parameters . . . . .</b>	 217
 <b>Appendix E. Special Notices . . . . .</b>	 221
 <b>Appendix F. Related Publications . . . . .</b>	 223
F.1 International Technical Support Organization Publications . . . . .	223
F.2 Redbooks on CD-ROMs . . . . .	223
 <b>How to Get ITSO Redbooks . . . . .</b>	 225
How IBM Employees Can Get ITSO Redbooks . . . . .	225
How Customers Can Get ITSO Redbooks . . . . .	226
IBM Redbook Order Form . . . . .	227
 <b>Index . . . . .</b>	 229
 <b>ITSO Redbook Evaluation . . . . .</b>	 231



## Figures

1.	The Network Computing Software Distribution Web Site	14
2.	IBM Network Station: PC Server Information	16
3.	System Properties: Updating the PATH Variable	17
4.	IBM Network Station Manager TCP/IP Configuration	20
5.	IBM Network Station Manager TCP/IP Configuration	21
6.	User Manager for Domain	22
7.	IBM Network Station Manager Login Box	23
8.	IBM Network Station Manager	24
9.	IBM Network Station Manager	25
10.	Windows NT Services Installed	26
11.	Web Server Updates	27
12.	Add/Remove Programs	30
13.	Select OK to Remove Selected Application	30
14.	Uninstall Complete Confirmation	31
15.	Microsoft TCP/IP Error	31
16.	Main Network Station SETUP Utility Panel	34
17.	Set Network Parameters - IBM Network Station SETUP Utility	35
18.	Set Boot Parameters - IBM Network Station SETUP Utility	36
19.	IBM Network Station - Kernel Loading Progress Bar	37
20.	Set Network Parameters - IBM Network Station SETUP Utility	39
21.	Configuration Files at Boot and Log Out - Read Order	47
22.	Startup Files at Login - Read Order	49
23.	Log In - Excerpts from Network Station Message Log	50
24.	IBM Level Startup File	51
25.	System Level Startup File	52
26.	User Level Startup File	52
27.	Sample Menu Bar	52
28.	Boot Sequence - How Information Is Obtained via DHCP	60
29.	Launch the Configuration Tool	62
30.	The DHCP Server Configuration GUI	62
31.	Double-Click on the File DHCP.DCF to Load	63
32.	Supplied Sample dhcp.dcf Configuration File	63
33.	Environment Used for Sample DHCP Configuration	64
34.	Server Parameter Miscellaneous Tab - Specify Client Support	66
35.	Modifying the Global Settings	67
36.	The Main View after Configuring the Global Options	68
37.	The Subnet Definition Tab	69
38.	The Main View after Subnet Configuration	70
39.	The Client Definition Tab	71
40.	The Client Definition DHCP Options Tab	72
41.	The Main View after Client Configuration	73
42.	The dhcp.dcf File	74
43.	The DHCP Server Parameters Logging Properties	75
44.	Log File Showing Rejected Client	76
45.	The DADMIN Command - Reinitializing the DHCP Server	77
46.	The Network Station Manager Main Panel	80
47.	The IBM Network Station Manager	82
48.	The IBM Network Station Manager	83
49.	The Network Station Manager Hardware Settings	84
50.	The Desktop Manager - System Default Settings	88
51.	IBM Network Station Console	96

52.	IBM Network Station Console - Version	97
53.	IBM Network Station Console - Memory	97
54.	IBM Network Station Console - X Connections	98
55.	IBM Network Station Console - Statistics	98
56.	IBM Network Station Console - QuickSetUp	99
57.	IBM Network Station Console - Setup Parameters	100
58.	IBM Network Station Console - Setup - File Pull-Down	101
59.	IBM Network Station Console - User Preferences	102
60.	IBM Network Station Console - Test Network	103
61.	IBM Network Station Console - Terminal/Telnet	103
62.	IBM Network Station Console - Login Host Chooser	104
63.	The IBM Network Station Manager	106
64.	The IBM Network Station Manager - Startup menu settings.	109
65.	The IBM Network Station 3270 Emulator	112
66.	The IBM Network Station Manager	114
67.	The Network Station 5250 Emulator	117
68.	The IBM Network Station Manager - Internet Menu	120
69.	The IBM Network Station Manager - Network Default Settings	121
70.	The IBM Network Station Manager - Network Customization	122
71.	The IBM Network Station Manager - User Setting - Network	124
72.	The IBM Network Station Manager - NSB Customization Page	125
73.	A Web Page on the IBM Network Station	127
74.	The IBM Network Station Manager - Java Applet Viewer	128
75.	The IBM Network Station Manager - Startup Programs - Browsers	130
76.	The IBM Network Station Manager Startup - Startup Menu - Browser	131
77.	The IBM Network Station Browser	132
78.	The IBM Network Station Browser - User's Preferences	134
79.	The IBM Network Station Manager - Navio Customization	138
80.	The Navio NC Navigator Home Page	140
81.	The Navio NC Navigator Network Preferences	141
82.	Using the NSM to Set the Network Station Admin Password	148
83.	The TFTP Configuration Screen	154
84.	The /ibmtcpip/etc/exports File - NFS Exported Directories	155
85.	The NFS Configuration Screen	156
86.	IBM Network Station Setup Utility Display - Diagnostic Verbose Option	160
87.	IBM Network Station Console Messages	161
88.	IBM Network Station Console Messages via Diag Port	162
89.	IBM Network Station Console - Options	163
90.	IBM Network Station Console Messages via TELNET 5998	164
91.	Sample Messages in the Message Log	165
92.	NT Event Viewer	167
93.	NT Event Viewer - Details of an Event	168
94.	NT Event Viewer - Specifying a Display Filter	169
95.	DHCP Logging Configuration Panel	170
96.	DHCP Server Sample Message Log	171
97.	MS Internet Service Manager Panel	172
98.	Web Server - Specifying Logging Options	172
99.	Setting Adapter to Pmode	174
100.	Network Monitor Tool Installation	175
101.	Network Monitor Tool - Main Panel while Capturing Data	176
102.	Network Monitor Tool - Capture Filters	177
103.	Network Monitor Tool - Filtering on Addresses	178
104.	Network Monitor Tool - Display Panel	179
105.	Network Monitor Tool - Display Filters	180
106.	Network Monitor Tool - Selecting the DHCP Frames Only	181

107. Network Monitor Tool - Display of DHCP Frames Only . . . . .	182
108. Network Monitor Tool - Displaying Details of Each Frame . . . . .	183
109. Network Monitor Tool - Printing Selected Frames . . . . .	184
110. Network Monitor Tool - Printing Selected Frames-Advanced Options . . . . .	184
111. Network Monitor Tool - Sample Printed Output . . . . .	185
112. Network Monitor Tool - Sample Printed Output . . . . .	186
113. Network Monitor Tool - Sample Printed Output . . . . .	187
114. Network Monitor Tool - Sample Printed Output . . . . .	188
115. Config Daemon Commands for Read-Only . . . . .	194
116. Config Daemon Commands for Read-Write . . . . .	195
117. Connecting to a Remote Station . . . . .	196
118. Boot Monitor Commands . . . . .	197
119. Message Log when File Extended Diagnostics is Enabled . . . . .	198



---

## Tables

1.	Download SW Products from Internet to Your PC . . . . .	16
2.	Configuration Files . . . . .	46
3.	Preference Files . . . . .	53
4.	BOOTP & DHCP Capabilities . . . . .	56
5.	Sample Configuration Values . . . . .	65
6.	Key Sequences to Access the Setup Utility and Boot Monitor Program	149
7.	Key Combinations For Setup Utility and Boot Monitor Program . . . .	215



---

## Preface

This redbook covers what one needs to know to install, configure and operate a Windows NT 4.0 Server to act as a DHCP server, a boot server and an application server for a network of IBM Network Stations.

It helps you understand what the installation process creates, what the configuration files contain, how they are structured and how to modify them, how to configure the IBM TCP/IP services on the boot server, how to use the Network Station Manager program to provide a user friendly configuration interface, how to use the functions and facilities on the network station itself to run applications, how to customize the user's desktop and some tools, tips and techniques which are useful to do problem determination.

### PLEASE NOTE

We have made a conscious effort NOT to repeat information here which is generic to the IBM Network Station and has already been published in other redbooks. Therefore, we have tried to focus ONLY on issues related to the Windows NT platform, whenever possible.

We list, in the Introduction Chapter, the other redbooks and what they contain that can be useful to the reader, in addition to the information provided here. Please refer to these other publications to get additional details on the IBM Network Station.

---

## The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh.

**Claude Bechard** is a Senior Technical Marketing Support Representative at the Systems Management and Networking ITSO Center, Raleigh. His current responsibility is to write and teach IBM classes worldwide on the IBM Network Station. His previous responsibilities, in the last 6 years, had been to support SNA communications products and he produced numerous redbooks on IBM Communications Server products. He is an IBM Canada employee, with 28 years of service with IBM, and holds a degree in Mechanical and Industrial Engineering from the University of Montreal.

**Sarah Spillman** is a software engineer from Rochester, MN. She has been with IBM for three years. She has experience with AIX and AFS as well as with the IBM Network Station. She is currently working on the AS/400 Division Network Station deployment strategy. She holds a Bachelor of Science in Business degree from the University of Minnesota.

**Umberto Scotti** is an Advisory Information Technology Specialist from IBM Italy. He has worked at IBM for 28 years and his area of expertise includes mainly the S/390 networking, client/server and network computing environments.

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

Richard Knox  
IBM Greenock Lab

John Pettigrew  
IBM Greenock Lab

---

## 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 231 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@vnet.ibm.com](mailto:redbook@vnet.ibm.com)



---

## Chapter 1. Introduction

This particular redbook is about the IBM Network Station and its use with a Windows NT-based server.

However, Windows NT is not the only platform that can be used as a boot server for an IBM Network Station; a S/390, an AS/400, or a RS/6000 can also serve as boot servers for the IBM Network Station.

Because of the many environments in which the IBM Network Station can operate, and because of the urgent need for information to be published on each of these different platforms, other redbooks have been created, one for each of the support platforms, which all contain good information about the IBM Network Station and about the specifics of the platform they address.

These other redbooks are:

- SG24-4954-01 - *S/390 - IBM Network Station - Getting Started*
- SG24-2016-00 - *RS/6000 - IBM Network Station - A Companion Guide*
- SG24-2153-00 - *AS/400 - IBM Network Station - Getting Started*

**Note:** Please note that the original S/390 redbook (SG24-4954-00) has been updated and is now SG24-4954-01.

Each of these redbooks cover the topics relative to their own specific platform, such as installation of the boot support code on a S/390, but also information that is generic to the IBM Network Station. This generic information about the IBM Network Station itself applies to all platforms; consequently, there is some duplicated information in these redbooks due to the fact that one must cover a minimum about the Network Station itself when dealing with its use and implementation of S/390 for example.

In this redbook about the Windows NT platform, we tried to avoid duplicating any information that is already available in these other redbooks, as much as possible, and we tried to focus on issues particular to the Windows NT environment.

Therefore, we encourage you to reference these other redbooks for additional information and details on the IBM Network Station itself.

As is characteristic of redbooks in general, you will find that each redbook covers the information in a varied amount of detail as well as with a different perspective, since the authors are different and have different backgrounds. We therefore found that despite minor duplications, the information on the IBM Network Station is of good value and can be useful to you.

In this particular document, we focus on the following:

- The installation of the IBM Network Station support code on the Windows NT 4.0 platform
- How the configuration files are organized on a Windows NT server
- An introduction to the configuration of the IBM DHCP server on Windows NT
- Some of the file and security aspects on Windows NT

- The tools and techniques available on Windows NT and the IBM Network Station to do problem determination

The following is a list of some of the topics that you might find in the other redbooks that are applicable to the Windows NT environment. Of course, some of the examples used are sometimes platform-specific but nevertheless they can give you additional insight into the IBM Network Station.

**Note:** We have indicated the chapter numbers in parentheses, but these might have changed since publication, so please use the Table of Contents of these redbooks for a more accurate pointer to the subject.

- In *S/390 - IBM Network Station - Getting Started*, SG24-4954-01:
  - Introduction to the Network Computing Concepts (Chapter 1)
  - IBM Network Station Positioning (Chapter 2)
  - IBM Network Station Setup (Chapter 5) - Provides a lot of detailed information about the SETUP utility, the default values and the boot monitor commands.
  - IBM Network Station Manager (Chapter 6) - Provides good information on the structure of the configuration files as well.
  - Configuration Parameters (Chapter 9) - Good detailed information on some typical use of configuration parameters.
  - Appendixes information on the Network Computer profile, hardware information, configuration parameters table, and 3270 emulator functions.
- In *RS/6000 - IBM Network Station - A Companion Guide*, SG24-2016:
  - Network Station Initialization and Use (Chapter 2) - Usage examples.
  - Network Station Performance Considerations (Chapter 8) - Initial information on boot performance.
  - Printing (Chapter 9)
  - Problem Determination (Chapter 10)
  - Appendixes - Information on emulators, a browser comparison chart and a network computer comparison chart.
- In *AS/400 - IBM Network Station - Getting Started*, SG24-2153:
  - IBM Network Station Setup (Chapter 4) - Hardware setup information.
  - Using the IBM Network Station (Chapter 6) - Detailed information about the emulators and the Java sample demos.
  - Personalization of the IBM Network Station environment (Chapter 7) - Detailed information on setting up preferences.
  - Appendixes - Good troubleshooting information.

---

## Chapter 2. Overview

As previously mentioned, we try to avoid duplicating information that has already been published; therefore, we will not repeat here the concepts of what a network computer is, what the NC Reference profile is, etc.

However, we do want to spend a few words to try to give an overview, technically speaking, of what the IBM Network Station is and how it operates. This is mainly for the benefit of those who are first getting into this network computer area.

---

### 2.1 What Is an IBM Network Station?

The whole point of a network computer is to give it all the benefits of a personal computer but without one of its major disadvantages, which is the cost and (increasing) complexity of maintenance.

That's why it is easier to think of the IBM Network Station as a Personal Computer with no significant local storage capability, so that all the software components that the IBM Network Station needs to operate reside on a server.

To operate, therefore, an IBM Network Station must get its operating system, its configuration data, its applications and its data from a server. Once it has loaded all these components, the IBM Network Station is somewhat (to a certain extent) independent from the server and can operate independently (dependent on the applications used).

In fact, the server can go down and the IBM Network Station can continue to operate by itself, in most cases; in cases where new applications need to be loaded or data needs to be fetched from the server, then the IBM Network Station may need to wait until the server comes back into operation.

A prime example of this is a local browser, which, once loaded, can allow a user to surf the Internet for hours, even with its boot server being down.

---

### 2.2 Role of the Boot Server

The role of the boot server therefore is to provide the IBM Network Station with the software components it needs to operate.

These major components are:

- An operating system (the kernel)

This is a UNIX-like operating system, approximately 2 MB in size, which is the first file loaded in order to get the IBM Network Station up and running.

- Configuration files

There are half a dozen or so of these files (this is variable) which contain lists of parameters with values that determine how the IBM Network Station is configured.

- Application and user preference files

These are also configuration files, in a sense, but they deal more with the appearance of applications and desktop settings, such as background color, etc.

- Font files and bitmaps files

Various files to provide bitmaps for desktop backgrounds, for example, and to provide fonts for the display of information.

- Startup files

These files also contain some parameters whose settings determine what takes place after the user logs in, that is, which applications get automatically started and what menu items appear on the user menu bar.

- Application modules

Finally, applications get loaded, on demand, as the user requests them.

These applications are:

- A 3270 emulator
- A 5250 emulator
- A network browser
  - The IBM Network Station browser, and/or
  - The Navio Browser
- Java Applets
- Java Applications

Since the IBM Network Station is a real-memory system (no virtual memory and paging), these applications usually only get loaded when they are required.

If there is a fixed set of applications that the user always require, and there is enough memory in the IBM Network Station to accommodate all these applications, they could be all loaded initially, after startup, and always remain loaded.

How often does an IBM Network Station need to boot from its server and download these components? In a normal operational environment, it is likely that the IBM Network Station may not be required to boot for days, weeks and even months, just as long as its power has not been cut off and that software changes have not required it to be refreshed.

The IBM Network Station itself only draws about 7 watts of current, on average, which is probably the equivalent of a night light. Therefore, it is recommend that you do not turn it off at night, but only power off the monitor.

Therefore, when the typical user returns to his workstation every morning, all these components are still loaded and operational. Only applications that get stopped and restarted will require their module(s) to be reloaded.

We will discuss later which components are required on the server to actually download these files to the IBM Network Station.

---

## 2.3 IBM Network Station Components

What are the major components then on the IBM Network Station itself?

The IBM Network Station includes:

- A boot monitor program in programmable read-only memory (PROM)

The PROM contains a boot monitor program whose role it is to provide the minimum set of programming required to contact a server and initiate the download of its operating system. So consider this as a very basic and minimal mini-operating system, permanently resident on the IBM Network Station.

- Some non-volatile random access memory (NVRAM)

There are some parameters settings that need to be conserved across reboots and restarts of the IBM Network Station. These are saved in the non-volatile memory. There are probably somewhere around 80 parameters, out of a total of approximately 600, that can be made to reside in NVRAM.

- Some video memory

This is required to drive the monitor. The choice is 1 or 2 MB.

- Some RAM memory

The minimum is 8 MB and the maximum is 64 MB. This RAM memory is used to contain the kernel operating system, the configuration data, and the application code downloaded from the server.

- A network adapter (token-ring or Ethernet)
- A PCMCIA adapter slot
- The usual display monitor, parallel, serial, mouse and keyboard ports required to hook up the various input/output devices.

---

## 2.4 The Boot Process

How does the IBM Network Station then get initialized?

These are the usual (simplified) steps that are part of the boot process:

- The user powers on the IBM Network Station
- After the usual self-verification, etc., the boot monitor program is given control.
- The boot monitor programs reads its configuration data from the NVRAM; this data has been previously set by an administrator. It usually consists of the IP address of the server, the IP address of the station itself, the default gateway, the network mask (a network station is a TCP/IP host), and the path to the kernel file.

**Note:** In fact, if using DHCP as a boot protocol, most of this data is not even required as it will also be obtained from the network.

- Using this configuration data, the boot monitor program contacts a server and initiates a download of the kernel file, using the TFTP protocol (default in an NT server environment).
- Once the kernel is loaded, it is given control and it initiates further TFTP request to get the configuration files, the preference files, bitmaps and fonts.

- A login client application is then given control; it displays a logon screen to the IBM Network Station user and contacts the login server application on the server to authenticate the user.
- Once authenticated, the kernel then initiates the download of user preference files (now that it knows which user is the current user) and the download of startup files.

**Note:** In the NT environment, all of the preceding downloads were done using the TFTP protocol, because it is a simpler protocol and is well suited to the read-only nature of these downloads; after the user logs in, most transfer activity taking place uses the NFS protocol, which is better suited to the read/write activity taking place from this point on.

- The desktop is then built according to user preferences, the menu bar is built and applications are started if requested.
- From this point on, the boot process is complete and the IBM Network Station is fully operational. All the user needs to do is to start using the applications that are available to him from the desktop.

---

## 2.5 Using DHCP

As mentioned above, when the boot monitor program is given control, it has the option (configurable) of using the data configured in NVRAM to find out what its own IP address is, what the address of its server is, what default gateway to use, etc.

This is called the NVRAM method of booting and requires that an administrator has previously entered this data on the IBM Network Station itself. This is fine in an environment where there is a relatively small number of stations.

However, for large networks, this is probably not adequate and we need a more flexible method of centrally controlling the information that would normally be entered in NVRAM.

The method to use then is the Dynamic Host Configuration Protocol (DHCP), which allows an IBM Network Station to retrieve its initial boot configuration data from the network.

This requires that a DHCP server (it does not have to be the same server as the boot server) be available to manage this configuration data. This is generally how this (simplified) process works:

- The IBM Network Station is powered on
- The boot monitor program is given control
- It reads its NVRAM configuration data, which specifies that it should use the DHCP method of booting
- The boot monitor program then issues a broadcast frame, called a DHCPDISCOVER frame, asking for its configuration data. The only information present in that request is the MAC address of the station initiating the request.
- The DHCP server, on receipt of the request, checks the MAC address of the originating station against its configuration data, and, provided it is a valid station, sends back to the station the data it needs, that is, the IP address

that the station should use, the IP address of the server it should boot from, its default gateway, its network mask and the path to the kernel file.

- At this point, the boot monitor program basically has the same data that it had previously, using the NVRAM method, read from the NVRAM. The processing is then the same, that is, it contacts the boot server and starts downloading the kernel, etc.

The main advantage of this method (DHCP) over NVRAM is that the administrator did not have to manually configure each network station. Also, each IBM Network Station is not restricted to using always the same IP address, but this address can be dynamically changed as part of the DHCP boot process to fit the needs of the organization.

DHCP is the recommended method of managing IBM Network Stations.

---

## 2.6 Server Components

So what do we need on a Windows NT 4.0 server to support a network of IBM Network Stations?

The major components are listed below. See Chapter 3, “Windows NT Server Installation” on page 11 for more details on the prerequisites.

- A base Windows NT 4.0 server, including the Microsoft Web server component.
- The Java Development Kit, available from the Web.
- The IBM Network Station Manager application. This is a Web browser GUI application that allows an administrator to manage the configuration files required for a network of IBM Network Stations.
- Network Station browsers; these are browser applications that execute on the IBM Network Station.
- IBM TCP/IP services. These are the TFTP and NFS services that are required to provide download support to the IBM Network Stations, the DHCP server and GUI configuration application, and the IBM Network Station login server, to authenticate Network Station users.

**Note:** The DHCP server is a replacement for the Microsoft-supplied DHCP service which is part of the NT server. The reason is that the IBM-supplied DHCP service contains functions not included in the Microsoft-supplied version.

---

## 2.7 The IBM Network Station Manager

What exactly is the IBM Network Station Manager and what does it provide?

The IBM Network Station Manager is a Web-based application, which can therefore be operated from any JavaScript-enabled browser, from anywhere on an Intranet or Internet network.

The IBM Network Station Manager application resides on the boot server and is used by an administrator to set the configuration parameters for all IBM Network Stations, for individual IBM Network Stations or for individual users.

Individual users can also use the IBM Network Station Manager to set their own preferences.

The configuration files required to set all the parameters needed by the IBM Network Station to operate properly can become fairly complex; the IBM Network Station Manager helps to mask the complexity and provides a user-friendly configuration tool to make the task of the administrator easier.

Most of the configuration parameters required can be set using the IBM Network Station Manager application. For the few that may not yet be available through the IBM Network Station Manager, the administrator can set them manually by editing the proper configuration files.

---

## 2.8 What Is WinCenter?

It seems that you cannot discuss a network computer topic today without mentioning WinCenter. The reason for this is that it is rare today 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.

The IBM Network Station is not an Intel-based machine that can execute native Windows applications but it is an x-server machine (or it behaves as an x-station) which allows it to execute the actual application (such as a 1-2-3 spreadsheet) on a remote machine and have the input (keyboard) and output (display) redirected to itself.

In order to execute these Windows applications on a remote server, this remote server must therefore have the ability to service multiple users at the same time; this is where the WinCenter product comes in.

The base for the WinCenter product is the Winframe product, from Citrix Inc., which uses Microsoft's Windows NT 3.51 as a base, and gives it a multi-user capability. In other words, if I have a server running the Winframe product, many users can connect into this server and all appear to use the Windows NT desktop as if they were the only user. To connect into the Winframe, the users (clients) use a proprietary protocol called ICA.

WinCenter, which is a product from NCD Inc., uses the Winframe product as a base, and adds to it the capability to support x-clients such as X-stations, network computers and the IBM Network Station. Therefore, the WinCenter product is really what allows an IBM Network Station to connect into a multi-user NT 3.51 server and to execute Windows applications just as if they were executing on the IBM Network Station itself.

Note that this is currently available only for the Windows NT 3.51 platform.

Therefore, as far as the IBM Network Station is concerned, a WinCenter server is an application server, and *not* a boot server.

In other words, the IBM Network Station still boots from a Windows NT 4.0 boot server (or any other boot server such as an AS/400, a RS/6000 or a S/390), and, once it is operational, it opens up an X-session with a WinCenter server in order to execute Windows applications on the WinCenter server machine.



### **2.8.1 Can a WinCenter Server also Be a Boot Server for Network Stations?**

The WinCenter product itself does not provide the boot services required by a network station. That is, it does not have a Network Station kernel or Network Station configuration files that it can download to the Network Station.

However, there is code available from IBM, at the same download site where the IBM Network Station support code for Windows NT 4.0 is available, which allows a WinCenter server to be a boot server for Network Stations.

This code provides the required Network Station kernel and configuration files, but does not provide the emulators, browsers, or Java support. The only application provided is an X session, which is in fact all that is required to access a WinCenter server and use Windows applications.

### **2.8.2 What about Using the IBM Network Station Manager on a WinCenter Server?**

At the time of this writing, there is beta code available from the same IBM download site that provides capabilities similar to what is provided on a Windows NT 4.0 server. We intend to update this publication in the future to add a section on the implementation of that code on a WinCenter server.

However, the Windows NT 4.0 code cannot be applied directly to a Windows NT 3.51 server because of the significant differences between these two levels of Windows NT.

Therefore, you will find the following differences in the implementation on a WinCenter server:

- DHCP

The Microsoft DHCP code is used instead of the IBM version.

- NFS

Now provided by InterDrive Server for Windows NT, from FTP Software, Inc.

- Java Development Kit

The JDK is not required in this implementation, because there are no IBM TCP/IP configuration utilities (which were written as a Java application) as in the Windows NT 4.0 version.

### **2.8.3 What about Plans for WinCenter on a Windows NT 4.0 Platform?**

We cannot comment on this subject as we are not privy to the plans of FTP Software Inc., Citrix Corp or Microsoft. However, it is reported in the specialized press that there are indeed plans to that effect, which have been discussed between the owners of the different products involved.

---

## **2.9 Summary**

In summary, the operation of the IBM Network Station itself is fairly simple, and the boot process can be made simple and flexible as well.

However, for an administrator to manage this environment, he may need to become familiar with some of the inner workings of the server components and with the structure and content of the configuration files.

The chapters that follow have the objective of making the reader understand the general process but also to give the administrator enough details to understand how the components work and be able to do problem determination.

---

## Chapter 3. Windows NT Server Installation

This chapter provides a quick summary guide of the installation process for the IBM Network Station Manager and associated support programs on a Windows NT 4.0 Server platform.

We briefly discuss the following topics:

- Prerequisites
- Windows NT 4.0 Server Installation
- Downloading the required products from the Web
- Installing the products
  - The Java Development Kit
  - The IBM DHCP Protocol Driver
  - The Network Station Manager for Windows NT Server 4.0
  - The IBM Network Station Browser
  - The NAVIO Browser
  - The IBM TCP/IP Services
- Uninstalling and re-installing

### Product Documentation

Please be aware that there is an excellent document, available with the product, which provides detailed information on prerequisites, installation and configuration.

This document is called *IBM Network Station for Windows NT 4.0* and can be downloaded along with the software products. In our case, the filename for this document was winab103.pdf. See 3.3, "Downloading Products from the World Wide Web" on page 13 for downloading instructions.

We do not intend to reproduce here, in this chapter, all the instructions of that document; our intent is rather to give a summary and an illustration of what we have observed while going through the installation process ourselves. We strongly recommend that the user download and print a copy of the supplied documentation.

---

### 3.1 Prerequisites

Before you start installing the products required to support the IBM Network Stations, you should have the following:

- The MAC address of the Network Stations that you will be supporting with your boot server. You will need these addresses in order to create entries in your DHCP configuration and to have your DHCP server assign IP addresses to these Network Stations.

**Note:** If you do not have these addresses at this time, you can still install all the required products and create the DHCP entries later when you do get the required addresses.

- IP addresses for your boot server and for the Network Stations that you will be supporting with this server, as well as an IP domain name. Each Network Station is an IP host on the network, which requires a unique IP address.

**Note:** As with any IP network, you can of course use any address you wish if your network is isolated from the rest of your organization, but if you are going to connect to the Internet with Web browsers or connect to your organization's network, the addresses used must be officially assigned by the proper authorities.

- Verify that the IBM Network Stations have enough memory to support the applications that the user requires. Reference the product documentation guide for the latest figures on memory requirements.

**Note:** Please remember that the IBM Network Station is a real memory system (no paging or swapping) so the total amount of memory required is the sum of all the applications which the users intend to use simultaneously.

- In addition to the IP addresses, you may also need to configure host names, domain name, and domain name server addresses, the subnet mask used on the network, the default gateway (router), and the broadcast address.

All of these parameters are usually supplied by your network administrator.

- We do not have any official figures on the minimum hardware required to run a boot server. As with all performance type data, this really depends on the number of Network Stations you intend to support with one server, and the total activity generated by these Network Stations.

---

## 3.2 Performing a "Clean" Installation of Windows NT Server 4.0

It is best to start fresh by installing a clean copy of the Windows NT Server before installing the IBM Network Station Server. Here is a summary of the installation process and the values expected during installation.

- At the beginning of the install process, create a partition of at least 500 MB and format the partition with NTFS. You need about 200 MB for the Windows NT operating system files and about 130 MB for the IBM Network Station Manager and its associated support code.
- Once the formatting and copying of files is done and you are asked to restart, specify the computer name for this server. We used `nstationserver` as our name. When asked, ensure that it is a primary domain controller (it is the default). Give it a domain name and password.

### Domain Controller or Additional Server

Because the MS Internet Server (Web Server) and the IBM Login server can only authenticate users if they are defined locally, making the server a primary domain controller ensures that all users will be in the local Windows NT security database.

However, you can still define the server as an additional server instead of a primary domain controller, in which case you must ensure that the IBM Network Station users are defined on this server.

The boot server cannot be defined as a backup domain controller.

- When asked if the Microsoft Internet Information Server should be installed, make sure it is yes (It is the default). You need this to operate the Network Station Manager, as it is an application accessed through a Web browser.

- On the Network Protocols screen, ensure that TCP/IP is selected.
- On the Network Services screen, all the services should be selected by default. That's OK.
- On the adapter card setup, specify your own MAC address if you want to, or use the burned-in address. Ours happened to be a TRN adapter and we used a MAC of 400052005210.
- On the TCP/IP setup box, click **NO** in response to "Do you want to use DHCP?". You will install a DHCP driver (an IBM version of the DHCP driver) later on. The TCP/IP Properties notebook appears. Enter the following:
  - IP address of the server. Ours was 9.24.104.240
  - Subnet mask. We used 255.255.255.0
  - Default gateway. Ours was 9.24.104.1
- On the DNS tab, enter:
  - Host name will be pre-filled with the host name you entered previously.
  - Domain name. We used itso.ral.ibm.com.
  - DNS. Our name server was 9.24.104.108
- Click on **OK**.
- The Show Bindings box appears. Click on **Next**, then **Next** again.
- When requested to enter a domain name for this server, enter a chosen unique name. We used nstationdomain arbitrarily.
- Click **Finish**. The MS Internet Information server Setup appears. Ensure that the Internet Service Manager and World Wide Web Service are selected.
- Click on **OK** and accept defaults.
- Set correct time zone and date/time, click on **OK**, then follow instructions for the Display Properties.
- Once the copying of files is completed, reboot the server and log in as Administrator.

---

### 3.3 Downloading Products from the World Wide Web

At the time of writing of this book, the IBM Network Station Manager products and associated support programs were only available by downloading them from the World Wide Web.

However, when the product becomes generally available, it will also be available in CD-ROM format.

#### 3.3.1 Create a Target Download Directory

On the server, create a target directory to receive the software you download. We used **NS** as the target directory name, which can be placed on any drive.

#### 3.3.2 Download Necessary Software Products from the World Wide Web

With your preferred Web browser, access the following site:

<http://www.as400.ibm.com/nc/swdist>

### CHANGE OF URL

Note that, at the time of publication, the above URL has been changed to **<http://service.boulder.ibm.com/netstation/>**. Therefore, please be aware that some of the panels shown below will be different. However, we believe that the overall download site has improved for the better.

The figure below illustrates the current look of the Web page at that site.

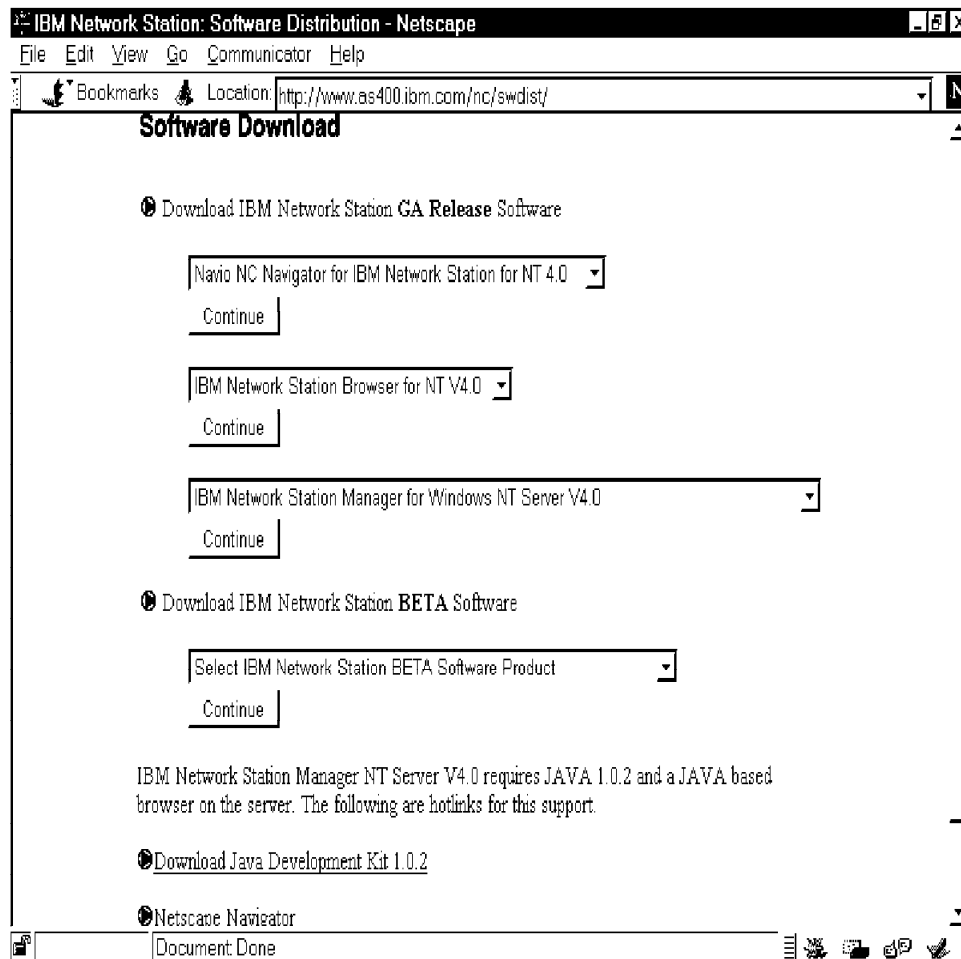


Figure 1. The Network Computing Software Distribution Web Site. Note the link to download the Java Development Kit and Netscape Navigator.

From this page, choose to download:

- Browsers for the Network Station

There are two browsers available for operation on the Network Station. These are browsers that execute as native applications on the Network Station itself. Which one to use is a matter of preference, most likely. Of course, both can be installed (and in fact both can be run simultaneously on the Network Station) and the administrator can give the Network Station user the choice of which one to use. In our example, we installed both in order to compare them. The two browsers are:

- The Navio NC Navigator for IBM Network Station NT 4.0
- The IBM Network Station Browser for NT 4.0

- The IBM Network Station Manager for Windows NT Server V4.0

This product provides a user-friendly graphical interface as a configuration tool to manage a network of IBM Network Stations.

- The IBM eNetwork Network Station Manager TCP/IP for Windows NT Server V4.0

This product installs the TCP/IP services required by the Network Station manager, such as a DHCP server for example. These services replace some of the equivalent services that are part of the standard NT Server. They provide functions additional to those available from the Microsoft version of these services. As an example, the IBM DHCP server supports unlisted clients, which MS's version does not.

See 3.9, "Installing IBM TCP/IP Services" on page 20 for additional details.

- The Java Development Kit V 1.0.2

This is the standard JDK as is available from the Web. It is a required component, because some of the IBM components rely on the services of the JDK for their operation, for example, the IBM TCP/IP configuration utilities.

- A JavaScript-enabled Web browser, such as Netscape's Navigator (Version 3 or Higher for Windows NT) or Microsoft's Internet Explorer Version 3.0 (or higher).

This is not a browser to operate on the Network Station but one to operate on the server, or another machine, to access the Network Station Manager application on the server. The Network Station manager is an HTTP-based application and requires the use of a browser that is JavaScript-enabled. This is optional if the user already has such a browser installed.

- Documentation

Ensure that you have the latest User's Guide for these products. To view or print the latest update, go to:

<http://www.as400.ibm.com/networkstation/pc>

where the following two documents are available:

- *IBM Network Station for Windows NT 4.0.* We strongly recommend the use of this document for your installation. It provides very useful information on prerequisite hardware and software, installation and configuration instructions.
- *IBM Network Station Use.* This is a useful guide concerning the setup of the IBM Network Station. It is available in several languages and is a copy of the manual packaged for delivery with the IBM Network Station.

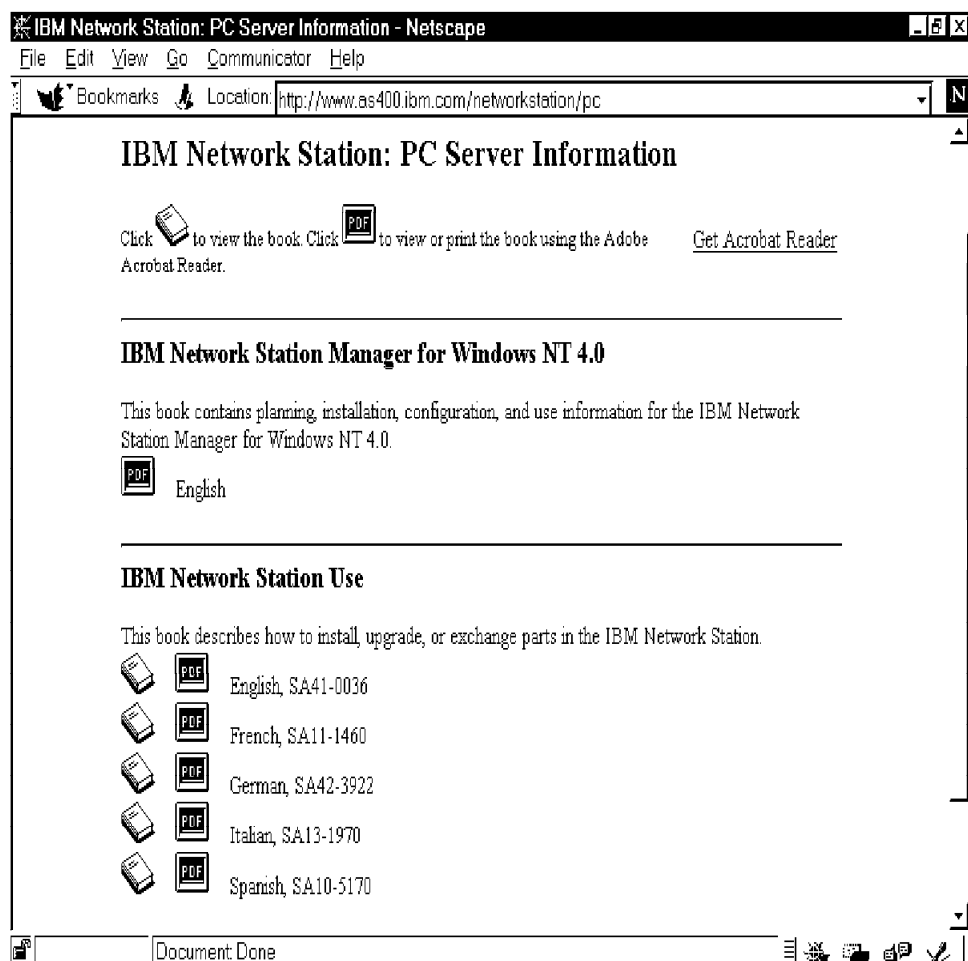


Figure 2. IBM Network Station: PC Server Information. The <http://www.as400.ibm.com/networkstation/pc> Web page

**Note:** From this Web page, you can also download the Adobe Acrobat Reader for Windows NT which is needed to view or print these documents. The hyperlink is shown in Figure 2 as [Get Acrobat Reader](#). We downloaded to our disk in the following fashion:

Table 1 (Page 1 of 2). Download SW Products from Internet to Your PC	
Software Products to download	Save as.....
Navio NC Navigator for IBM Network Station NT 4.0	drive:\NS\NSBROWSE\setup(navio).exe
IBM Network Station Browser for NT 4.0	drive:\NS\NSBROWSE\setup(ibmbr).exe
IBM Network Station Manager for Windows NT Server V4.0	drive:\NS\setup.exe drive:\NS\setup.1 drive:\NS\setup.2 drive:\NS\setup.3
IBM eNetwork Network Station Manager TCP/IP for Windows NT Server V4.0	drive:\NS\nsmtcpip.exe
Download Java Development Kit 1.0.2	drive:\jdk.exe



Table 1 (Page 2 of 2). Download SW Products from Internet to Your PC	
Software Products to download	Save as.....
Netscape Navigator (Version 3 or Higher for Windows NT)	use default value for your Server NT software product installation

### 3.4 Installing the Java Development Kit

1. Click on **Start→Programs→Windows NT Explorer** and locate drive:\JDK.EXE.
2. Copy the JDK.exe to the root directory where Windows NT is installed because this .EXE creates a JAVA subdirectory which must reside on the same root as the Windows NT system.
3. Double click on the **JDK.EXE** to initiate the setup program. This explodes the self-extracting JDK.EXE and creates the JAVA subdirectory.
4. Once the extraction is completed, you need to update the system path variable to include the JAVA/BIN subdirectory. To do so, click on **Start→Settings→Control Panel→System Environment**.
5. Scroll down the System Variables box and select **Path** as shown below:

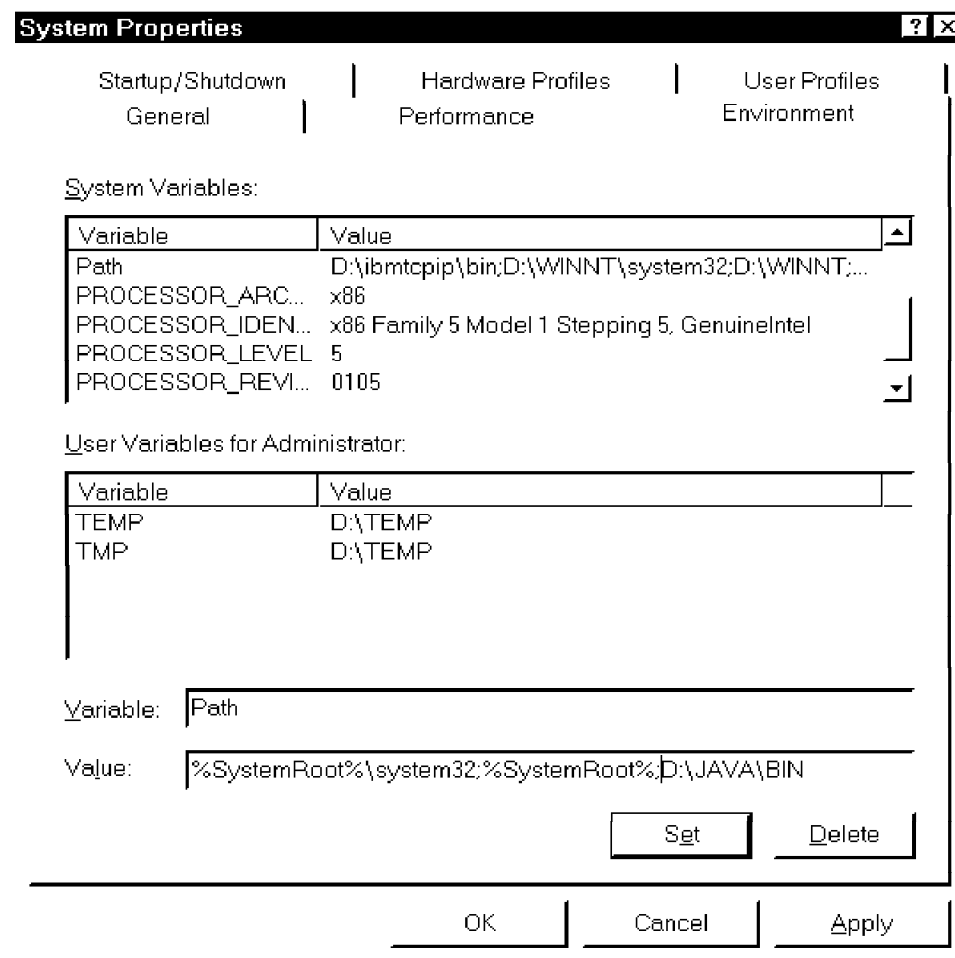


Figure 3. System Properties: Updating the PATH Variable

6. The current value should read `%SystemRoot%\system32;%SystemRoot%`

7. Position the cursor at the end of the above line, add the string  
;drive:\JAVA\BIN , click on **Set**, and then **OK**.
8. At this point, you need to shut down and restart Windows NT, and log back on as administrator.

At this point, if you want to test (optional) the successful installation of the JDK, you can do so as follows, using a DOS Command Prompt:

```
cd java\demo\TicTacToe  
appletviewer example1.html
```

**Note:** Some useful information on removing or troubleshooting can be found at:  
<http://www.javasoft.com/products/jdk/1.0.2/index.html>

---

### 3.5 Installing the IBM DHCP Protocol Driver

1. **Start**→**Programs**→**Windows NT Explorer** and locate  
drive:\NS\NSMTCPIP.EXE.
2. Double click on **NSMTCPIP.EXE**. This self-extracting zipped file creates a  
drive:\NS\WEDGE directory, in which are the components required to install  
the DHCP driver. It also creates a INSTALL.EXE in the NS directory which will  
be used later to install the TCP/IP services.
3. **Start**→**Settings**→**Control Panel**→**Network Protocols** and click on **Add**
4. Click on **Have a disk**.
5. In the Insert Disk Box, enter:  
drive:\NS\WEDGE
6. The select OEM Option box appears and the **IBM DHCP Driver** is highlighted.
7. Click on **OK** to install this driver.
8. You are returned to the Protocol Screen after installation.
9. Click on **Close** to end the driver installation.

**Note:** When asked if you want to shut down and reboot, Click on **No**,  
because there are other components that can be installed before we do a  
shutdown.

#### Locked Properties

Once the IBM DHCP Protocol Driver is installed, your Network Properties  
become locked. If you need to change Network Properties at a later time, you  
must first unlock them, using instructions as described in 3.14, "Disabling and  
Removing the IBM DHCP Driver" on page 31.

---

### 3.6 Installing the IBM Network Station Manager

The IBM Network Station Manager for Windows NT Server 4.0 is a Web-enabled  
application that installs on a Windows NT 4.0 Server. Once installed, any  
JavaScript-enabled Web browser, from any platform, can access the IBM  
Network Station Manager, via the Web server running on the server, in order to  
configure and manage IBM Network Stations.

1. **Start**→**Programs**→**Windows NT Explorer**, locate drive:\NS\Setup.exe and double click on **Setup.exe** to start the installation process.
2. When prompted for the destination directory, accept the default value if acceptable and click on **Next**.

**Note:** The destination directory *must* be on the same drive as the IBM TCP/IP Services. The installation program checks the above path and sets it as the default destination. We are using the same drive for Windows NT installation and all the IBM Network Station-related Software products.

Here is a brief description of the NSM install process:

- The Setup.exe unpacks itself and any setup.1 etc. files
- Setup.exe invokes the control pgm (\_setup.exe)
- \_setup.exe
  - Checks that no other instance is running
  - Issues a reminder that the user account must be Administrator
  - Invokes prereq.exe and waits for its completion
  - prereq.exe
    - Checks that local machine is a server and not a backup domain controller
    - Checks that user account is Administrator
- \_setup.exe (after completion of prereq.exe)
  - Starts the InstallShield product
  - Executes the control script (setup.ins) using setup.pkg
  - Welcome screen/Copyright reminder
  - Default directory prompt
  - Invokes the configuration program (config.exe)
  - config.exe
    - Creates NSMAdmin and NSMUser groups with "log on as batch" and "log on locally" rights
    - Adds the Administrator accounts to the above groups
    - Creates the NFS EXPORTS file in \ibmtcpip\etc
    - Installs the NSM Login NT service as autostart
    - Adds the NSM HTML and CGI directories to the MS IIS (Web) server configuration and makes the Network Station Manager the default page

---

### 3.7 Installing the IBM Network Station Browser

- **Start**→**Programs**→**Windows NT Explorer**, locate the drive:\NS\NSBROWSE\Setup(IBM BR).exe and double click on it.

The setup process creates a **drive:\NSTATION\MODS\NSB\** directory.

---

### 3.8 Installing the NAVIO Browser

- **Start** →**Programs**→**Windows NT Explorer**, locate drive:\NS\NSBROWSE\Setup(NAVIO).exe and double click on it.

The setup process creates a **drive:\NSTATION\MODS\NAV\** directory.

### 3.9 Installing IBM TCP/IP Services

1. **Start**→**Programs**→**Windows NT Explorer**, locate drive:\NS\Install.exe and double click on it.
2. Select the **Install TCP/IP applications**, click on **Next** and accept the default installation drive, if appropriate.  
  
It *must* be the same drive as the drive where the IBM Network Station Manager is installed.
3. You are warned that the IBMTCP/IP directory already exists; this is normal so you can click on **YES** to overwrite, and click on **Next** to install.

Install creates a drive:\IBMTCP/IP\ETC\DHCP.DCF file. This file is the default configuration file for DHCP (Dynamic Host Configuration Protocol). It contains an embryonic configuration that must be updated by the administrator to reflect his own network environment. See Chapter 6, "Understanding Dynamic Host Configuration Protocol (DHCP)" on page 55 for more information.

After the TCP/IP components are installed, the IBM TCP/IP Configuration panel is presented, as shown below:

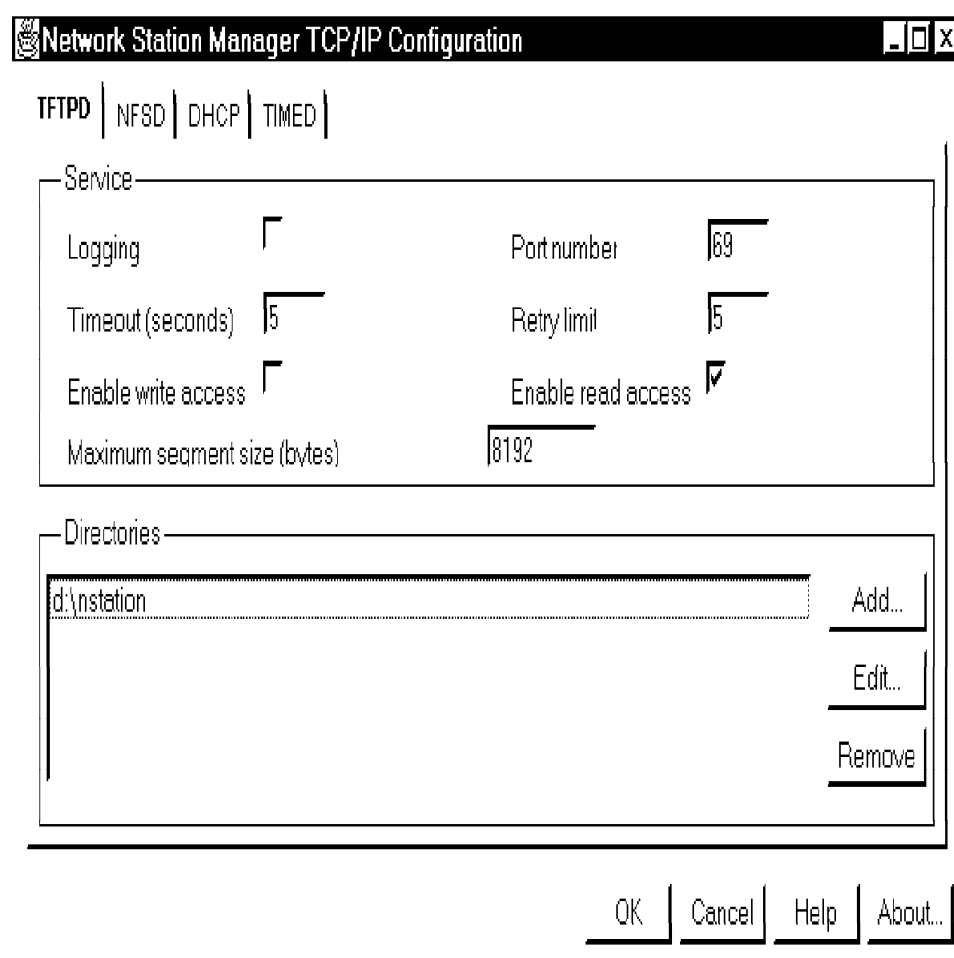


Figure 4. IBM Network Station Manager TCP/IP Configuration. TFTP configuration tab.

1. Click on the **TFTPD** tab.

2. In the Directories area, click on **Add**.
  3. In the add TFTP Directory box, enter drive:\nstation, then click on **OK**.
  4. Ensure that the **Directories** box reads as in Figure 4 on page 20.
- Note:** You can optionally click on the logging checkbox if you want the TFTP driver to log messages to the NT application log (for problem determination purposes).
5. Click on **NFSD** tab to get the panel below.

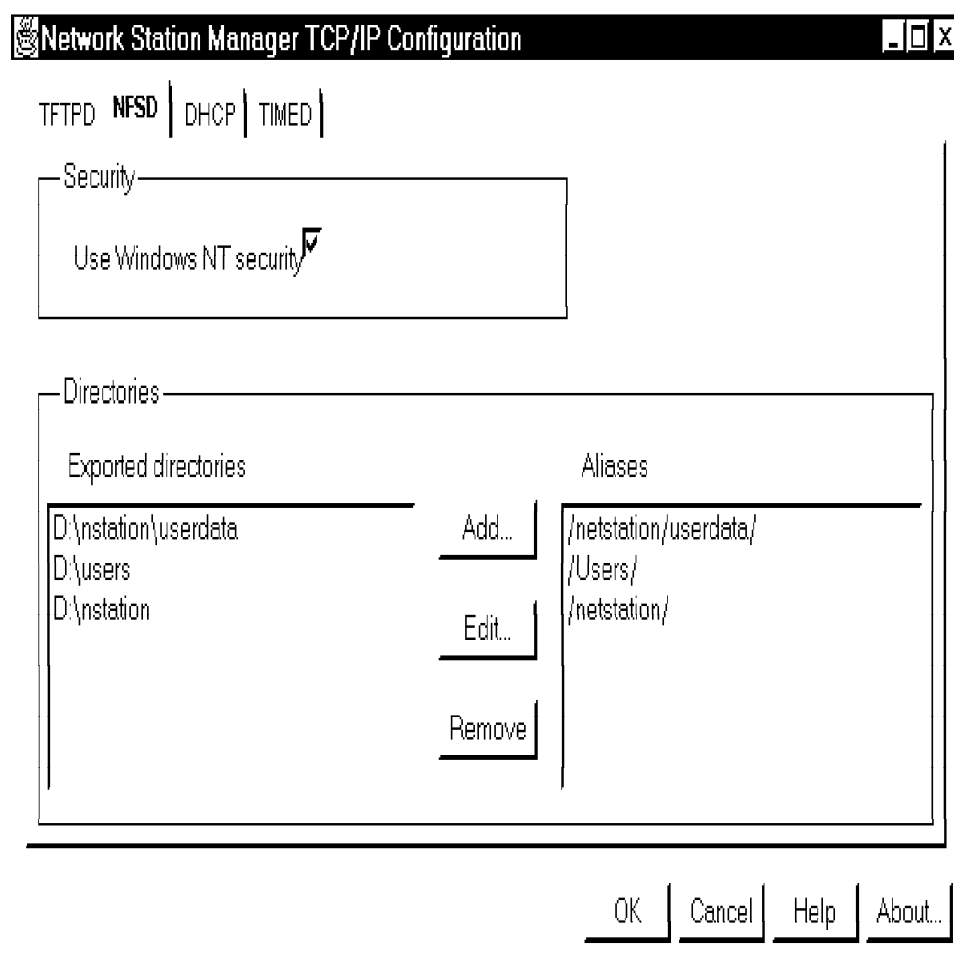


Figure 5. IBM Network Station Manager TCP/IP Configuration. Network file system server configuration tab.

6. Ensure that the Exported Directories and the Alias Directories reads as shown in Figure 5.
- If for some reason you do not have the entries as shown in the figure, you can manually add these entries.
7. Click on **TIMED** tab.
  8. Ensure that the **Adjust Local Time** box is ticked.
  9. Click on **DHCP** tab.
  10. Ensure that the DHCP Configuration File Name is DHCP.DCF.
  11. Click on **OK** tab.
  12. Shut down and restart Windows NT to allow these changes to take effect.

### 3.10 Creating Network Station User Accounts

During the installation of the Network Station Manager, the following Windows NT User Groups are created:

- **NSMAdmin** to include users with authority to administer IBM Network Stations. These users can use the Network Station Manager to make settings for *any* IBM Network Station and *any* user.
- **NSMUser** to include users with authority to use the Network Station Manager to make basic settings for their *own* logon environment.

**Note:** Only users belonging to these groups will be authenticated when they do a logon on a Network Station or attempt to use the Network Station Manager from a Web browser.

Refer to the Windows NT online documentation for instructions on how to define a user and how to include a user in a group.

**Note:** Your server must be physically connected to the network in order to be able to use this function. If not, you get an error message indicating that Windows NT is unable to find a path to the network. We have done the following:

1. **Start→Programs→Administrative Tools (Common)→User Manager for Domains.**

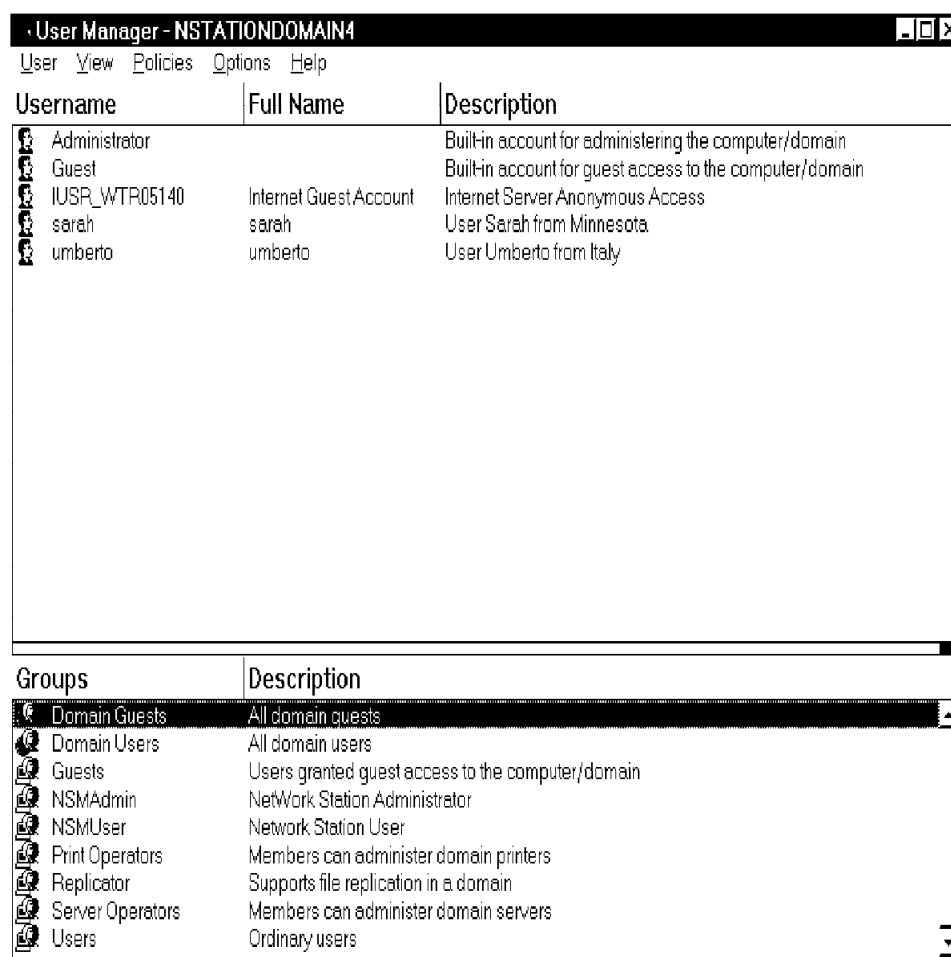


Figure 6. User Manager for Domain. How to add the new groups, NSMAdmin and NSMUser.

2. Click on the **User** menu, click on **New User**, and enter all details for this user.
3. Click on **Groups**, select **NSMUser** and click on **Add**.
4. Select **NSMAdmin** and click on **Add** only if you want to grant this user the administration authority.
5. Click on **OK** to exit and click on **Add** to add this user to the Windows NT Security database.
6. Click on **Close** to exit New User creation and **Exit** to exit User Manager screen.

---

### 3.11 Starting the IBM Network Station Manager for Windows NT Server 4.0

The IBM Network Station Manager for Windows NT Server 4.0 is a Web-enabled application which is installed on a Windows NT Server. Any JavaScript-enabled Web browser, from any platform, can access the Network Station Manager by specifying the following URL:

`http://Web Server IP Address or hostname/nstation/html/admin.htm`

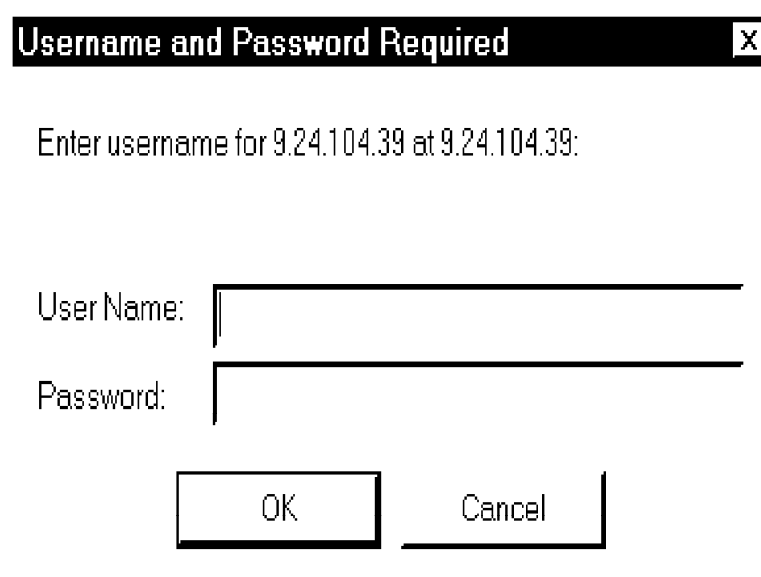
If you are using a Web browser on the server itself, the easiest way to access the Network Station Manager is to specify the URL as:

`http://127.0.0.1/nstation/html/admin.htm`

which is the address of the loopback interface. In fact, 127.0.0.1 should be sufficient, since the default home page is the Network Station Manager main screen (as was installed by default).

You can also use the actual real IP address of your server instead of the loopback address.

The IBM Network Station Manager prompts for a user name and password, which must match a user definition in the Windows NT security database, and this user must belong to either the NSMAdmin group or the NSMUser group.



Username and Password Required

Enter username for 9.24.104.39 at 9.24.104.39:

User Name:

Password:

OK Cancel

Figure 7. IBM Network Station Manager Login Box

If you are an authorized user, you get the following main menu for the IBM Network Station Manager.



Figure 8. IBM Network Station Manager. From this page you can start to configure IBM Network Stations.

From this page, if the user belongs to the NSMAdmin group, he can make any settings for *any* IBM Network Station or *any* user.

If the user belongs to the NSMUser group, he can make settings only for his *own* user ID.

If the browser used to access the NSM is not JavaScript-enabled, the user gets the following message:



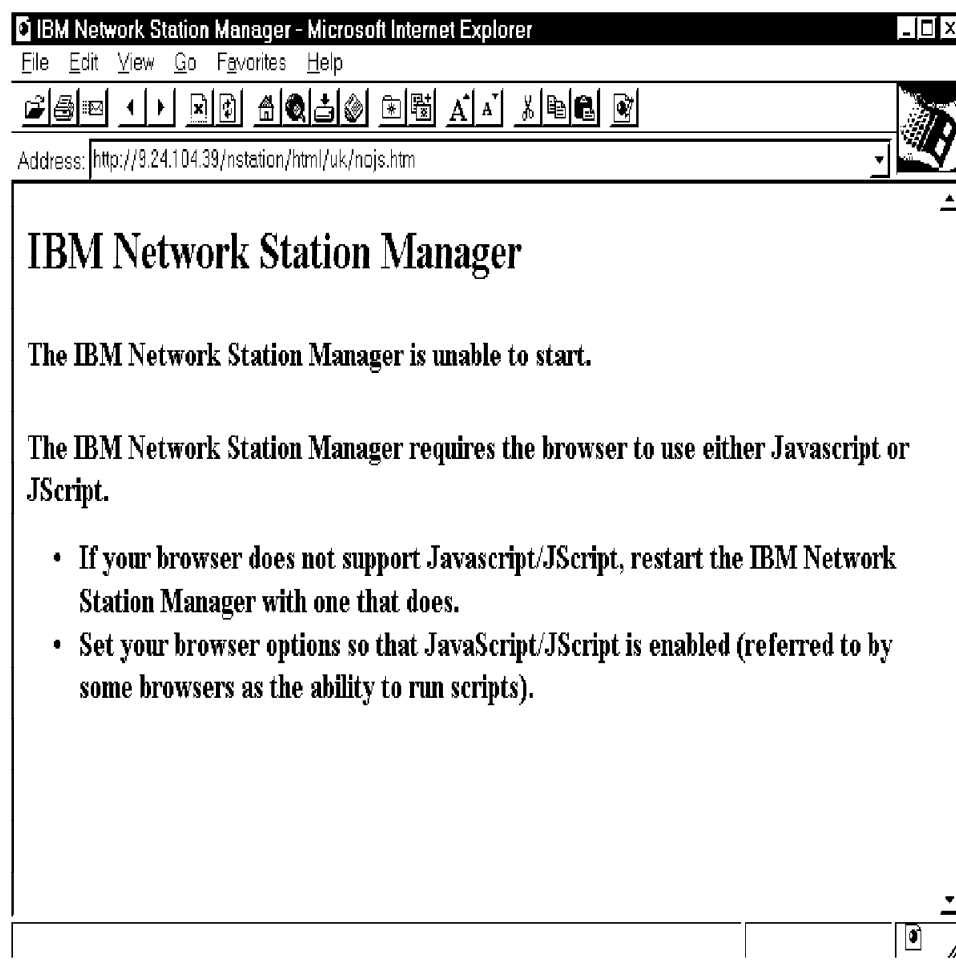


Figure 9. IBM Network Station Manager. Your Web browser must be Javascript-enabled or you get this message.

**Note:** In our tests here, we used Netscape Communicator 4.01 on Windows NT but the Microsoft Internet Explorer Version 3 or higher works as well. From an IBM Network Station, you can use IBM Network Station Browser or Navio Browser to access the IBM Network Station Manager.

---

## 3.12 Installation Results

The following components and services were installed as a result of the installation process.

- NT Services

The following NT services were installed. These were installed as autostart so they should all be active after a reboot:

- TFTP (Trivial File Transfer Protocol) Server.
- DHCP (Dynamic Host Configuration Protocol) Server.
- NFS (Network File System) Server.
- RPC Port Mapper Server.
- Time Server.
- NSL (Network Station Login) Server.

The panel below (Click on **Start**→**Settings** →**Control Panel**→**Services**) displays the NT services (the first six services listed in the display) that should be active on your system after a reboot.

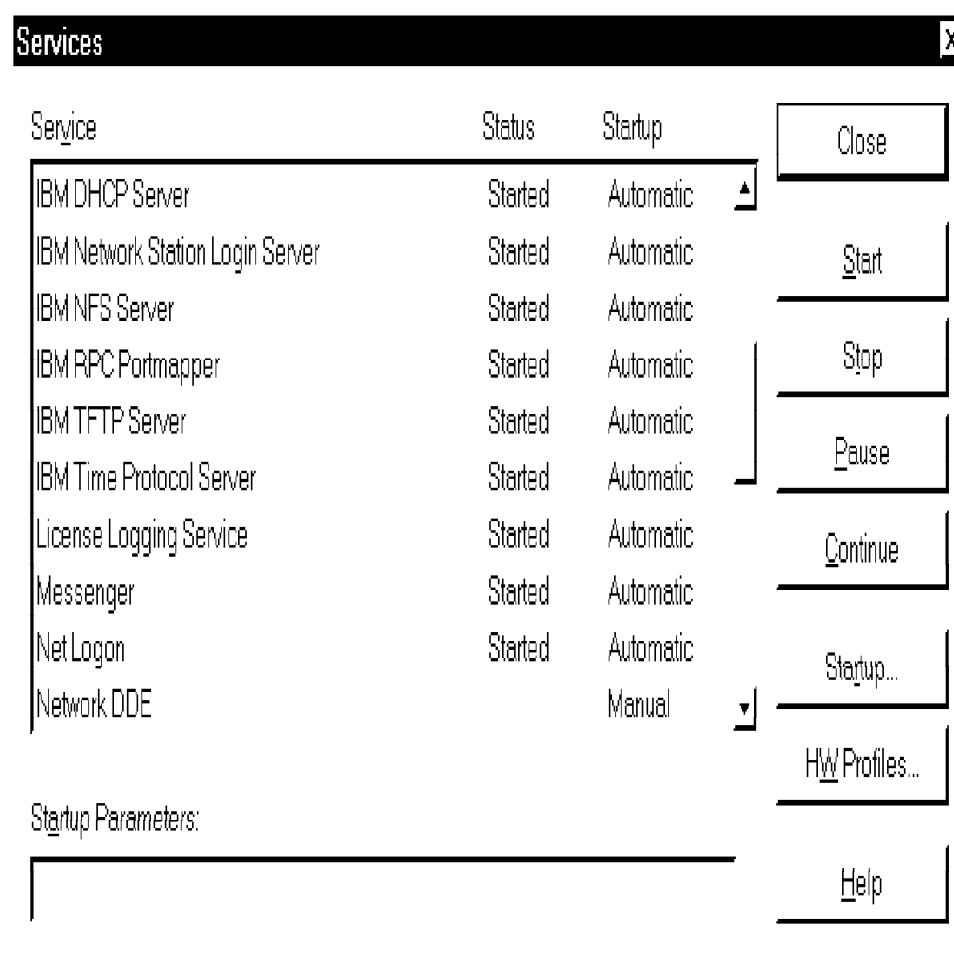


Figure 10. Windows NT Services Installed

- Web Server Entries

The installation process also updates the MS Internet Information Server (Web Server) by adding the required directories and by making the Network Station Manager the default document, as shown in the panel below. To get this panel, click on **Start**→**Programs**→**Microsoft Internet Server(Common)** →**Internet Service Manager**, then double click on **WWW** (that's the World Wide Web service), double click on the entry (with the green light) that appears below the WWW entry, and select the **Directories** tab.

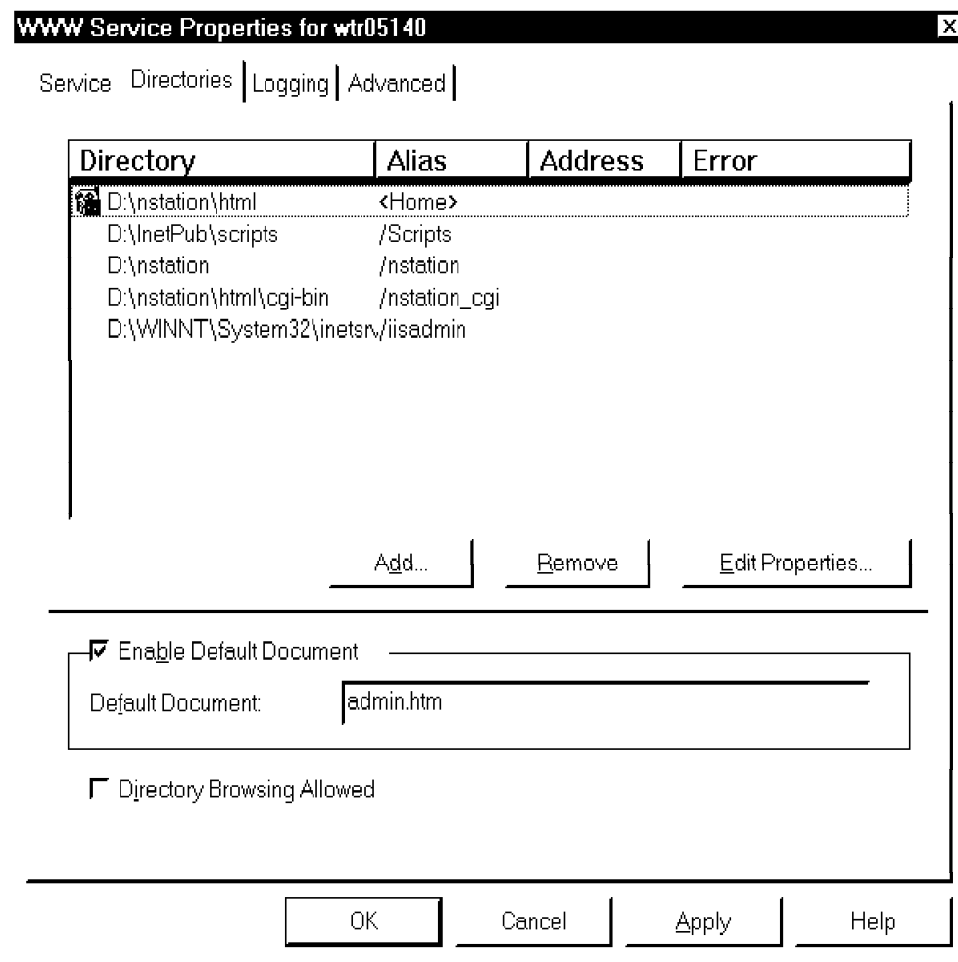


Figure 11. Web Server Updates

- EXPORTS file

An EXPORTS file is created that contains the path and directories that can be mounted by NFS clients, as well as the permissions for read/write that these clients have. The default EXPORTS file, which is located in x:\ibmtcpip\etc, is as shown below:

```
x:\nstation -Alias /netstation/ -ro
x:\nstation\userdata -Alias /netstation/userdata/
x:\users -Alias /Users/
```

The information from the EXPORTS file appears in the TCP/IP Configuration for NFS, as shown in Figure 5 on page 21.

- DHCP.DHCPD.CFG file

A DHCP.DHCPD.CFG file is created as the default DHCP configuration file. This file is also located in x:\ibmtcpip\etc and it contains a few sample entries which the user can modify to suit his own particular environment. The default supplied file contains the following entries:

```
logFileName dhcpd.log
leaseExpireInterval 1 Hours
leaseTimeDefault 1 Days
supportBOOTP false
supportUnlistedClients false
```

```

Option 2 1
Option 67 /nstation/kernel
subnet 10.0.0.0 255.255.255.0 10.0.0.2-10.0.0.254
{
  Option 1 255.255.255.0
  client 6 0x0000E580167a ANY (alias=ns1
  {
    Option 12 netstation1
  }
  client 6 0x0000E5123456 ANY (alias=ns2
  {
    Option 12 netstation2
  }
}

```

- Registry Entries

The following NT registry entries are created, for the IBM Network Station Manager product.

```

HKEY_LOCAL_MACHINE
  SOFTWARE
    IBM
      Network Station Manager
        Current Version
          "Install Location = x:\nstation"
          "Version = 1.00"
HKEY_LOCAL_MACHINE
  SYSTEM
    Current Control Set
      Services
        NSLD
          "HomeDirPrefix" = " /Users/"
          "NextUID" = "0x00000001"
          "PrefsDirPrefix" = "/netstation/UserData"
HKEY_LOCAL_MACHINE
  SYSTEM
    Current Control Set
      Services
        EventLog
          Application
            NSLD
              "EventMessageFile" = "x::\nstation\Login\nslmsg.dll"
              "Types Supported" = 0x00000007
        W3SVC
          Parameters
            "Authorization" = 0x00000002
            "DefaultloadFile" = "admin.html"
          Virtual Roots
            "/" = "x:\nstation\html,,1"
            "/nstation" = "x:\nstation,,1"
            "/nstation_cgi" = "x:\nstation\html\cgi-bin,,4"

```

- Directories

There are three directories that contain all the installed components. The total amount of disk space is about 52 MB for the three directories.

Assuming we installed on the C: drive, they are:

- c:\JAVA - The Java JDK

This is approximately 5.2 MB in size.

- c:\IBMTCP/IP - The IBM TCP/IP Services

This is approximately 4.4 MB in size.

- c:\NSTATEMENT - The IBM Network Station Manager and related files

This is approximately 41.8 MB in size, including the installation of the two Network Station browsers.

---

### 3.13 Uninstalling the Product Components

If you wish to uninstall the IBM Network Station Manager and related support components, it is recommended that they be removed in the reverse order of their installation, that is:

1. The IBM Network Station Manager TCP/IP Services
2. The Network Station browser(s) (The Navio browser and the IBM Network Station browser)
3. The IBM Network Station Manager

To uninstall from the Windows NT Desktop perform the following:

- Click **Settings**→**Control Panel**→**Add/Remove Programs**, highlight the product to be removed, and click the **Add/Remove** button.
- Select **Yes** on the Confirm on Delete window
- Select **OK** when you see the uninstall completed confirmation message.

Here is an example of how to remove the IBM TCP/IP Services.

1. Click **Settings**→**Control Panel**→**Add/Remove Programs** and the panel below appears.

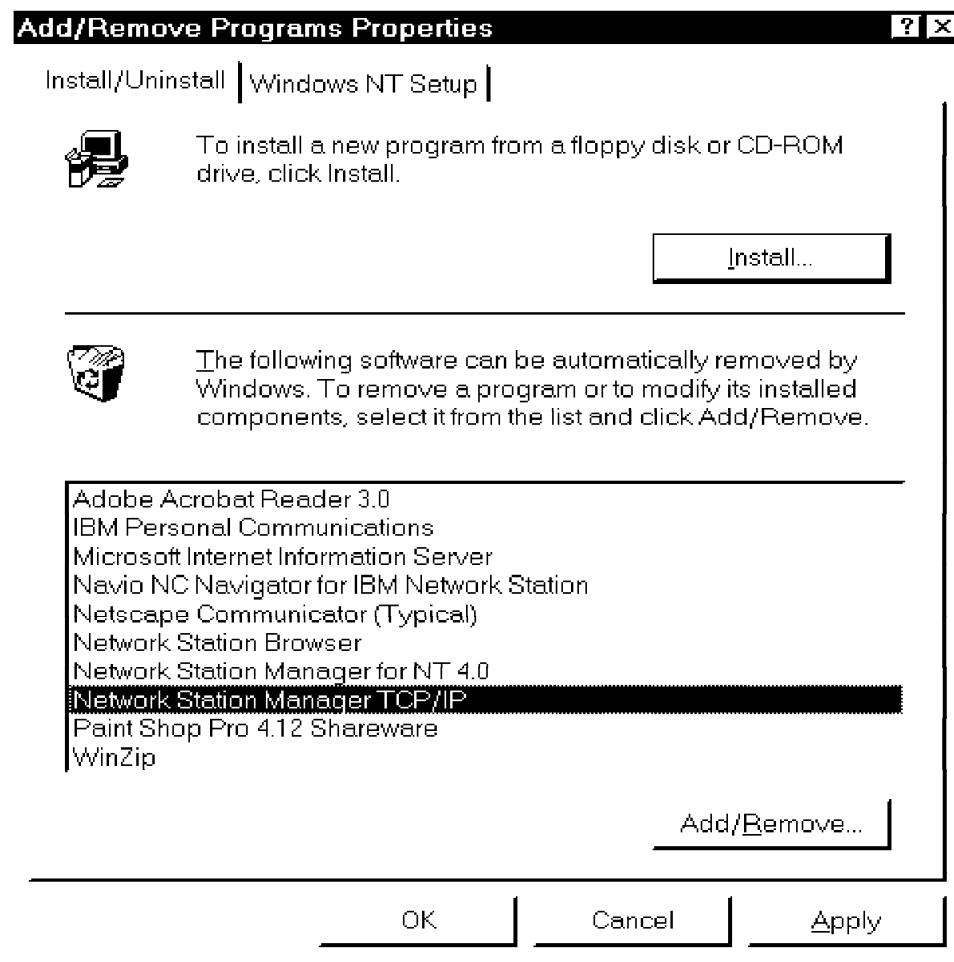


Figure 12. Add/Remove Programs

2. Select the Network Station Manager TCP/IP entry and click on **Add/Remove**.

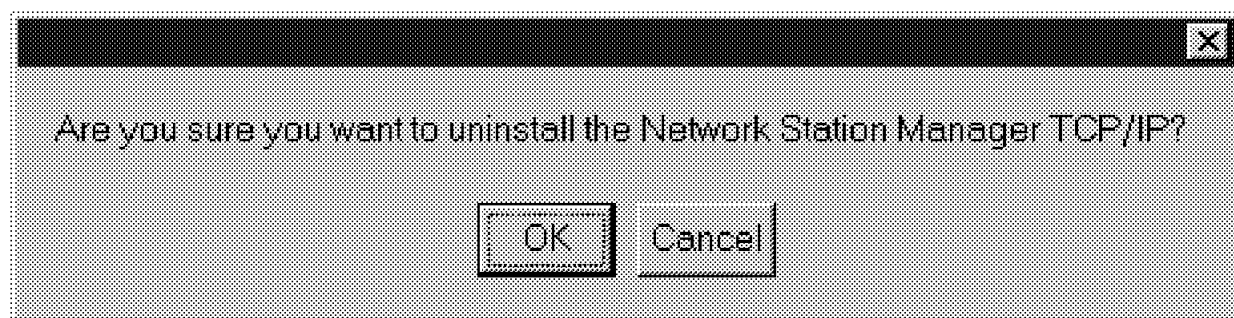


Figure 13. Select OK to Remove Selected Application

3. Confirm that you indeed want to delete

You then get the following panel on which the different components to be removed are checked off one after another, giving the user a visual indication of the removal activity taking place.

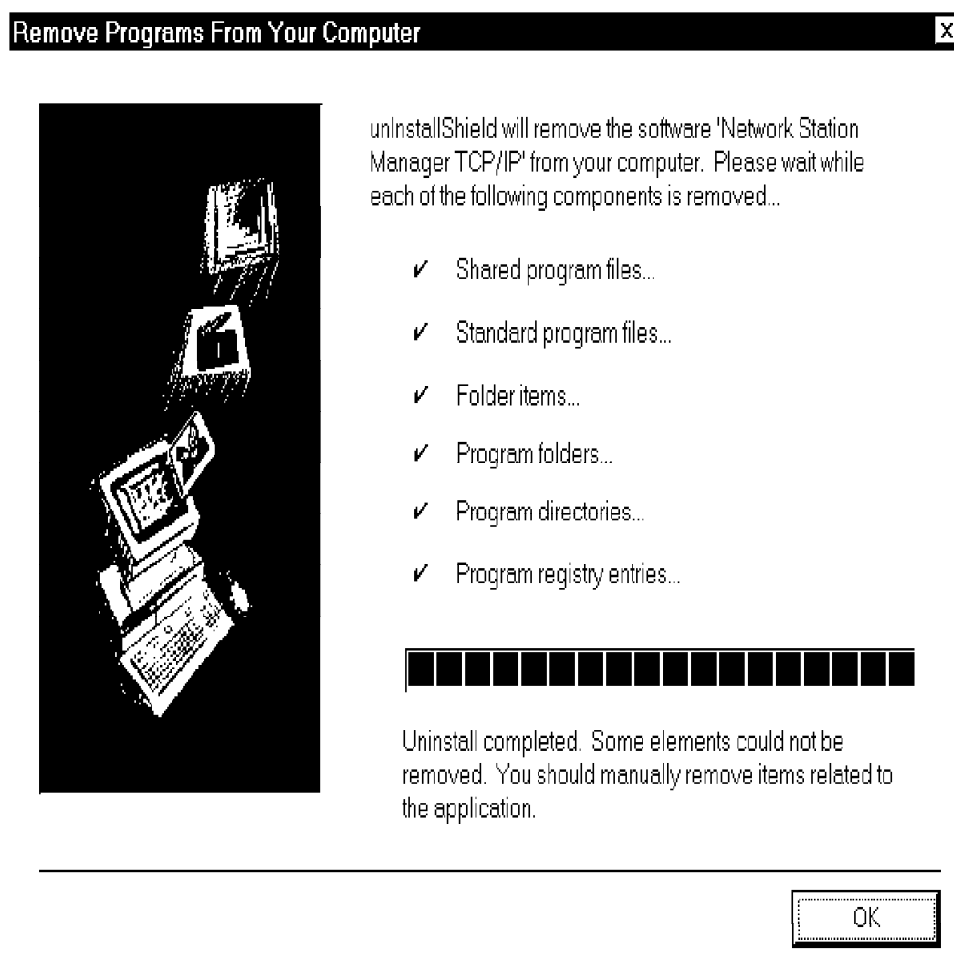


Figure 14. Uninstall Complete Confirmation

4. The Uninstall Completed message appears below the progress bar.

### 3.14 Disabling and Removing the IBM DHCP Driver

**Note:** Once the IBM DHCP Protocol Driver is installed, you are prevented from changing the DHCP Driver or TCP/IP Protocol Properties. If you try to edit the TCP/IP Properties, you get the following error message:



Figure 15. Microsoft TCP/IP Error

This is normal. If you wish to change the TCP/IP properties, the DHCP driver must be disabled and removed first by carrying out the following steps:

1. Open a window with a command prompt.
2. Type **wejcfigex -disable** and **wejcfigex -remove** to disable and remove the IBM DHCP Driver.
3. Open the Network Control Panel by clicking on **Start→Settings→Control Panel→Network→Protocols**
4. Select the hp2.DHCPDriver, click on **Remove**, and confirm the removal by clicking on **Yes**.
5. You can then make the required changes to your TCP/IP properties. You will then be asked to reboot, after making changes to the TCP/IP properties.

To re-install the DHCP protocol driver after you have made the required change to your TCP/IP Protocol Properties, follow the same procedure as outlined in 3.5, "Installing the IBM DHCP Protocol Driver" on page 18, after which you will need to reboot again.



---

## Chapter 4. IBM Network Station Installation and Configuration

The next step, after installation of the boot server, is to install and set up a Network Station so that it can boot from the server.

---

### 4.1 Physical Installation

For the physical installation of the Network Station, please refer to the installation instructions supplied with the Network Station.

If these are not available to you, you can get a copy of these instructions from the Web, as indicated in Chapter 3, "Windows NT Server Installation" on page 11.

Another source is to refer to the *AS/400 - IBM Network Station - Getting Started* redbook in which the basic installation instructions are referenced.

---

### 4.2 Setup/Configuration Methods

There are two primary methods that can be used to boot from a server:

- Using configuration settings stored in the NVRAM (non volatile RAM)

These settings are entered manually using the SETUP utility panels of the IBM Network Station.

- Using a BOOTP or DHCP server in order to obtain the same configuration settings.

This is called booting from the network, and requires no configuration settings at the Network Station other than to select this method of boot. On the other hand, it requires that an administrator configure the BOOTP or DHCP server to allow the Network Station to boot from this server.

---

### 4.3 Configuration of the Network Station

Once the Network Station is installed and connected to the network, power on the Network Station and wait until the POST (Power On Self Test) 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:

## Main Setup Screen

SCRN02 Station	IBM Network  Setup Utility
F2 = View Network Parameters F3 = View Boot Parameters F4 = View Hardware Configuration	
F5 = Set Network Parameters F6 = Set Boot Parameters F7 = Set Monitor Parameters F8 = Set Language Parameters	
F9 = Verbose Diagnostic Messages Enabled	
Enter = Reboot	

cbechard-08/97

Figure 16. Main Network Station SETUP Utility Panel

The first three entries (F2, F3, F4) are used to view the parameter settings. These may be the only options available once the administrator has set a password on the Network Station in order to prevent the user from modifying the setup parameters.

If you need to reset this password, because you inherited a Network Station from someone who had set this password, and were not supplied the password, you will need to physically reset the Network Station. Please refer to Chapter 12, "Problem Determination - Tools, Tips and Techniques" on page 159 for instructions on how to remove the password.

A good practice, at the beginning, is to use the PF9 key to enable verbose 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 F8 key and following the instructions.

Similarly, press F7 to set the monitor resolution and follow the instructions supplied, which are pretty self-explanatory.

### 4.3.1 Setting Up for a Boot from NVRAM

The simplest initial way to verify that your boot server is configured properly and that your Network Station functions properly is to boot using settings in NVRAM.

Press F5 to set the network parameters; this action displays the panel shown below:

#### Set Network Parameters Screen

SCRN05 IBM Network Station  
Set Network Parameters

IP Addresses from ..... Network **NVRAM**

Network Station IP Address ..... 9.24.105.189  
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  
Gateway IP Address..... 9.24.105.1  
Subnet Mask ..... 255.255.255.0  
Broadcast IP Address ..... 255.255.255.255

Ethernet Standard ..... Version 2 **IEEE 802.3**

Use cursor keys to select option

Enter = Save F12=Cancel F11=Restore Parameter

cbechard-08/97

Figure 17. Set Network Parameters - 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 which 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  
If you have multiple boot servers, you can specify a second and a third server to be tried if the first server is unavailable.
- Third Boot Host IP Address
- 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 need also to select between the Version2 or IEEE802.3 standard.

Press enter to save these parameters.

Back on the main SCRNO2 Setup utility panel, press F6 to set the boot parameters. This displays the panel shown below:

### Set Boot Parameters Screen

SCRNO6 IBM Network Station  
Set Boot Parameters

Boot File .....

TFTP Boot Directory ..... /nstation/

NFS Boot Directory .....

Configuration File ..... standard.nsm

Configuration Directory ..... /nstation/configs/

TFTP Order ..... 1

NFS Order ..... Disabled

MOP Order ..... Disabled

LOCAL Order ..... Disabled

Appended to Boot Directory, 64 character  
limit

Enter = Save F12=Cancel F11=Restore Parameter

cbechard-08/97

Figure 18. Set Boot Parameters - IBM Network Station SETUP Utility

This is where you specify the files and the path to the files residing on the server that are required to boot the Network Station.

First enter the name kernel in the Boot File parameter. You can also leave it blank if you prefer, as the default is the value kernel.

In the TFTP boot directory, enter the value /nstation/ This is the path to the kernel file that resides in /nstation/kernel.

Leave the NFS boot directory empty.

Specify the value `standard.nsm` in the Configuration File field and the value `/nstation/configs/` in the Configuration Directory field. Do not forget the trailing `/` as this path gets concatenated with the file name to produce the `/nstation/configs/standard.nsm` string.

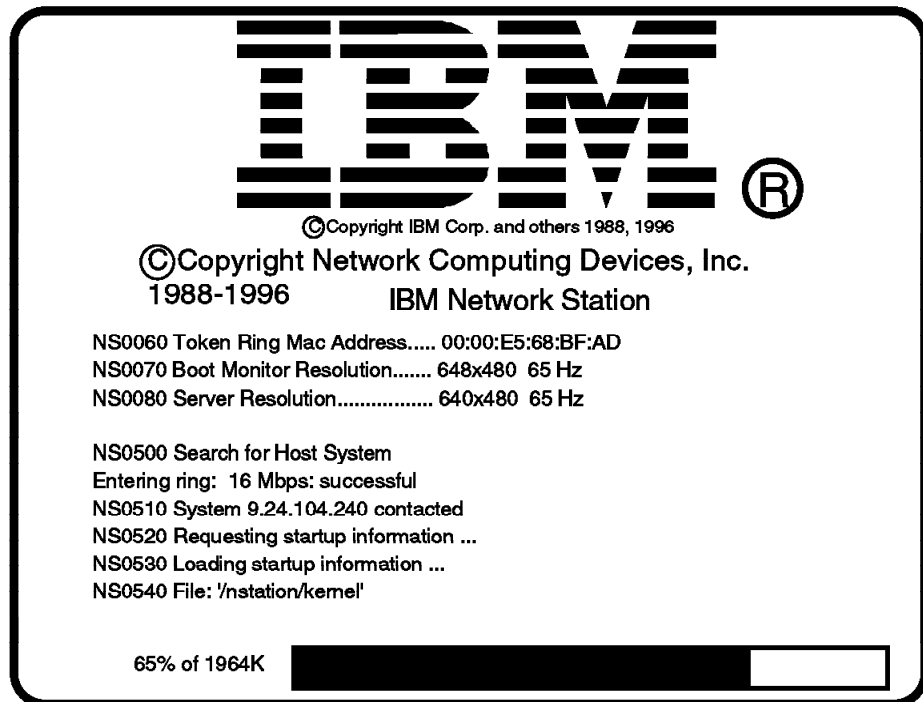
Finally, ensure that TFTP Order is specified as 1, and the other entries as Disabled. In fact, they could have a value other than disabled, such as 2 for the NFS order for example, which means that if the TFTP method is unsuccessful, the second one to be tried is NFS.

In our case, we only want to try TFTP because the boot server you installed in the previous chapter was configured automatically for a TFTP boot.

Press enter to save these entries. This takes you back to the main SETUP panel, where you can press enter 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 network station:

## Booting



cbechard-08/97

Figure 19. IBM Network Station - Kernel Loading Progress Bar

### 4.3.2 Logging On

Assuming the boot process is successful, after the kernel is loaded, it takes control and loads the configuration files from the server. Assuming that the verbose option was turned on using the F9 key on the main setup panel, you should see the messages being displayed on the monitor as each configuration file is read, followed by font files.

You should then see a logon screen displayed, asking for user ID and password. After entering a proper user name and password (these were defined on the server and made part of either the NSMAdmin or NSMUser group), the next display should be a menu bar at the bottom of the screen on the Network Station.

At this point, the boot process is complete and the user can start using applications such as the emulators, or the browsers, X-sessions, or Java applets or applications.

### 4.3.3 Setting Up for a Boot Using DHCP

Once you have an NVRAM boot working successfully, you can configure your DHCP server to service DHCP clients. See Chapter 6, "Understanding Dynamic Host Configuration Protocol (DHCP)" on page 55 for guidance in configuring your DHCP server.

On the 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 F5 to enter the network parameters setup panel, as shown below:

## Set Network Parameters Screen

SCRN05

IBM Network Station  
Set Network Parameters

IP Addresses from .....

Network

NVRAM

DHCP IP Addressing Order: .....

1

BOOTP Addressing Order: .....

Disabled

RARP IP Addressing Order: .....

Disabled

Ethernet Standard .....

Version 2

IEEE 802.3

Use cursor keys to select option

Enter = Save

F12=Cancel

F11=Restore Parameter

cbechard-08/97

Figure 20. Set Network Parameters - IBM Network Station SETUP Utility

Select NETWORK instead of NVRAM on the IP Addresses from line. This eliminates the NVRAM set of parameters to display only the network related parameters, as shown below:

You only need to ensure that the DHCP Order 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 you were successful at booting from the DHCP server.

If unsuccessful, please refer to Chapter 12, "Problem Determination - Tools, Tips and Techniques" on page 159 for guidance on the tools to use to do problem determination.





---

## Chapter 5. IBM Network Station Customization Files

The IBM Network Station customization files contain the parameters required to successfully start the Network Station for any user, while still providing enterprise-wide rules support and ensuring security. The Network Station customization files are read by the Network Station at boot time and log out time (prior to another user doing a login).

The IBM Network Station customization files reside on a boot server and are read and interpreted by the kernel program as part of the IBM Network Station initialization, login, and logout procedures. The files must reside on the same server as the kernel is read from. The kernel requests the configuration files from the same server as the boot file was loaded from and it uses the same protocol (TFTP) that is used to load the kernel.

There are three main types of Network Station customization files that contain the parameters for the Network Station environment.

- Configuration files
- Startup files
- Application and user preference files

---

### 5.1 Configuration Files

Configuration files provide hardware and kernel-specific parameter information to the Network Station. These files can be broken down into three levels:

1. Global level - applies to all Network Stations and all users
2. Workstation level - applies to one specific Network Station
3. User level - applies to one specific user

#### 5.1.1 Global Level Configuration Files

Configuration files at the global level include parameters that specify IBM-supplied hardware and kernel-specific defaults. These files are read at boot time and at logout time. They are either modifiable through the Network Station Manager or manually by an administrator. These files reside in `/nstation/configs` and include:

- `standard.nsm`
- `required.nsm`
- `control.nsm`
- `defaults.nsm`
- `defaults.dft`

There are several files that the administrator should avoid modifying manually, and we identify these below with a DO NOT MODIFY remark.

There are a few reasons why the administrator should refrain from manually altering these files, for example:

1. It is easy to make mistakes when manually altering files with an editor. Therefore, to avoid costly mistakes, it is preferable to let the configuration GUI, such as the IBM Network Station Manager, modify these files.
2. As the product evolves over time, some changes may be made by the developers to some of these configuration files, which may not agree with

the changes made manually. It is therefore preferable to use the GUI interface, which, in the event of a change, would make that change transparent to the user.

3. By making changes in a separate file (for example defaults.dft) and using this file to override the parameters in the files managed by the Network Station Manager, we isolate our specific changes and make it easier to refresh a release for example. That is, you can replace the supplied files at any time without fear of losing the custom changes you made.

#### **Avoid editing files**

Another reason for being very careful in editing files manually is that the Network Station expects to see only LFs (Line Feed) at the end of a line instead of CRLF which is usually what a PC editor puts out at the end of a line. This could potentially cause the Network Station to enter into a PANIC state.

If you must edit, then try to use an editor that recognizes the difference between a DOS file and a UNIX file. We used the PFE32 Editor (Programmer's File Editor) by Alan Philipps. We found this editor to be very practical and it is available free of charge from the Web. Its Web home page is:

<http://www.lancs.ac.uk/people/cpaap/pfe/>

We list below the configuration files, along with a short description and a recommendation as to whether these files should be manually modified or not:

#### **standard.nsm**

MODIFY MANUALLY ONLY IF ADDING ADDITIONAL READ STATEMENTS

This is the default initial configuration file, also known as the generic configuration file, shipped by IBM. Its role is to call other Network Station configuration files in the correct sequence.

**Note:** The sequence is very important since setting a value for a parameter can be done many times, and the last value specified is the one which is retained.

This is a simple file that can easily be modified manually by an administrator and it should be used if there is a need to add read statements for additional configuration files that have been manually created by an administrator, or to change the order in which the files are read.

#### **required.nsm**

DO NOT MODIFY

This file contains configuration settings for the Network Station hardware and kernel; these parameters must be set in order for the Network Station to work properly. This file is shipped by IBM and should *not* be altered. If changes need to be made to any of these settings, you should use the Network Station Manager program, which will include statements in the defaults.nsm file or, you can update the defaults.dft file to override the parameters in the required.nsm file.

## **control.nsm**

### **DO NOT MODIFY**

This file contains system-level default values for configurable Network Station hardware and kernel preferences. This file is not accessed by the Network Station Manager. This file is shipped by IBM. If you need to make system level changes to override the parameters in this file, use the Network Station Manager, which inserts parameters in the defaults.nsm file for the system-level preferences.

## **defaults.nsm**

### **CREATE & MODIFY USING NSM**

This file contains administrator-supplied system-level values for configurable Network Station hardware and kernel preferences. Default values for these preferences are kept in control.nsm. Any system-level hardware or kernel preference that is configurable through the NSM is updated in the defaults.nsm file.

For example, if you want to specify that a specific level of the boot monitor firmware be applied to the Network Station, you would *not* edit the control.nsm file. Rather, use the Network Station Manager and select Hardware, System defaults, Next, Update boot monitor from this file, Select bp28ae in the list box, and then Finish. This action updates the defaults.nsm file with the following line:

```
set boot-prom-update-file="/nstation/proms/bp28ae"
```

and this parameter overrides what is specified in the control.nsm file (which is, by default, set to the value nil).

## **defaults.dft**

### **CREATE & MODIFY MANUALLY**

This is a special manually created file containing configurable system level Network Station hardware and kernel preferences.

The administrator should use this file to specify parameters that will override those specified in the defaults.nsm file, rather than modify the defaults.nsm file (which should be accessed only by the Network Station Manager). In this way, the defaults.nsm file is protected and the administrator's changes are kept in a separate file.

For example, suppose that you want to enable the console on the Network Station so that all options are enabled for the user. The console is a Network Station utility panel from which Network Station services can be initialized by the user. By default, some options on the console are greyed out to prevent access by the user. To enable these options, you can specify the following in the defaults.dft file:

```
set xserver-initial-x-resources = "ncdconsole.disableReboot: false\n\
ncdconsole.disableLoginMenu: false\n\
ncdconsole.disableTerminalMenu: false\n\
ncdconsole.disableSetupMenu: false"
set exec-disabled-commands = {
#   { login }
#   { logout }
#   { serial }
#   { dialer }
#   { quicksetup }
#   { setup }
```

```
# { pref }  
}
```

In the first four lines above, setting the value to false enables the corresponding pull-down menu on the console; and in the lines that follow these, the # makes the corresponding line a comment, which is equivalent to enabling the command.

These options then override what is specified in required.nsm and defaults.nsm files, since the defaults.dft file is normally read after the required.nsm file.

## 5.1.2 Workstation Level Configuration Files

Configuration files at the workstation level are Network Station unit specific. These files are read at boot time and at logout time, provided that they have been enabled for reading by the Network Station.

They reside in /nstation/configs, along with other configuration files; they are created (all three files) by the Network Station Manager at any time that the administrator uses the NSM to make a setting for a particular workstation. The files are:

- hostname
- hostname.nst
- hostname.trm

**Note:** Creating these files using Network Station Manager does not mean that they are enabled and that they will be read at boot time by the Network Station. Other configuration parameters must be specified to indicate that these workstation-specific files should be used, as described below.

### Reading the hostname file

It is possible to specify an initial configuration file (that is, the first file to be read at boot time) based on the unit name of an individual IBM Network Station. In order for this to work, the unit name of the IBM Network Station must be set in the DHCP configuration. If you are using Domain Name Servers (DNS), the Network Station can obtain its host name from a DNS server by supplying the DNS server with an IP address and getting a name back (This is called a RARP or Reverse Address Resolution Protocol).

To activate this feature, set the following parameter in defaults.dft:

```
set unit-query-for-name-at-boot = tcpip
```

It is this statement which causes the Network Station to do a RARP and to then use this name as the name of the initial configuration file to read (instead of the normal standard.nsm).

A short description of each file follows.

#### hostname

##### CREATE & MODIFY USING NSM

This file is a Network Station unit-specific (as opposed to general) initial configuration file. Its role is to call other Network Station configuration files in the correct sequence, supplying specific parameters for the unit named "hostname". The file is created by the

Network Station Manager when the administrator changes values by choosing **Hardware→Workstation defaults**

#### **hostname.nst**

##### **CREATE & MODIFY USING NSM**

This file contains administrator-supplied values for configurable Network Station hardware preferences for the Network Station named "hostname". This file is created by the Network Station Manager when the administrator changes values in **Hardware→Workstation defaults**. This file contains the actual instructions for setting the hardware preferences.

#### **hostname.nsm**

##### **MODIFY MANUALLY**

This file is created by the NSM along with the two previous ones. It is initially empty, and it should be used by the administrator to include parameters to override those in the hostname.nst file. This follows the same principle as the other files, where one file is dedicated to the parameters that are updated by the Network Station Manager and another which is reserved for the administrator to manually add parameters that are destined to override previous settings or simply be new additional settings.

### **5.1.3 User Level Configuration Files**

Configuration files at the user level contain parameters that define user-specific hardware preferences. These files are read at user login time. They are configured via the Network Station Manager or created manually by an administrator and reside in /nstation/userdata/userxxx/, where "userxxx" refers to a specific, defined user. These files are:

- userxxx.nsu
- userxxx.usr

A short description of each file follows:

#### **userxxx.nsu**

##### **CREATE AND MODIFY USING NSM**

This file contains values for configurable Network Station hardware preferences for the user named "userxxx". The file is a user-specific login configuration file, and is created by the Network Station Manager when the administrator or the user changes values by clicking on **Hardware→User defaults** or **Internet→User defaults** or **Applet viewer→User defaults**.

#### **userxxx.usr**

##### **MODIFY MANUALLY**

Special, manually updated file containing configurable hardware preferences for the user named "userxxx". It is created by the NSM initially, but with no content. It is to be used by the administrator to add settings or to override previous settings made in the "userxxx.nsu" by the NSM.

### 5.1.4 The Three Levels of Configuration Files

The following table summarizes the three levels of configuration files and indicates the recommended method to be used for modification.

Table 2. Configuration Files			
File Name	Do NOT Modify	NSM Created and/or Modified	Admin Modified
Global level /nstation/configs/			
standard.nsm	x		
required.nsm	x		
control.nsm	x		
defaults.nsm		x	
defaults.dft			x
WorkStation level /nstation/configs/			
hostname		x	
hostname.nst		x	
hostname.trm			x
User level /nstation/UserData/userxxx/			
userxxx.nsu		x	
userxxx.usr			x

As a reminder, notice that for each level, there is one (or more) files which are used and controlled by the Network Station Manager, which we recommend that no one should alter manually.

If additional configuration parameters are required, they should be manually inserted in the file reserved for the administrator. This can be necessary if there is a need for a parameter which is not supported by the GUI of the Network Station Manager, or if there is a need to override the value specified by the Network Station Manager.

With this arrangement, we are making sure that the files used by the Network Station Manager are not contaminated by errors that the administrator might introduce by attempting to manually update the file, and we are also isolating all the custom changes so that they can easily be identified.

**Note:** This arrangement also makes it very easy to remove any custom changes, in a problem determination effort for example, by simply removing the read statement for the custom files. This way, the Network Station can be booted with only the IBM-supplied files.

### 5.1.5 Configuration Files Used at Boot and Log Out - Read Order

At boot time, the kernel requests that the default configuration files be processed. The name of the initial requested file, by default, is standard.nsm, but several configuration switches allow the unit to also search for files named after the MAC address, the IP address or the unit name for example.

The unit name is defined in the DHCP configuration files. The Network Station may take advantage of this capability and use the file called "hostname" as the first search file.

The hostname file simply contains read directives that cause the imbedding of three other files. These imbedded files may, in turn, have read directives. The normal read order is shown here:

1. Hostname (if present)
2. Standard.nsm
  - a. required.nsm
  - b. control.nsm
  - c. hosts.nsm
  - d. defaults.nsm
  - e. defaults.dft
3. hostname.nst
4. hostname.trm

**Note:** The read order is important because each parameter setting supersedes any previously set parameters. If duplicate values are specified in subsequent files, the last value specified takes effect. This is different from the startup.nsm files, described in the next section, where the effect of certain parameters is cumulative.

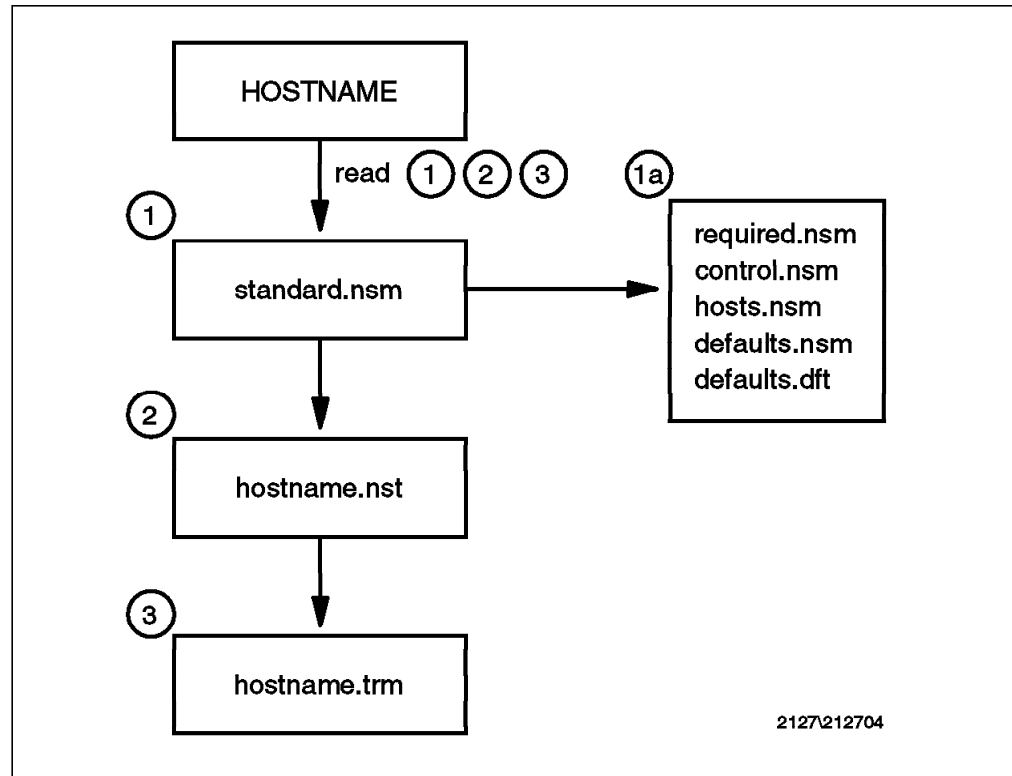


Figure 21. Configuration Files at Boot and Log Out - Read Order

The sample (partial) log file below is an example of a log created when we logged a user off of their Network Station session. Notice that the station re-reads its configuration files at that time. The log shows that one of these files, the hosts.nsm file, could not be read; in this case, the file was simply not there because it was not required. This is not a severe error.

This log was captured by telnetting to port 5998 of the Network Station. See Chapter 12, "Problem Determination - Tools, Tips and Techniques" on page 159 for additional details on using this function.

```
%CONFIGD-I-READ, reading config file: /nstation/configs/standard.nsm
%CONFIGD-I-READ, reading config file: /nstation/configs/required.nsm
%CONFIGD-I-READ, reading config file: /nstation/configs/control.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
```

---

## 5.2 Startup Files

When a user logs in, the system needs to know which applications to start, which menu bar options to set as well as which preferences this user has (such as the background bitmap and color for example).

This information is retrieved from user-specific configuration files and startup files.

There are two user-specific configuration files; they are:

- \nstation\userdata\userxxx.nsu
- \nstation\userdata\userxxx.usr

where userxxx represents the user ID of a user. There are three levels of startup.nsm files:

- IBM level - IBM-supplied - applies to all users
- System level - enterprisewide - applies to all users
- User level - applies to one specific user

Startup files contain the parameters that define the content of the menu bar as well as specify which applications should be started at login time. These startup files are read at user login time. They reside in separate directories, enabling them to have the same name. The startup.nsm files are found in the following directories:

- IBM level - /nstation/ProdData/SysDef/startup.nsm
- System level - /nstation/UserData/SysDef/startup.nsm
- User level - /nstation/userdata/userxxx/startup.nsm (where userxxx refers to a specific, defined user)

### 5.2.1 Startup Files Used at Login - Read Order

After successfully authenticating a user, the Application Login Utility directs the user-specific configuration file "userxxx.nsu" to be read, followed by the userxxx.usr file, and the three startup files, as illustrated below:



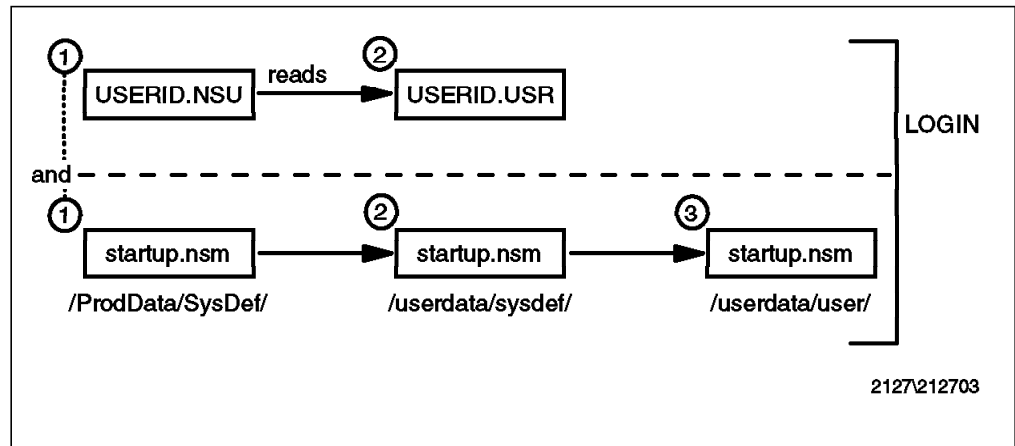


Figure 22. Startup Files at Login - Read Order

The utility reads and interprets the three startup.nsm files in the following order:

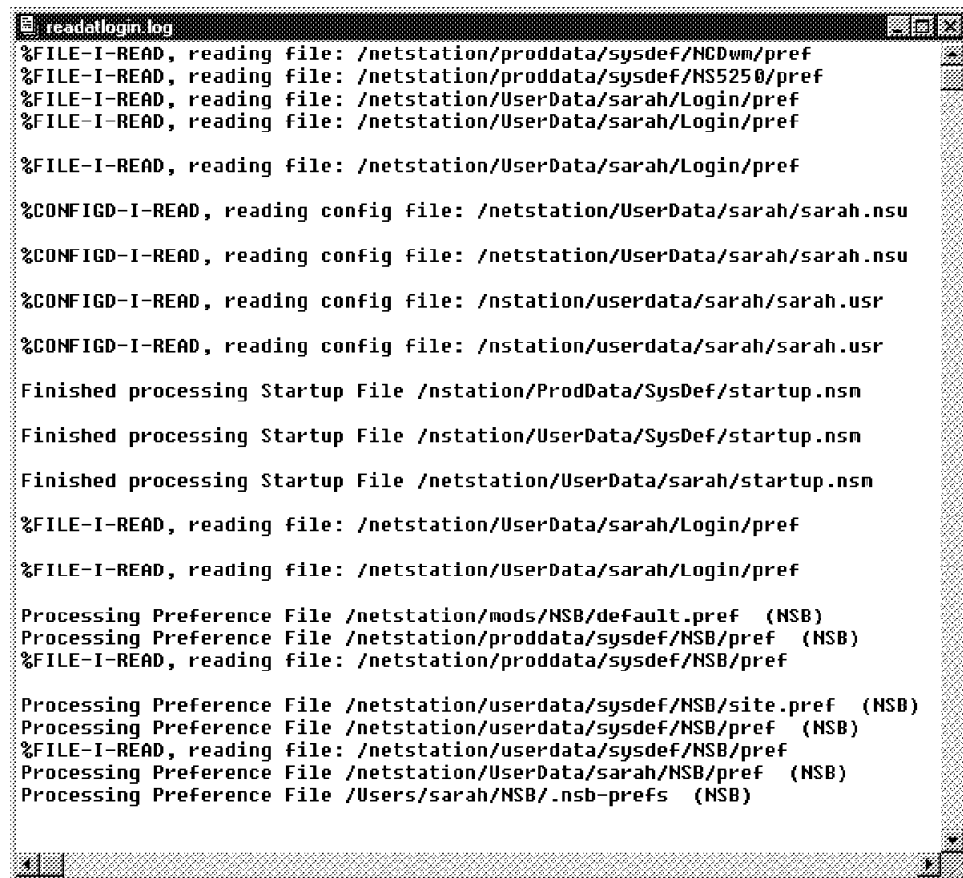
1. Read the /ProdData/sysdef/startup.nsm file
2. Read the /UserData/sysdef/startup.nsm file
3. Read the /UserData/userxx/startup.nsm file

creating the menu bar and starting any specified applications.

Note that the startup.nsm MENUITEM parameters are cumulative; therefore, the menu bar contains the sum of all the entries specified in the three startup.nsm files.

The startup files are modified using the Network Station Manager, or, if necessary, manually by an administrator.

The next figure is an example of a log created when a user called sarah does a logon to a Network Station session. Notice the startup and application preference files that are read.



```
readatlogin.log
%FILE-I-READ, reading file: /netstation/proddata/sysdef/MCDwm/pref
%FILE-I-READ, reading file: /netstation/proddata/sysdef/NS5250/pref
%FILE-I-READ, reading file: /netstation/UserData/sarah/Login/pref
%FILE-I-READ, reading file: /netstation/UserData/sarah/Login/pref

%CONFIGD-I-READ, reading config file: /netstation/UserData/sarah/sarah.nsu
%CONFIGD-I-READ, reading config file: /netstation/UserData/sarah/sarah.nsu
%CONFIGD-I-READ, reading config file: /nstation/userdata/sarah/sarah.usr
%CONFIGD-I-READ, reading config file: /nstation/userdata/sarah/sarah.usr

Finished processing Startup File /nstation/ProdData/SysDef/startup.nsn
Finished processing Startup File /nstation/UserData/SysDef/startup.nsn
Finished processing Startup File /netstation/UserData/sarah/startup.nsn

%FILE-I-READ, reading file: /netstation/UserData/sarah/Login/pref
%FILE-I-READ, reading file: /netstation/UserData/sarah/Login/pref

Processing Preference File /netstation/mods/NSB/default.pref (NSB)
Processing Preference File /netstation/proddata/sysdef/NSB/pref (NSB)
%FILE-I-READ, reading file: /netstation/proddata/sysdef/NSB/pref

Processing Preference File /netstation/userdata/sysdef/NSB/site.pref (NSB)
Processing Preference File /netstation/userdata/sysdef/NSB/pref (NSB)
%FILE-I-READ, reading file: /netstation/userdata/sysdef/NSB/pref
Processing Preference File /netstation/UserData/sarah/NSB/pref (NSB)
Processing Preference File /Users/sarah/NSB/.nsb-prefs (NSB)
```

Figure 23. Log In - Excerpts from Network Station Message Log

## 5.2.2 The Menu Bar Items and Startup Programs

The startup.nsm files define which items appear on the menu bar as well as what programs start automatically when a specific user does a login on the Network Station.

Along with startup programs and menu bar items, other statements are found in the startup.nsm files. These statements, such as the SET command, define parameters for the user session. For example, there are SET statements specific to the INTERNET settings, which are updated by the Network Station Manager.

A value specified in a SET statement is overwritten by subsequent SET statements for the same parameter so that the read order is important for these parameters (as opposed to MENUITEM commands, which are cumulative).

### IBM-Provided Menu Bar Defaults

The IBM shipped menu bar defaults cannot be changed with the NSM. If you must change these default values, you need to manually edit the /nstation/ProdData/sysdef/startup.nsm file.

### Modifying the Menu Bar for System-Wide Preferences

You should not edit the /nstation/ProdData/SysDef/startup.nsm file to change the menu bar for all users. Rather, if you want to impose systemwide changes, use the NSM to configure system startup parameters, or, carefully edit the startup.nsm file found in /nstation/UserData/SysDef.

The following three figures show the three startup.nsm files:

- The IBM-level startup.nsm file contains IBM-shipped values and should *not* be manually modified.

The MENUITEM command defines application buttons that will appear on the menu bar. For example, the first MENUITEM here assigns the label "5250" to this menu item; this is the text that appears on the menu button on the menu bar. The ns5250 is the actual command that gets executed when the user clicks on the button. In this case, this causes the module called ns5250.nws to be fetched from the /nstation/mods directory on the server.

The RUN command autostarts an application. In this example, the RUN wm command starts the Window Manager on the Network Station.

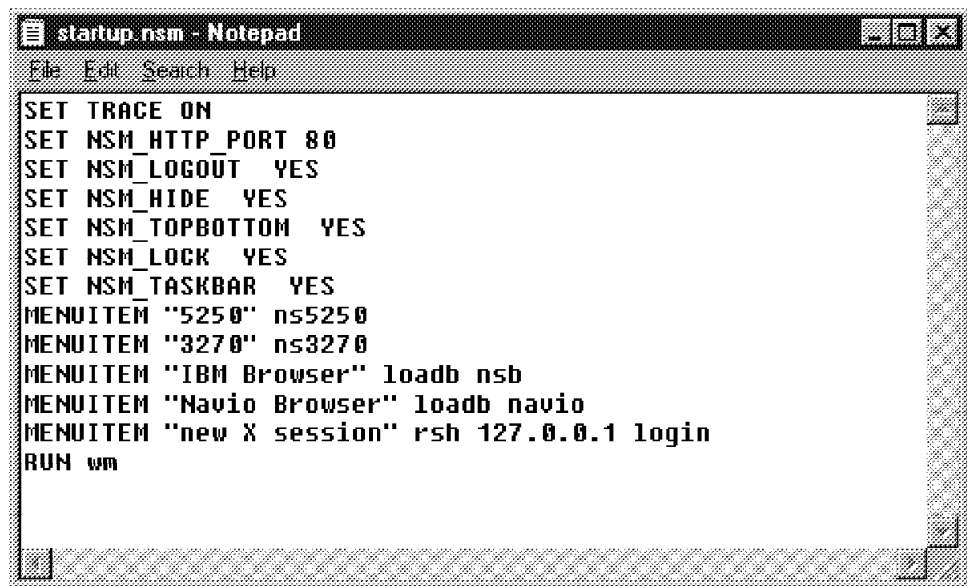


Figure 24. IBM Level Startup File

- The system-level startup file first sources the IBM startup file. The system level startup.nsm is where you specify enterprise-specific options for your menu bar, for your variables and for any program you wish to autostart.

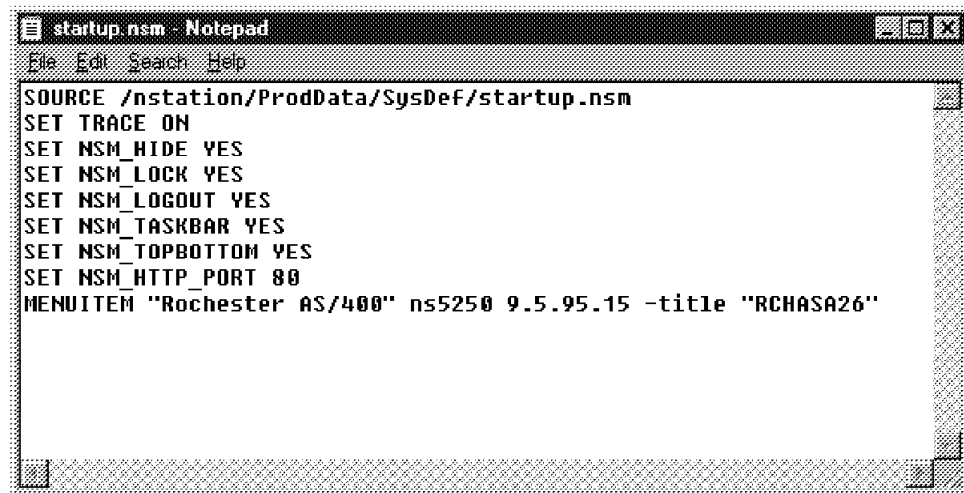


Figure 25. System Level Startup File

- The user-level startup.nsm file contains user-specific variables, menu bar items and autostart programs.



Figure 26. User Level Startup File

Notice, on the menu bar below, that the items shown are the sum of all MENUITEM statements present in all three startup.nsm files.



Figure 27. Sample Menu Bar

## 5.3 Application Preference Files

The application preference files allow system administrators and/or users to customize application resources.

Preferences can be set for the native Network Station applications. The native Network Station applications include:

- Window Manager

- 3270 Emulator
- 5250 Emulator
- IBM Network Station Browser
- Navio NC Browser

There is a hierarchy of four preference files, which are read in order, each of which provides more specific overrides. The first is shipped with the product, and the other three are set by the Network Station Manager as a result of running NSM to set preferences for the system and for users.

For each level and application, there is a single file named `pref` which contains the preferences. These files are kept in separate subdirectories and are interpreted upon the launch of an application.

#### Application Directory Names

In the table below, "applicationxx" refers to one of the specific Network Station applications, such as:

- NCDwm
- NS3270
- NS5250
- nsb
- nav

The subdirectories where the preference files are located are summarized below:

Table 3. Preference Files		
Path/File Name	Created by	Modifiable
/mods/applicationxx/pref	Written at install of the browser	Static - Do not modify
/ProdData/Sysdef/applicationxx/pref	Written at install of NSM	Static - Do not modify
/userdata/sysdef/applicationxx/pref	Written by NSM	Modify using NSM
/userdata/userxx/applicationxx/pref	Written by NSM	Modify using NSM

**Note:** Regarding the Network Station browser's preferences, you may notice preference-related files under the `/users/userxx/nav` or `/users/userxx/nsb` directories.

These directories are created when a user first invokes one of the browsers. The `/users` directory is exported in the `/ibmtcpip/etc/exports` file to allow the users to update preferences at his/her own user level from the browser pull-downs.

The preference files contain options specified using the browser itself, not options specified via the Network Station Manager configuration tool.

The files are named:

- `preferences` - For the Navio browser
- `.nsb-pref` - For the IBM Network Station browser



---

## Chapter 6. Understanding Dynamic Host Configuration Protocol (DHCP)

DHCP is a method by which an IP host (any machine which is IP capable) can obtain its IP address from a server on the network.

Normally, an IP host is configured by the user or by an administrator with a specific address, usually determined by the physical location where the user attaches his IP host to the network.

However, as users are becoming more mobile these days, and are taking 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 to use for the duration of the connection.

This is what DHCP is designed to do, and therefore, since an IBM Network Station is an IP host, it can be configured to dynamically request an IP address from a DHCP server instead of using a pre-configured fixed IP address.

This chapter therefore describes how a boot server can also be configured to function as a DHCP server for a network of IBM Network Stations.

---

### 6.1 Booting the Network Station

The operating system (kernel) is loaded into the Network Station's memory at boot time by a program called the boot monitor program, which resides in the Network Station's programmable read-only memory.

In order to load the kernel, the address of a boot host or boot server must be available to the Network Station's boot monitor program. In addition to obtaining the boot host's IP address, the Network Station must obtain its own, unique IP address in order to participate on the network, since it uses the IP protocol in order to load all of its required software and configuration.

These required addresses are obtained either by an administrator manually entering static definitions in the Network Station's NVRAM, or by the Network Station broadcasting a request on the network (to a BOOTP or DHCP server).

If one chooses to set these addresses in the Network Station's NVRAM, it requires that each Network Station be configured manually by an administrator. However, if one chooses to use a boot protocol such as BOOTP or DHCP, these addresses are then obtained from a BOOTP or DHCP server on the network.

---

### 6.2 Network Protocols

Network Protocols, such as BOOTP and DHCP allow IP information to be provided through the network. These protocols assume that the only information that a Network Station needs to provide to a BOOTP or DHCP server is the MAC address of its network adapter.

They assume that the rest of the information needed by the Network Station to download the kernel (operating system) is provided by the server.

The server has a process for each protocol. The process receives a MAC address and uses it as a search argument in a database to locate an entry that matches the MAC address. From the Network Stations' point of view, the protocols differ mainly in the amount and type of information that can be provided by the server to a client. The protocol capabilities are summarized below:

<i>Table 4. BOOTP &amp; DHCP Capabilities</i>		
Information	BOOTP	DHCP
Network Station IP address	Returned. Fixed	Returned. Can be dynamically set via address pool
Server IP address	Returned	Returned
Boot file name	Returned	Returned
Boot file path	Returned	Returned
Other options	Not available	Available

The DHCP protocol is more flexible because it has all of the BOOTP capabilities, in addition to being able to assign addresses dynamically from a pool of addresses and being able to return more information to the client.

## 6.3 DHCP vs BOOTP

The choice between BOOTP and DHCP depends on the use of your Network Station and which method of assigning IP addresses works best for your environment. If you want to use a few Network Stations in a small network, BOOTP may be sufficient. For large networks with many Network Stations, DHCP provides a lot more flexibility for dynamic management of the IP addresses. The following section describes the differences in more details.

### **DHCP is the choice on the NT platform**

Note that the IBM TCP/IP Services supplied with the version of the IBM Network Station Manager include a DHCP server (and not a BOOTP server) as the server of choice for the Windows NT 4.0 platform. This DHCP server is able, however, to receive and service BOOTP client requests, if necessary.

### 6.3.1 Dynamic IP Address Allocation

In large network environments, it is important to have a mechanism for assigning IP addresses to Network Stations automatically. DHCP is designed to solve this problem; it can assign either a permanent IP address or a dynamic IP address for every host or Network Station within a range of predetermined IP addresses.

The static assignment is similar to BOOTP. The MAC address of every potential Network Station is defined in the DHCP server configuration, along with an IP address that is reserved for the station with this MAC address. When the Network 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 Network Station's unique identifier; it is either hardcoded in the network adapter, or it can be configured by an administrator. The MAC address of your Network Station is displayed during the power on phase, or is available from the Network Station console if you select **Statistics**→**Show Version** from the console menu bar.

For dynamic IP assignment, the DHCP server is configured with a pool of available IP addresses; when it receives a client's request, it still identifies 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 might be 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.

With BOOTP, only static assignment can be used, which makes it necessary to register every Network Station's MAC and does not allow the re-use of IP addresses. 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 needs it.

### 6.3.2 Helpful Documentation

We summarize here only the most important aspects of DHCP. In order to get additional detailed information, there are, in the \ibmtcpip\help folder, a few HTML files that provide an excellent documentation on DHCP and TCP/IP. These files are:

- dhsamst.htm - DHCP Server Administration

This contains an overview of dynamic IP, DHCP and Dynamic Domain Name System (DDNS) servers, how DHCP clients obtain configuration information, how to plan, set up and start a DHCP environment. There is also information on how to modify the DHCP configuration file (DHCPD.CFG) as well as what DHCP options can be specified. An example of a DHCP configuration file is provided.

- dhscmst.htm - IBM DHCP Server Configuration Program

This contains information on creating and modifying DHCP configurations.

- dipamst.htm - DHCP & Dynamic IP Introduction

This is an introduction to DHCP and Dynamic IP, and information on automating IP network access and how to distribute customized sets of options to clients. This text also provides information on the major components in a Dynamic IP network. It helps to understand the use of single and multiple DHCP servers.

The easiest way to view these help files is to open the Windows NT Explorer, select the \ibmtcpip\help folder and double click on the file you wish to view,

which launches your default Web browser. For example, to open the DHCP Server Administration help file, click on **Start→Programs→Windows NT Explorer→**. Select the drive on which the Network Station Manager Support is installed, double click the **ibmtcpip** folder, double click on the **help** folder, select **dhsamst.htm** and double click to launch the browser.

---

## 6.4 Boot Sequence - How Information Is Obtained via DHCP

As discussed previously, clients obtain their IP addresses and configuration information through DHCP requests. Here is a short description of the different types of DHCP requests and how they work.

We provide this description as it may be of help when doing problem determination and tracing frames between the Network Station and the DHCP server.

**DHCPDISCOVER:** As a Network Station boots, the boot monitor program reads its configuration information from the Network Station's NVRAM to determine whether to obtain all of its boot information also from NVRAM or from the network by contacting a BOOTP or DHCP server.

If it is told to find information via the network, the Network Station announces its network 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 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 subnet.

**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 which are defined in its configuration files.

The offer includes a client IP address (for the Network Station) and also includes the IP address of itself (the server). Before issuing an offer, the server checks for duplicate addresses on the network and it checks the configuration file to see if the assignment 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. 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).

**DHCPREQUEST:** This frame flows from the client to the server, indicating acceptance of a particular offer.

The client can receive offers from many servers. It waits about 4 seconds after the first offer received to wait for other offers. At the end of the time period, the client compares all offers and makes a selection based on which offer is the one that offers all the options that were requested. The client then 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.

It also requests startup information such as the boot file, boot file directory, IP gateway, etc.

**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 acknowledgement 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.

**DHCPDECLINE:** After receiving the DHCPACK, the client determines if 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 illustrates how DHCP information is obtained.

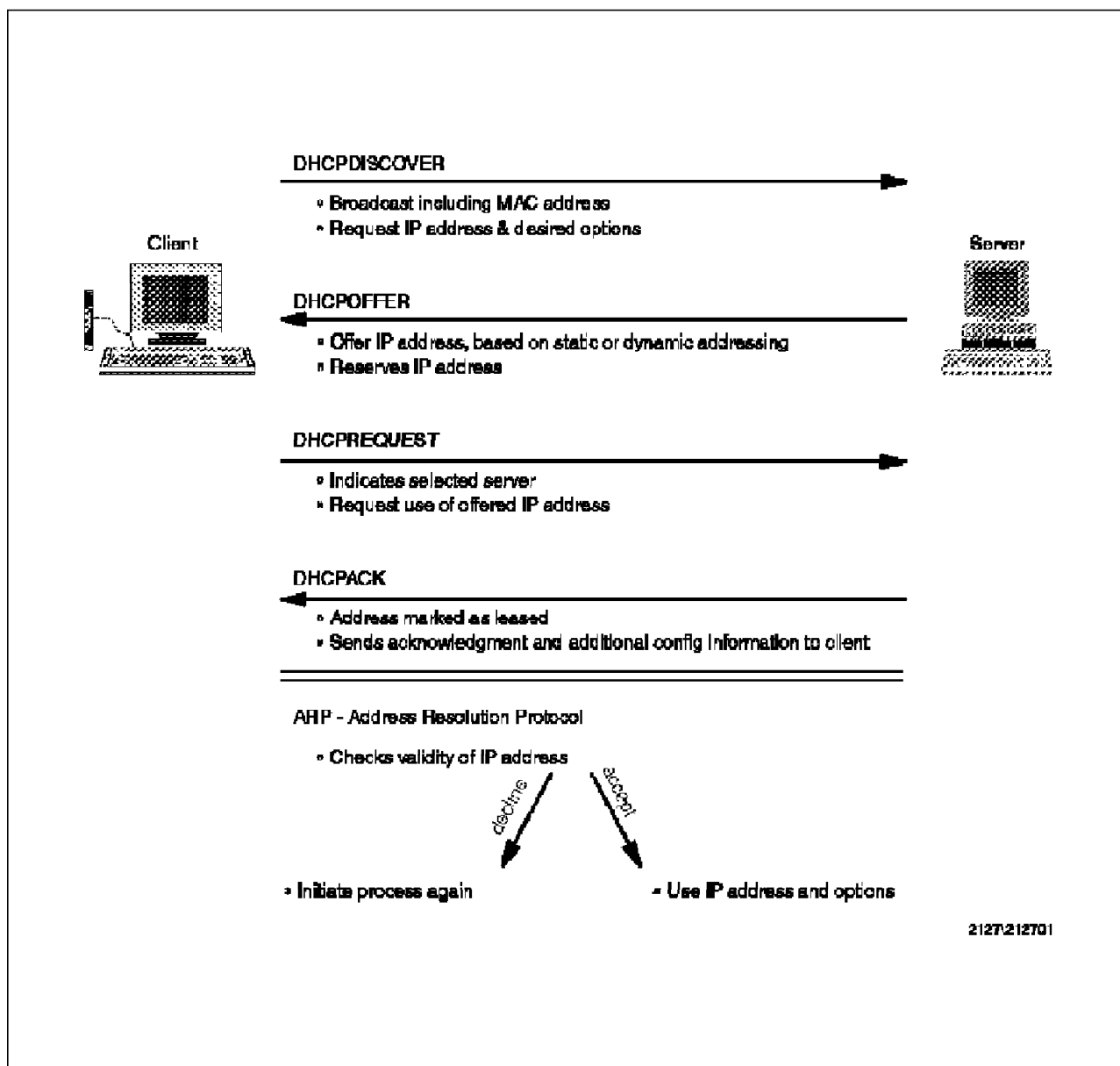


Figure 28. Boot Sequence - How Information Is Obtained via DHCP

## 6.5 The DHCP Server Configuration Program

The DHCP options must be configured to represent your unique TCP/IP network. The `\ibmtcpip\etc\dhcpsd.cfg` file is the main configuration file where configuration information regarding the DHCP server and clients is stored. A Graphical User Interface (GUI) is provided for configuring the file and is referred to as the DHCP Server Configuration program.

The configuration file is like a "map" of your network. Within this file, you create a hierarchy of configuration parameters for the network by specifying values that are served globally to all clients, while other values are specific only to certain clients.

For example, say that the network mask you use is 255.255.255.0 for all subnetworks and all clients in the network. The network mask is DHCP Option 1 (all parameters have been assigned a DHCP option number and the network mask happens to be number 1, whereas default router for example is DHCP Option 3). Rather than redefining Option 1 on all subnets and all clients, you define it once at the global level, and it then applies to all subnets and all clients. This is what is meant by a hierarchy of configuration parameters.

To configure your DHCP Server, use the DHCP Server Configuration program. To access the configuration program, click on: **Start→Programs→Network Station Manager TCP/IP→Configuration Utility**.

#### Multiple Instances

Note that if for some reason, the DHCP Configuration Utility is abnormally ended, it may leave some registry entries that may prevent you from starting it again.

If you get a message saying that multiple instances of the Configuration Utility cannot be run, use the TCPCFG command from a command line to start the utility, and specify the -F parameter (tcpcfg -f). This clears the unwanted registry entries and allow you to start the configuration tool.

### 6.5.1 Configuring Your Environment

From the DHCP tab of the Network Station Manager TCP/IP Configuration window, select **Launch** to launch the DHCP Server Configuration program.

#### Launch and DHCP configuration file name

The name specified in the DHCP configuration file name field is the default name of the DHCP configuration file and *not* the file that you are launching.

This may be a bit confusing because the Launch button and this filename appear in the same box labeled DHCP configuration.

The Launch button means only that you are launching or starting the configuration GUI tool, and not that you are opening this file. Once the GUI is launched, you choose the configuration file to be opened by using the file pull-down and choosing a 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 the one that appears in the DHCP configuration file name field under the Launch button.

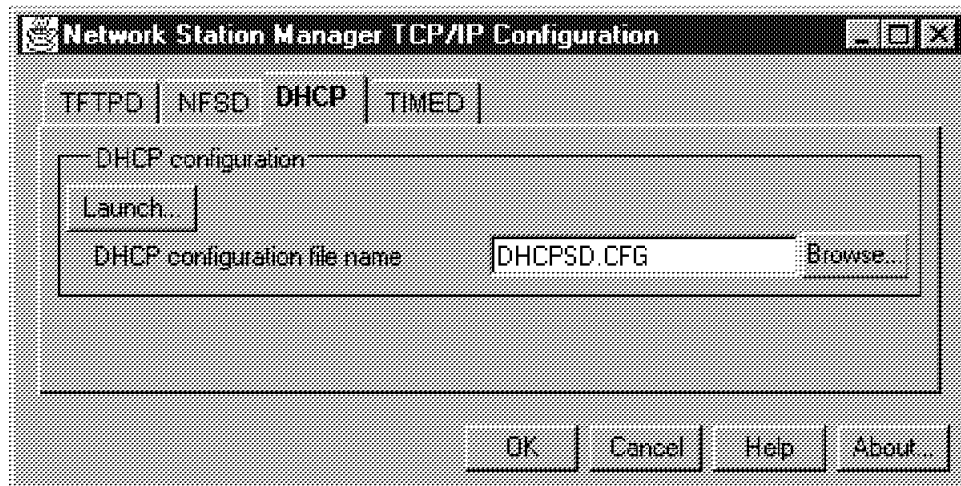


Figure 29. Launch the Configuration Tool

The following figure shows the DHCP Server Configuration GUI. This is where you create/modify your network configuration. In the case of the network shown below, no entries have been made yet; only the server parameters appear as well as the global entry, which is empty for now.

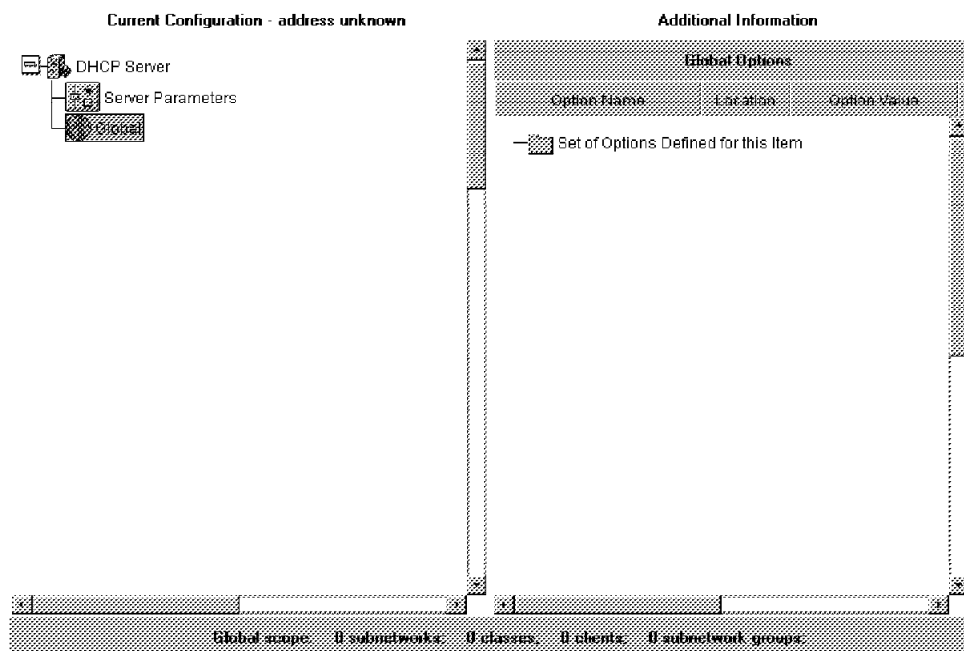


Figure 30. The DHCP Server Configuration GUI

The easiest method to create your own network representation is to load the DHCP.D.CFG file and modify to your own specifications. Select **File→Open** from the DHCP Server Configuration menu bar. Double click on **dhcpsd.cfg** to load the file.

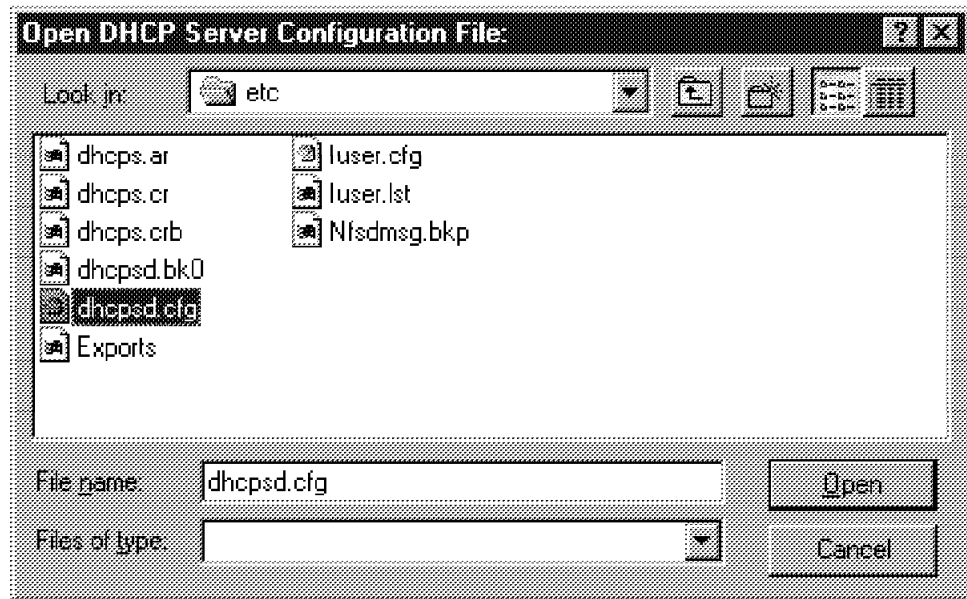


Figure 31. Double-Click on the File DHCP.DCFG to Load

Once you have the dhcpsd.cfg file loaded you may proceed to modify the options to describe your own network structure.

As shown below, the supplied embryonic dhcpsd.cfg file contains a subnet labeled 10.0.0.0 with clients ns1 and ns2.

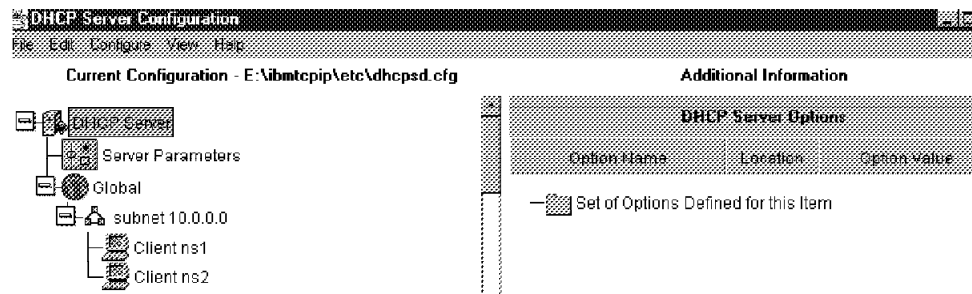


Figure 32. Supplied Sample dhcpsd.cfg Configuration File

The following options are configurable:

- **Server parameters**

Settings for lease periods, logging options, DDNS, and miscellaneous definitions that control the operation of the DHCP server.

- **Global**

Settings that apply to all clients, unless overridden at a subnet, class, or client level. The Global Notebook allows you to exclude addresses, make DDNS and BootP choices, and define DHCP options applicable to all.

- **Subnets**

Definitions of ranges of IP addresses to be leased to clients.

- **Classes**

DHCP options and other definitions served to a group of clients that identify themselves as belonging to a named class or group. All Network Stations by default belong to the "IBM Network Station" vendor class.

- **Clients**

DHCP options served to a particular client uniquely identified by a means such as a MAC address. These clients represent the Network Stations. When requesting a listing of Network Stations via the Network Station Manager tool, these clients appear as selectable entities (provided they have DHCP option 12 defined).

---

## 6.6 A Sample DHCP Configuration

The following discussion takes you through an example of a simple DHCP server configuration. Our objective here is to give you a simple environment that you can emulate to get up and running quickly. More complex configurations can be tackled later on, once the basics have been understood. Our sample environment contains:

- 1 DHCP server
- Token-ring network
- 1 Subnet
- 2 IBM Network Stations
- Two domain name servers

All of these are on the same subnet (subnet 9.24.104.0). This is illustrated in the figure below:

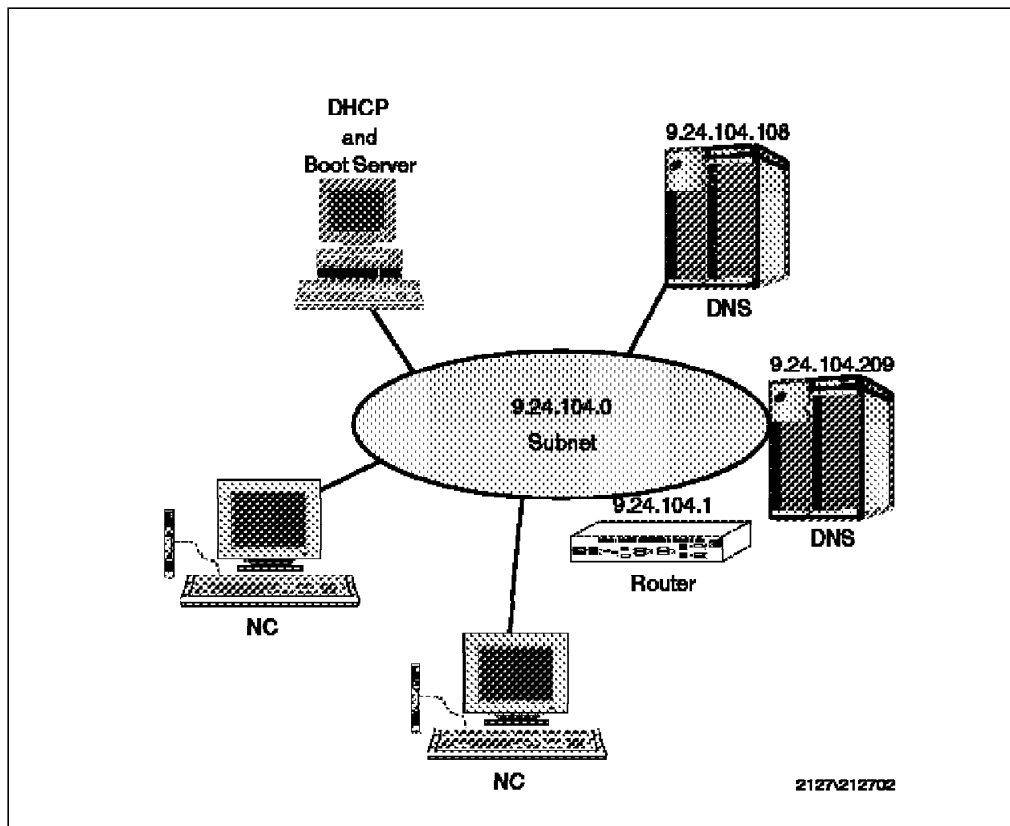


Figure 33. Environment Used for Sample DHCP Configuration



The following information was used. These options are configured at either the global, subnet or client levels.

<i>Table 5. Sample Configuration Values</i>	
Option	Value
Boot File Name	/nstation/kernel
Domain Name	itso.raleigh.ibm.com
DNS Address	9.24.104.108 & 9.24.104.209
Subnet number (subnet address)	9.24.104.0
Subnet mask (option 1)	255.255.255.0
Default Gateway (router) (option 3)	9.24.104.1
Start DHCP Pool Address (IP Range From)	9.24.104.190
Last DHCP Pool Address (IP Range To)	9.24.104.236
Client ID (MAC address)	0000e5686f14
Client ID (MAC address)	0000e5806363

You should configure options at the highest possible level. This is to ease maintenance and administration. Grouping according to similar characteristics at the highest level eases the task of defining the same options for each client. It is also helpful when changes need to be made to the configuration values.

For example, if you need to configure the subnet mask as 255.255.255.0, and you know that all subnets and all clients will use this mask, then it should be defined as a global options which is applicable to all. In this way, this subnet mask option never needs to be defined in any of the other subnet definitions or client definitions.

---

## 6.7 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 **Server Parameters** from the DHCP Server Configuration window. Select **Configure, Modify selected object**. From the DHCP Server Parameter window, select the **Miscellaneous** tab.

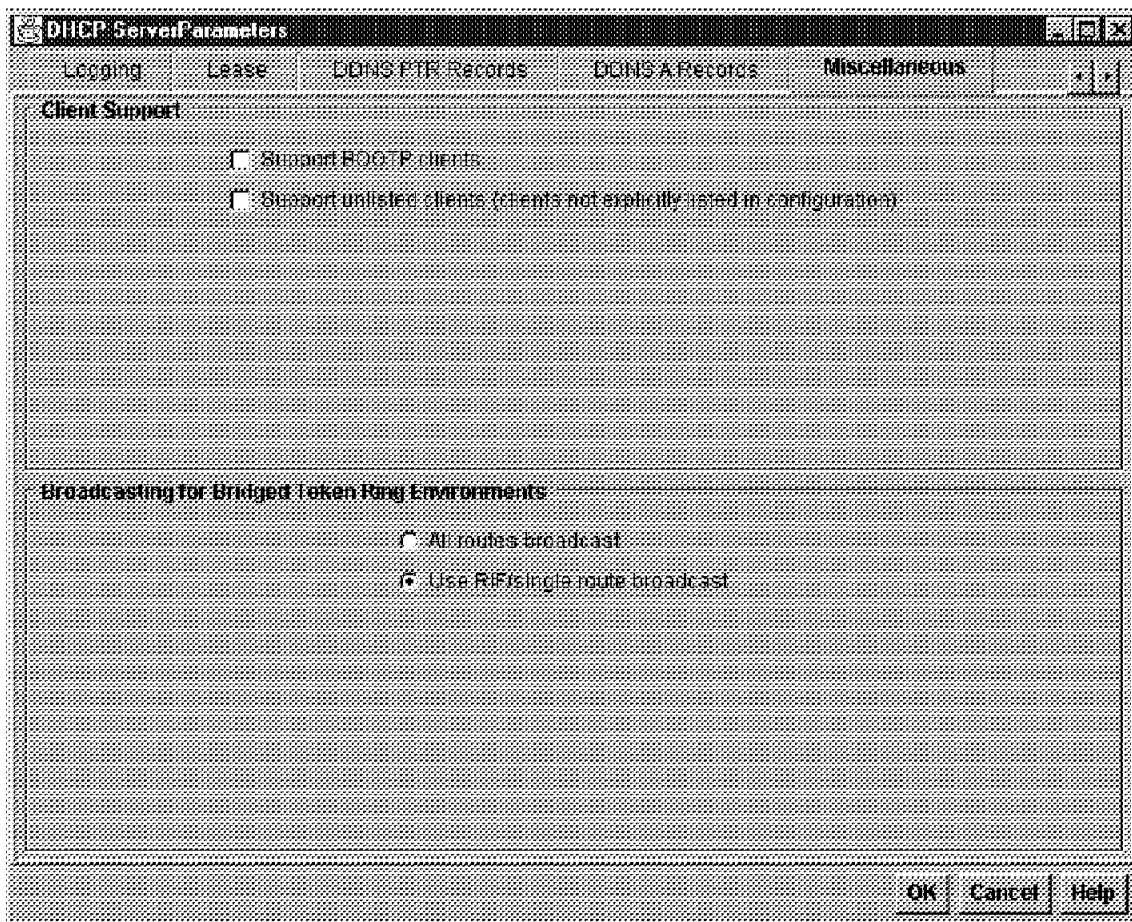


Figure 34. Server Parameter Miscellaneous Tab - Specify Client Support

**Note:** In this example, we are *not* supporting unlisted clients. Rather, we defined our clients as you will see later in this example. If you want to support unlisted clients, check the **Support unlisted clients** box.

### 6.7.1 Global Definitions

To modify the Global options, begin by highlighting **Global** on the DHCP Server Configuration window. From the menu bar select **Configure, 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.

Let's take a look at the structure of the panel below. Anytime you choose to modify an object from the Configure pull-down and select the **DHCP options** tab, you see a panel similar to this.

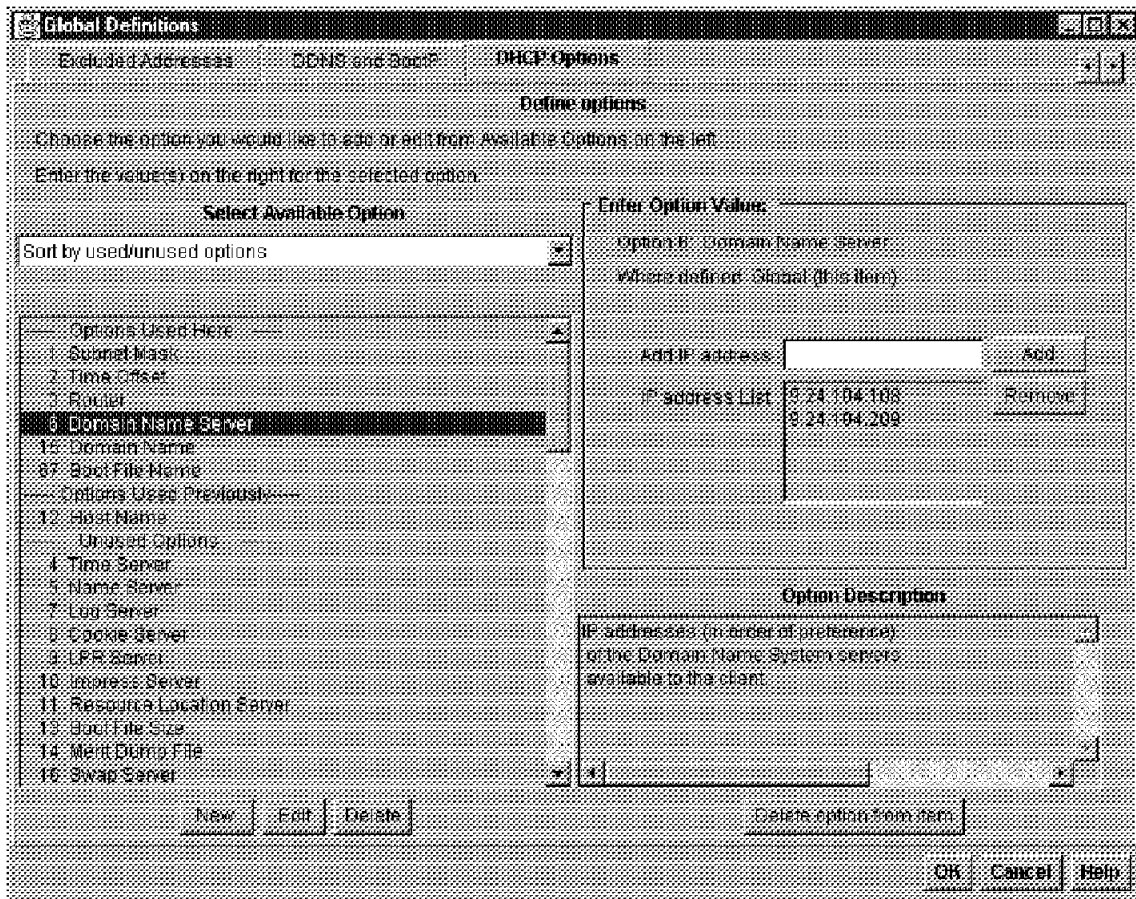


Figure 35. Modifying the Global Settings

The DHCP Options window is divided into several sections:

**Select Available Option:** This section allows you to sort the options list. The options list has all of the DHCP servers configurable options. Each option is associated with a number. This number is used in the configuration file. The options list can be sorted by used/unused options, by used/unused number, by option number or alphabetically.

**Options:** The pane in the bottom left quadrant is the list of configurable options. When the sort is set to used/unused, the options that are defined at the current level (in this case the global level) are displayed first.

**Enter 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, the option has not yet been configured. In this case, we selected Option 6 - Domain Name Server on the left, and on the right appears the current values currently set for this option (9.24.104.108 and 9.24.104.209 in this example).

**Option Description:** This section (bottom right quadrant) gives a short description of the selected option.

#### Our Example-Global Definition

In our illustration, at the global level, we configured:

- boot file name - /nstation/kernel
- subnet mask - 255.255.255.0
- router - 9.24.104.1
- domain name server - 9.24.104.108 and 9.24.104.209
- domain name - itso.raleigh.ibm.com

We configured these options globally, because all levels share these common characteristics.

Select **OK** to return to the main panel.

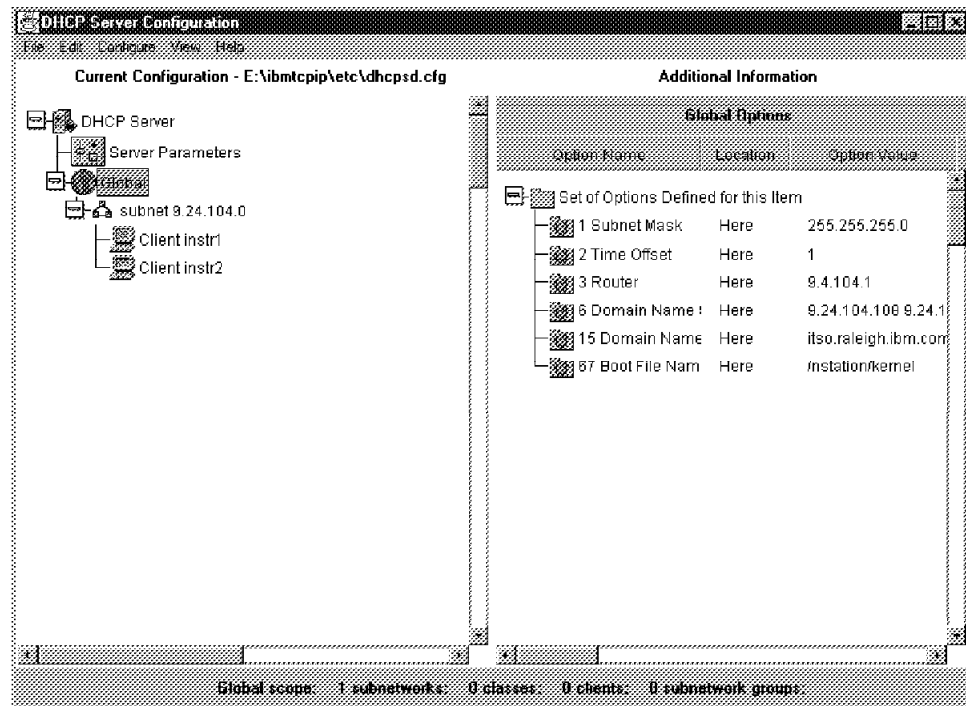


Figure 36. The Main View after Configuring the Global Options

Notice that, on the main panel, the right side now reflects the configuration changes we just made. The Location column lists "Here", indicating that the options listed are defined at the Global level, since this is the level currently selected.

After making modifications, we strongly recommend that you save the new file immediately. Unless you have a machine with a very fast processor, the configuration tool will appear to be very slow (we were using a 486 60Mhz PS/Value Point) and may sometimes hang. So we found that it is best to save after each modification. If the program hangs while attempting to load the notebook, simply close the application and restart the program. To save, select **File**→ **Save** from the DHCP Server Configuration menu bar.

## 6.7.2 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. Select **Configure**→**Modify selected object** from the menu bar.

The screenshot shows the 'Subnet Definition' window with three tabs: 'Subnet Definition', 'DNS and BootP', and 'DHCP Options'. The 'Subnet Definition' tab is active. It contains the following sections:

- Address Range for Subnet:** Fields for 'Subnet name', 'Subnet address' (9.24.104.0), 'Subnet mask' (255.255.255.0), and 'IP address range' (From: 9.24.104.190, To: 9.24.104.236).
- Addresses Excluded from Range:** Fields for 'From' and 'To' with an 'Add' button, and an 'Exclusion list' with a 'Remove' button.
- Lease Time and Comment:** Radio buttons for 'Default lease time: 1 Days', 'Enter a lease time:' (with spinners for Years, Months, Days, Hours, Minutes, Seconds), and 'Permanent lease'. A 'Comment' text area is at the bottom.

Buttons for 'OK', 'Cancel', and 'Help' are at the bottom right.

Figure 37. The Subnet Definition Tab

The Subnet Definition window is divided into three sections:

- Address Range for Subnet

Here is where you can specify the subnet address, and mask, as well as the range of IP address you want to make available within the IP address pool.

- 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.

- Lease Time and Comment

Use this field to set lease characteristics. A lease is the time period during which a client may use an IP address.

### Our Example-Subnet Definition

At the subnet level we configured:

- Subnet address - 9.24.104.0
- Subnet mask - 255.255.255.0
- IP address range - 9.24.104.190 to 9.24.104.236

Select **OK** to update your configuration and return to the main window. Notice that the Additional Information column lists options that are configured. In this case, the subnet options are being provided from the previously configured global options because no options were modified at the subnet level; this is why the Location column shows the word Global.

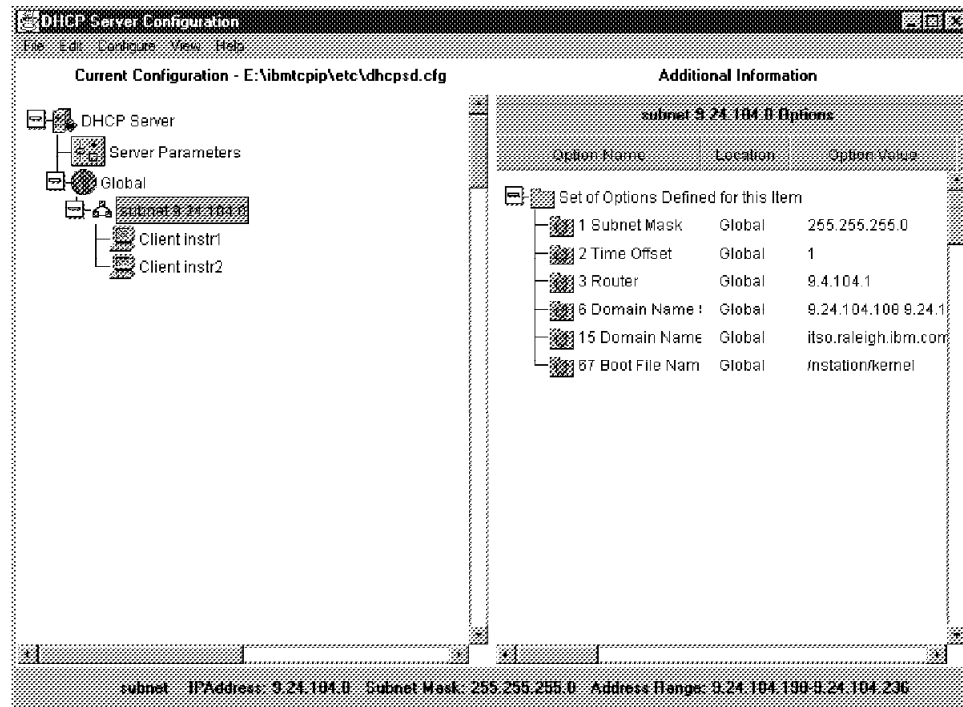


Figure 38. The Main View after Subnet Configuration

### 6.7.3 Client Definition

The next step is to configure specific clients. Each Network Station is a client. To create a new client, select the subnet to which the client belongs, and select **add client** in the configure pull-down. To modify an existing client definition, highlight the client you wish to modify from the DHCP Server Configuration window. From the menu bar select **Configure**→ **Modify selected object**. The Client panel, similar to the one below, appears:

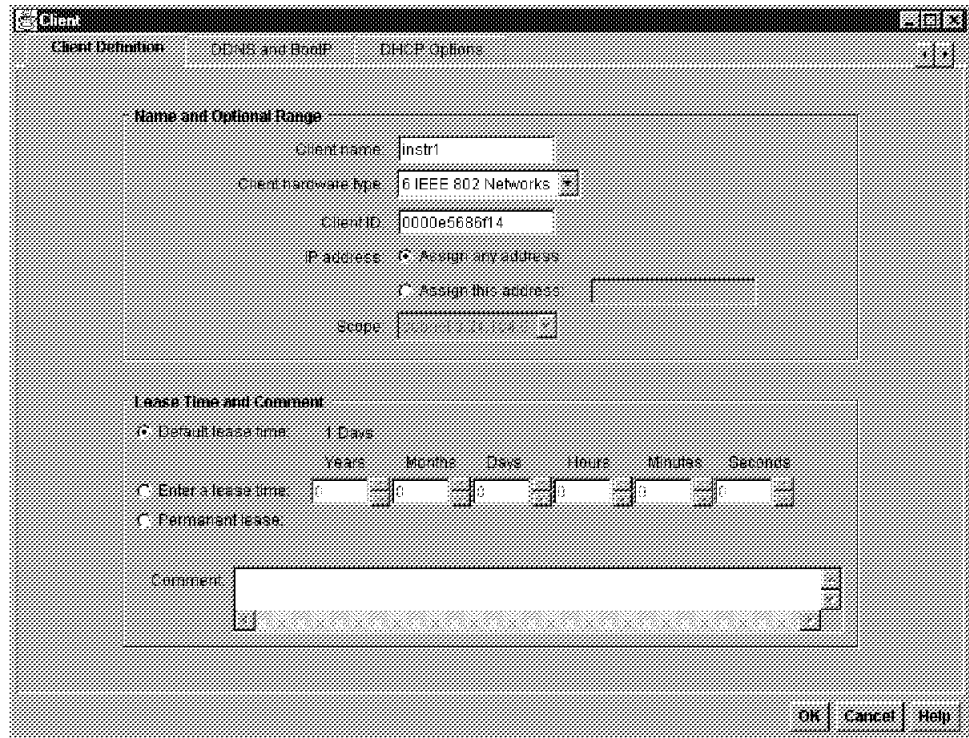


Figure 39. The Client Definition Tab

The Client Definition panel is divided into two sections:

- Name and optional range
- Lease time and comment

Use the Name and Optional Range 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.

- Scope

Clients are defined at either a global or subnet level. In our scenario, our clients are defined at the subnet level.

Use the Lease Time and Comment section to define lease options for a specific client.

### Our Example-Client Definition

In this example, we used:

- Client name - instr2
- Client hardware type - IEEE 802 Network
- Client ID (MAC address) - 0000e5806363
- IP address allocation preference - assign any address

To define options specific to this client, select the **DHCP Options** tab. Select **Host Name** from the options list. Enter the name of the host (your Network Station)

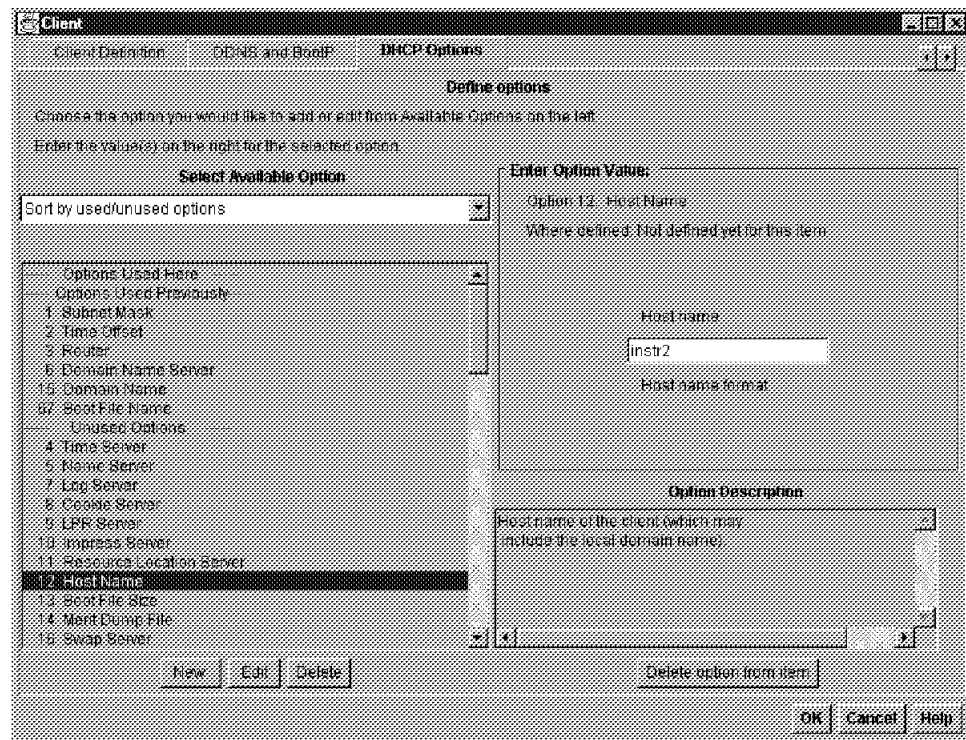


Figure 40. The Client Definition DHCP Options Tab

### Our Example-Client Definition

In this example, we configured the host name as instr2. This name is the name which is used by the Network Station Manager when browsing/listing clients. Note that the host name specified in the OPTIONS list does *not* need to be the same name that you specified in the Client Name field from the Client Definition tab.

Select **OK** to save and return to the main window.

Notice that the Additional Information column has been updated and reflects the client characteristics. In this case, the host name is shown as being defined "HERE", indicating that it is defined at the selected Client level.



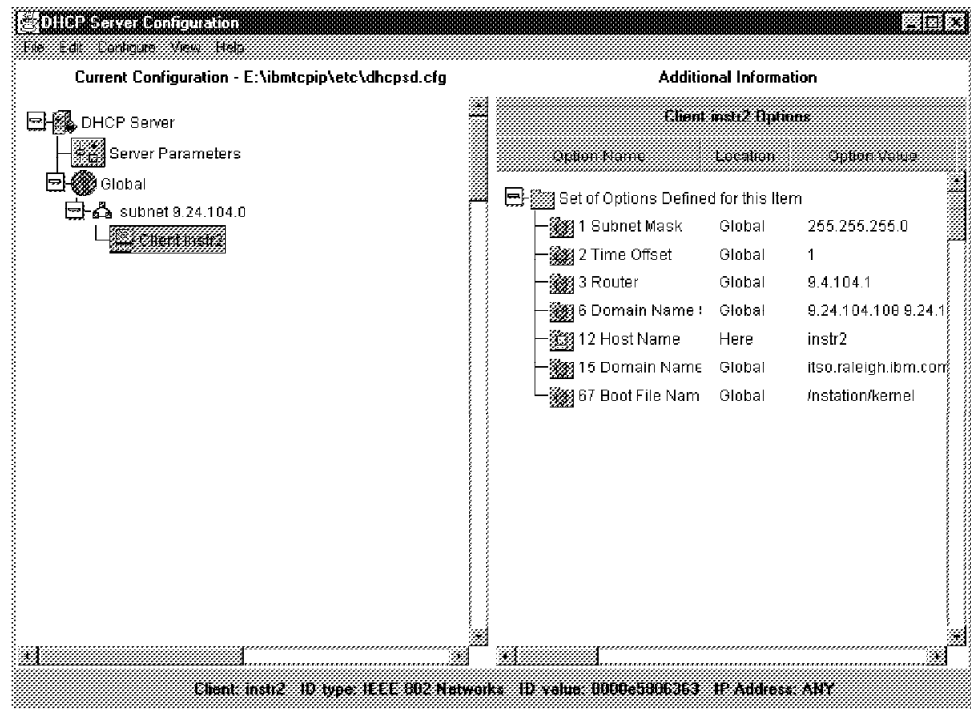
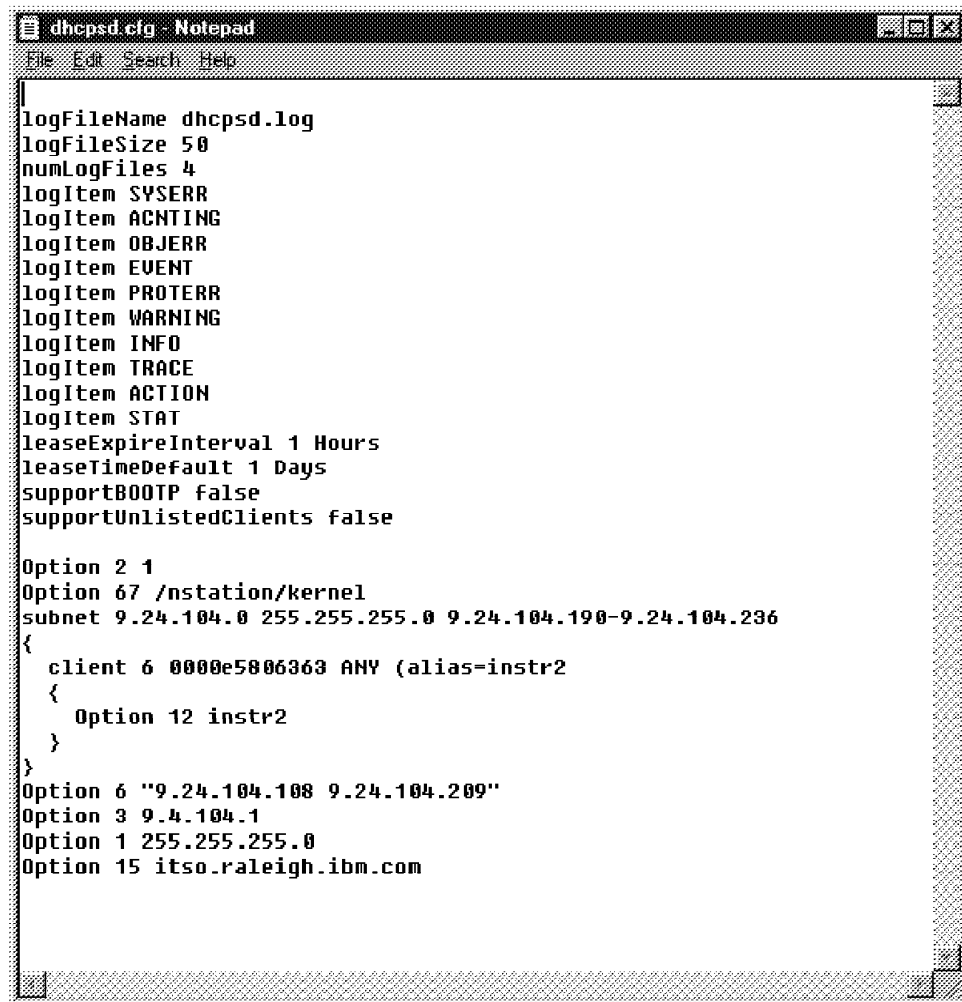


Figure 41. The Main View after Client Configuration

All of the configuration changes and additions are recorded in the `dhcpsd.cfg` file. By default it is located in `/instation/ibmtcpip/etc` subdirectory.

Below is a listing of our `dhcpsd.cfg` file after the changes we made from our sample scenario.



```
dhcpcd.cfg - Notepad
File Edit Search Help

logFileName dhcpcd.log
logFileSize 50
numLogFiles 4
logItem SYSERR
logItem ACNTING
logItem OBJERR
logItem EVENT
logItem PROTERR
logItem WARNING
logItem INFO
logItem TRACE
logItem ACTION
logItem STAT
leaseExpireInterval 1 Hours
leaseTimeDefault 1 Days
supportBOOTP false
supportUnlistedClients false

Option 2 1
Option 67 /nstation/kernel
subnet 9.24.104.0 255.255.255.0 9.24.104.190-9.24.104.236
{
  client 6 0000e5806363 ANY (alias=instr2
  {
    Option 12 instr2
  }
}
Option 6 "9.24.104.108 9.24.104.209"
Option 3 9.4.104.1
Option 1 255.255.255.0
Option 15 itso.raleigh.ibm.com
```

Figure 42. The dhcpcd.cfg File

Notice that DHCP option 2 (which is set to 1) and DHCP option 67 (which is set to /nstation/kernel) are made at the global level. This is true also of options 6, 3, 1, and 15.

Option 12 (set to instr2) is made at the client level, which is under the subnet 9.24.104.0.

Notice as well that we have set the unlisted client support to no (false).

You may manually edit the DHCP configuration file. However, there is more opportunity for error than when you use the GUI, so we recommend that you use the GUI interface whenever possible.

Refer to Appendix A in the dhsamst.htm file in \ibmtcpip\etc for instructions on how to work with the configuration file manually.

## 6.7.4 Problem Solving/Logging

We recommend that you enable DHCP logging, especially in the initial phases of implementation, to help with problem determination.

Logging is configured by selecting **Server Parameters** on the main window, then **Configure**→**Modify selected object**.

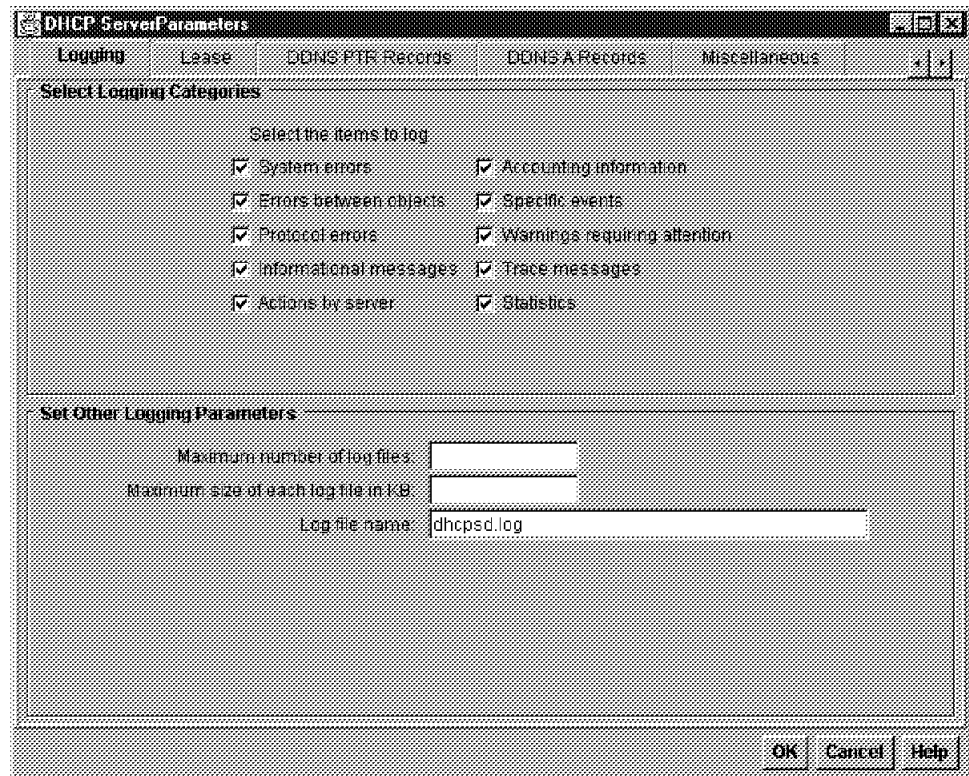


Figure 43. The DHCP Server Parameters Logging Properties

To enable logging by the server, all of the following must be specified:

- Number of DHCP log files

**Notes:**

1. If the value for numLogFiles is 0 or the statement is omitted, no logging occurs.
2. If a new log file is created after the maximum number is reached, the oldest log file is removed.
3. The maximum number of files is specified by the file system.
4. All older files are renamed by incrementing the previously appended integer filetype by 1. For example, DHCPLOG.003 is an older log file than DHCPLOG.001.

- Size of DHCP log files

Maximum log file size in kilobytes. The minimum size is 1 KB.

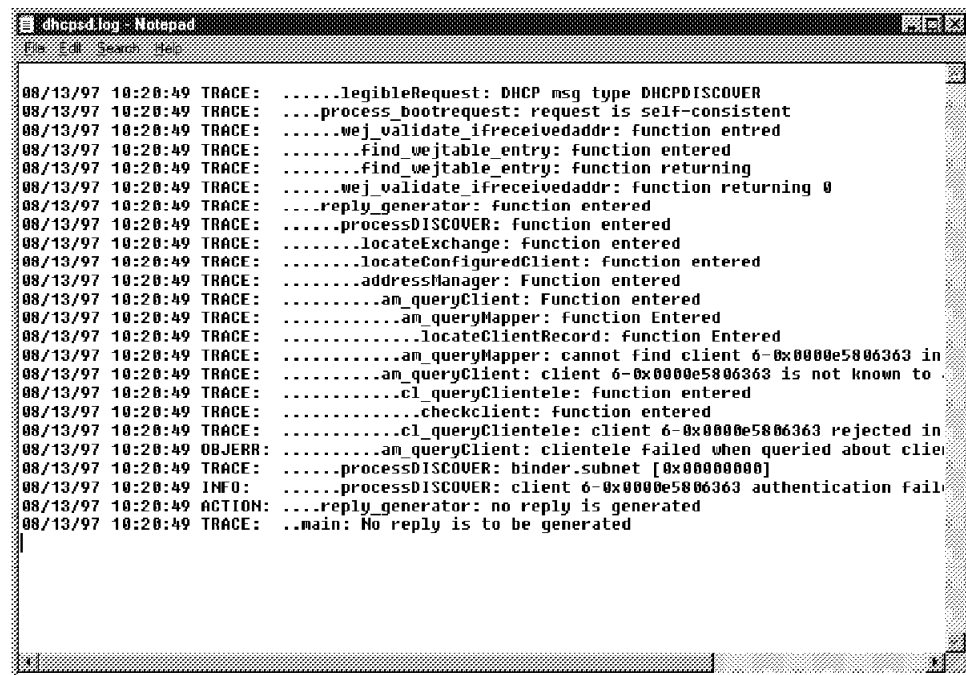
- Names of DHCP log files
- At least one information type to log

Refer to the online documentation for a breakdown of each logging category. This can be found in dhsamst.htm in \ibmtcpip\etc.

If you do not specify a path, the log file will be stored in \winnt\system32\dhcpcd.log. It is probably easier to put this log file in a less crowded subdirectory such as ibmtcpip\etc.

The messages that are logged, especially when tracing, are very detailed and provide a lot of good information to follow how the DHCP server processes incoming requests.

In the example below, where the DHCP server is not configured to support unlisted clients, we see a request coming in from a client with a MAC address of 0000e5806363. The server processes the request, determines that this client is unknown, rejects the request and therefore does not generate a reply.



```
08/13/97 10:20:49 TRACE: .....legibleRequest: DHCP msg type DHCPDISCOVER
08/13/97 10:20:49 TRACE: ....process_bootrequest: request is self-consistent
08/13/97 10:20:49 TRACE: .....wej_validate_ifreceivedaddr: function entered
08/13/97 10:20:49 TRACE: .....find_wejtable_entry: function entered
08/13/97 10:20:49 TRACE: .....find_wejtable_entry: function returning
08/13/97 10:20:49 TRACE: .....wej_validate_ifreceivedaddr: function returning 0
08/13/97 10:20:49 TRACE: ....reply_generator: function entered
08/13/97 10:20:49 TRACE: .....processDISCOVER: function entered
08/13/97 10:20:49 TRACE: .....locateExchange: function entered
08/13/97 10:20:49 TRACE: .....locateConfiguredClient: function entered
08/13/97 10:20:49 TRACE: .....addressManager: Function entered
08/13/97 10:20:49 TRACE: .....am_queryClient: Function entered
08/13/97 10:20:49 TRACE: .....am_queryMapper: function Entered
08/13/97 10:20:49 TRACE: .....locateClientRecord: function Entered
08/13/97 10:20:49 TRACE: .....am_queryMapper: cannot find client 6-0x0000e5806363 in
08/13/97 10:20:49 TRACE: .....am_queryClient: client 6-0x0000e5806363 is not known to
08/13/97 10:20:49 TRACE: .....cl_queryClientele: function entered
08/13/97 10:20:49 TRACE: .....checkClient: function entered
08/13/97 10:20:49 TRACE: .....cl_queryClientele: client 6-0x0000e5806363 rejected in
08/13/97 10:20:49 OBJERR: .....am_queryClient: clientele failed when queried about clie
08/13/97 10:20:49 TRACE: .....processDISCOVER: binder.subnet [0x00000000]
08/13/97 10:20:49 INFO: .....processDISCOVER: client 6-0x0000e5806363 authentication fail
08/13/97 10:20:49 ACTION: ....reply_generator: no reply is generated
08/13/97 10:20:49 TRACE: ..main: No reply is to be generated
```

Figure 44. Log File Showing Rejected Client

## 6.8 Administration of a Running DHCP Server

To maintain a running DHCP server, IBM provides the dadmin command to:

- Re-initialize a DHCP server by causing the server to re-read its configuration file
- Delete a lease
- Control server tracing
- Display client information
- Display IP address information
- Display server statistics

To display information about the command syntax, enter: `dadmin -?` on a command line.

If you make changes to the configuration file, and you want these changes to become effective (for example, you just added a new client), you need to re-initialize the running server. This is done using the following command: `dadmin -h hostname -i -v` where `hostname` is the IP address or hostname of the DHCP server, `-i` tells the server to reinitialize and `-v` is verbose mode.

```
C:\>dadmin -i

PLEASE WAIT....Gathering Information From the Server....Please WAIT

Server successfully reinitialized

C:\>
```

*Figure 45. The DADMIN Command - Reinitializing the DHCP Server*

**Note:** It is not necessary to stop and restart the DHCP NT service in order to refresh the configuration file; only the `dadmin -i` command is required for that purpose.



---

## Chapter 7. IBM Network Station Manager

The IBM Network Station Manager is a browser-based tool for centrally administering IBM Network Stations and their users. Using the IBM Network Station Manager, the administrator can set IBM Network Station settings on a systemwide basis, or an individual user basis, or a workstation basis.

Since the NSM is a standard browser application, it can be accessed through any browser from any platform, as long as the browser used is JavaScript enabled.

The IBM Network Station Manager is actually a user-friendly configuration tool, presenting a graphical interface to the administrator who needs to administer a large number of Network Stations.

Actually, configuration settings and changes made using the Network Station Manager result in an update, by the NSM, of the actual configuration files, such as `required.nsm`, and `defaults.nsm` for example (to name only two).

The administrator also has the capability to manually edit these files, instead of using the NSM graphical interface; however, the NSM has been designed in order to prevent making mistakes in editing configuration parameters and should therefore be used whenever possible.

The URL to specify to access the Network Station Manager on an NT server is:

**`http://IP-host-address or hostname/nstation/html/nsmgr.htm`**

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 the IP-host-address.

At this point, you are presented with a Userid/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, since, as a user, he cannot be allowed to change systemwide settings or settings for other users.

If the user belongs to the NSMAdmin group, he is then allowed to specify settings for all users and all workstations. The panel below is the main Network Station Manager panel, after the user has been properly authenticated.



Figure 46. The Network Station Manager Main Panel

On the left hand side of the panel is the Setup Tasks list, with the following entries (where we have expanded the Startup and Internet tasks, which have subtasks not shown in the figure above):

- Hardware
- Startup
  - Programs
  - Menus
  - Environment Variables
- Desktop Manager
- 5250
- 3270
- Internet
  - Network
  - IBM Browser
  - Navio NC Navigator
  - Applet Viewer

The best way to get familiar with these settings is to browse the different tasks to see what can be configured. We do not cover each of these tasks in detail



here, as most are self explanatory, but we do give a few examples using the Hardware and the Desktop Manager tasks.

---

## 7.1 Hardware Settings

Select **Hardware** from the Setup Tasks list.

This action display a page where you can choose from **System Defaults**, **Workstation Defaults** or **User Defaults**.

Not every parameter available for system default is available for workstation default and user default too.

To modify parameters for a specific workstation, you need to either enter the name of a workstation, if you know it, or to click the **Browse** button to get a list of all the workstations that have been defined so far.

Note that this list is obtained from the DHCP configuration file (x:\ibmtcpip\etc\dhcpsd.cfg) where specific clients must have been defined and include a setting for DHCP Option 12 (host name).

See Chapter 6, "Understanding Dynamic Host Configuration Protocol (DHCP)" on page 55 for more information on configuring DHCP.

Note that an asterisk (\*) in front of the workstation profile indicates that a preference file already exists for that workstation and the administrator has viewed the preference file or added additional preferences for that workstation.

Select a workstation from the list and click **Select and return**.

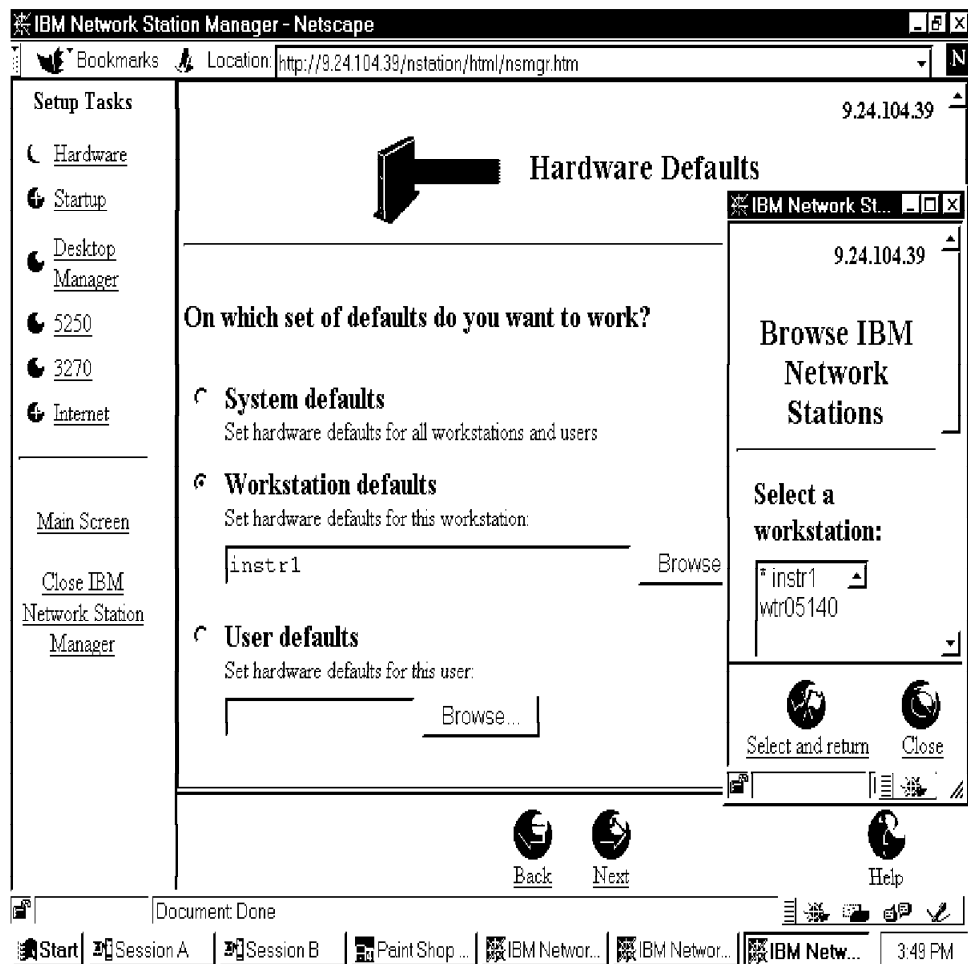


Figure 47. The IBM Network Station Manager. This shows the Hardware menu and workstation selection.

The same concept applies to a user configuration. A click on **Browse** in the user defaults section provides a list of all users defined in the Windows NT Server Security database and who belong to either the NSMAdmin and NSMUser groups.

An asterisk (\*) in front of the user profile indicates that a preference file already exists for that user; in other words, this user already has some parameters that have been set.

Select a user profile from the list and click **Select and return**.

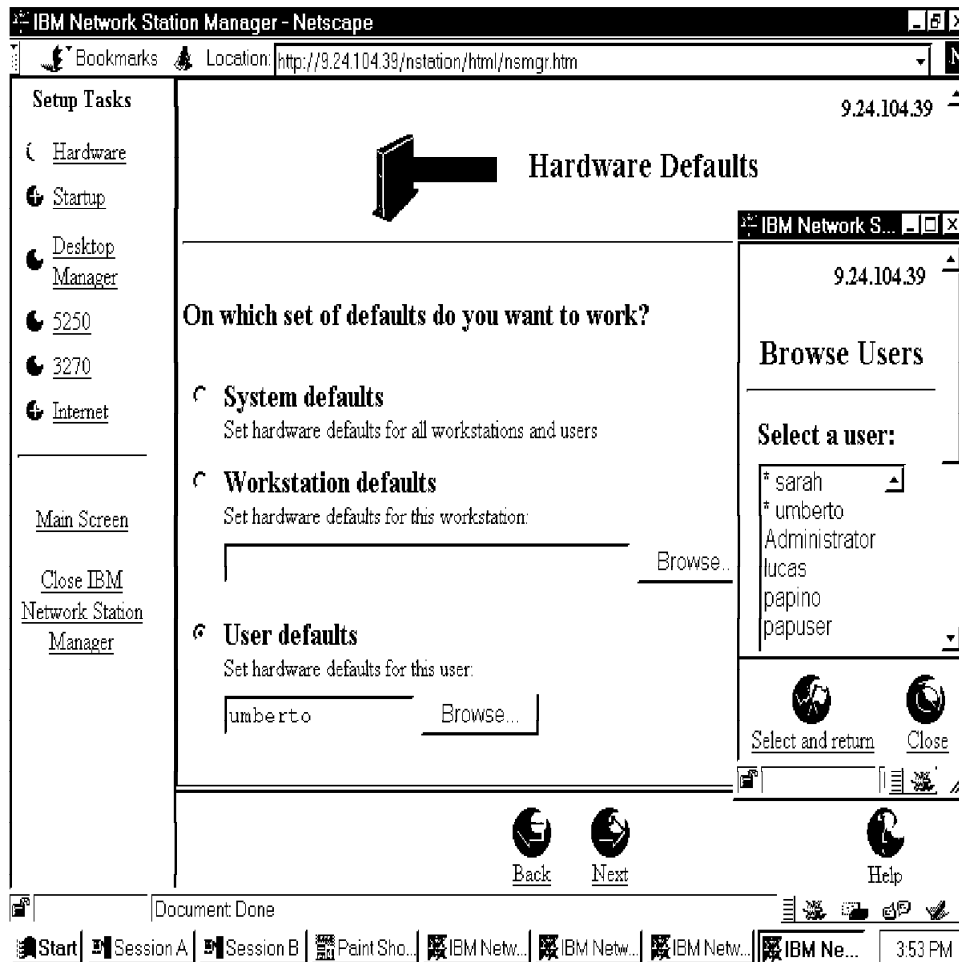


Figure 48. The IBM Network Station Manager. This shows the Hardware menu and user selection.

If we select System defaults, let's take a look at a few of the parameters we can set.

The intent is not to review every parameter of every menu but only to comment on some that might have a special meaning or that might require a special explanation. For additional information, please use the Help available on every window of the IBM Network Station Manager by clicking on the **Help** button on the bottom right hand corner of every page.

Select **System Defaults**, then click on **Next** to display the panel shown below:

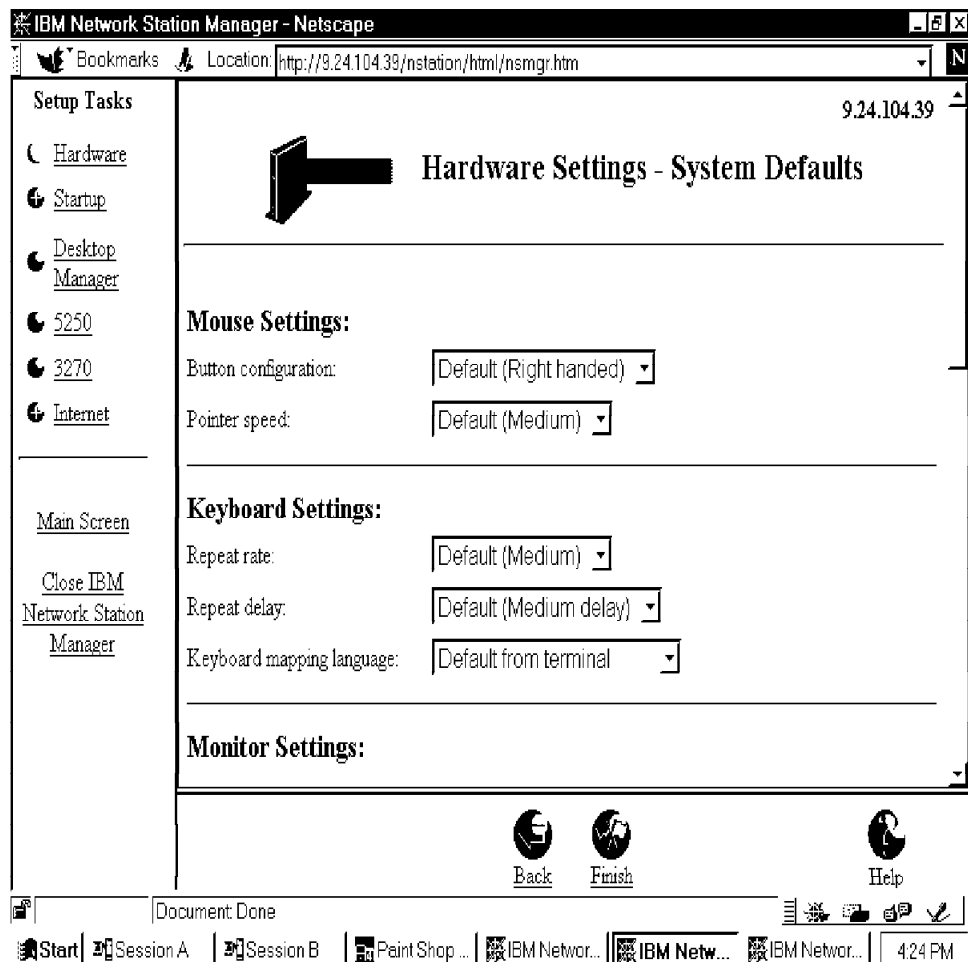


Figure 49. The Network Station Manager Hardware Settings

The following is a list of all the parameters that are available from this window (if you scroll down the window to see the rest of the parameters):

- Mouse Settings
  - Button Configuration
  - Pointer speed
- Keyboard Settings
  - Repeat Rate
  - Repeat Delay
  - Keyboard Mapping Language

This value determines the language-specific special symbols (such as accents) that your keyboard can produce. The IBM Network Station can autodetect which keyboard is attached. It will use that information to select which language to use for keyboard mapping. If the keyboard that is attached cannot be recognized by the IBM Network Station, the keyboard mapping defaults to English (US).

**Note:** To determine the current setting, use the IBM Setup Utility.

- Monitor Settings
  - The number of minutes before the screen saver turns on

- Screen saver

Select from the list of available screen savers. The default is the IBM bitmap.

- Minutes before monitor standby
- Minutes before monitor suspend
- Minutes before monitor power down

These power settings enable you to configure your monitor to save electrical power. The settings are presented, on the selection panel, in an ascending order (standby, suspend, power-down) according to how much electrical power can be saved. If you choose 0 as a value, the setting is not used.

These power-saving settings are only valid if your monitor has the Data Display Channel (DDC) capability of the Video Electronics Standard Association (VESA).

**Note:** The monitor must be powered-on before the IBM Network Station system unit for the power management features to be active.

- Desktop background

The value of this field determines the background of the desktop. The default is the IBM bitmap.

- Miscellaneous Settings

- Administrator password

The password provides access to the IBM Setup Utility to change the boot settings for example. Without a password, the user is only able to view the parameters, and not to change them.

- Contact person

The name of the system administrator for your IBM Network Station.

- Terminal location

The physical location of this IBM Network Station.

- Parallel (printer) port

This field determines if the printer attached to the IBM Network Station system unit can be used for remote printing. If the value selected is On, the printer works as a printer in the network. If the value detected is Off, the printer will not work as a printer in a network. The default is On.

- Allocate memory to speed window refresh

This field determines if additional memory, in the IBM Network Station system unit, should be used to help refresh a window after the window has been moved or altered in size. The default is No. Having windows refresh quicker is desirable. However, in IBM Network Station system units, with small amounts of memory, having this value set to Yes might impact the number of open windows you can have.

- Update boot monitor from this file

This field is set to specify that the boot monitor program, residing in the PROM on the Network Station, should be updated the next time the Network Station boots from the server.

The update sequence includes a time period during which damage may occur to the IBM Network Station if power is lost. During this period the IBM Network Station displays a warning to *not* power off the system. To avoid unnecessary downloads of the flash PROM, it is recommended that this field be set to the default value once all IBM Network Stations are updated.

**Note:** At the time of this writing, the current boot monitor level is bp28ae.

Click on **Finish** to complete the Desktop Manager setup.

### 7.1.1 Files Created by NSM for Hardware Settings

As the user enters configuration data into the Network Station Manager panels, the NSM updates the configuration files with the appropriate statements to reflect the configuration changes.

The following are a few examples of some of the changes made by the NSM to these configuration or startup files.

- Changing a keyboard setting.

In Hardware System Default Settings, we entered:

Keyboard setting.....Italian

The resulting update to

drive:\nstation\nstation\CONFIGS\default.nsm

is the following parameter:

set xserver-keyboard-type=italian

- Workstation data update.

Then we choose workstation **instr1** from the workstation list and we enter the following data:

Minutes before monitor standby.....60

Minutes before monitor suspend.....60

Minutes before monitor power down.....60

Contact person.....Joe Nobody

Terminal location.....ITS0 Raleigh

If this is the first time that we enter configuration data for this workstation, the NSM creates the following three files:

drive:\nstation\configs\instr1

drive:\nstation\configs\instr1.nst

drive:\nstation\configs\instr1.trm

The first file (instr1) contains the following data:

read standard.nsm

read instr1.nst

read instr1.trm

The Network Station can now be configured to read, as its initial configuration file, the instr1 file instead of the default standard.nsm file. It still causes the standard.nsm file to be read, because the instr1 file points to it, but it also cause the two other instr1 files to be read after all the other

configuration files have been read. See Chapter 5, “IBM Network Station Customization Files” on page 41 for additional details on how to configure to read these workstation-specific configuration files. The drive:\nstation\configs\instr1.nst contains:

```
set pref-power-manage-powerdown-time=60
set pref-power-manage-standby-time=60
set pref-power-manage-suspend-time=60
set unit-contact="Claude Bechard"
set unit-location="ITS0 Raleigh"
```

The drive:\nstation\configs\instr1.trm file is empty.

- Update to a specific user

We then select user **wilma** from the user list, and Hardware Default, and we set the Mouse Setting to:

Button Configuration.....Right Handed

This is so that when user Wilma logs on to any Network Station, the right button of the mouse gets enabled as the primary button.

This updates file drive:\nstation\userdata\wilma\wilma.nsu with:

```
set pref-mouse-arrangement=right-handed
read /nstation/UserData/wilma/wilma.usr
```

The drive:\nstation\userdata\wilma\wilma.usr remains empty.

---

## 7.2 Desktop Manager Setting

Select **Desktop Manager** from the Setup Tasks list on the left of the IBM Network Station Manager panel.

This brings up a new page where you can choose from **System Defaults**, **Workstation Defaults** or **User Defaults**.

If we choose System Defaults, the following panel is displayed:

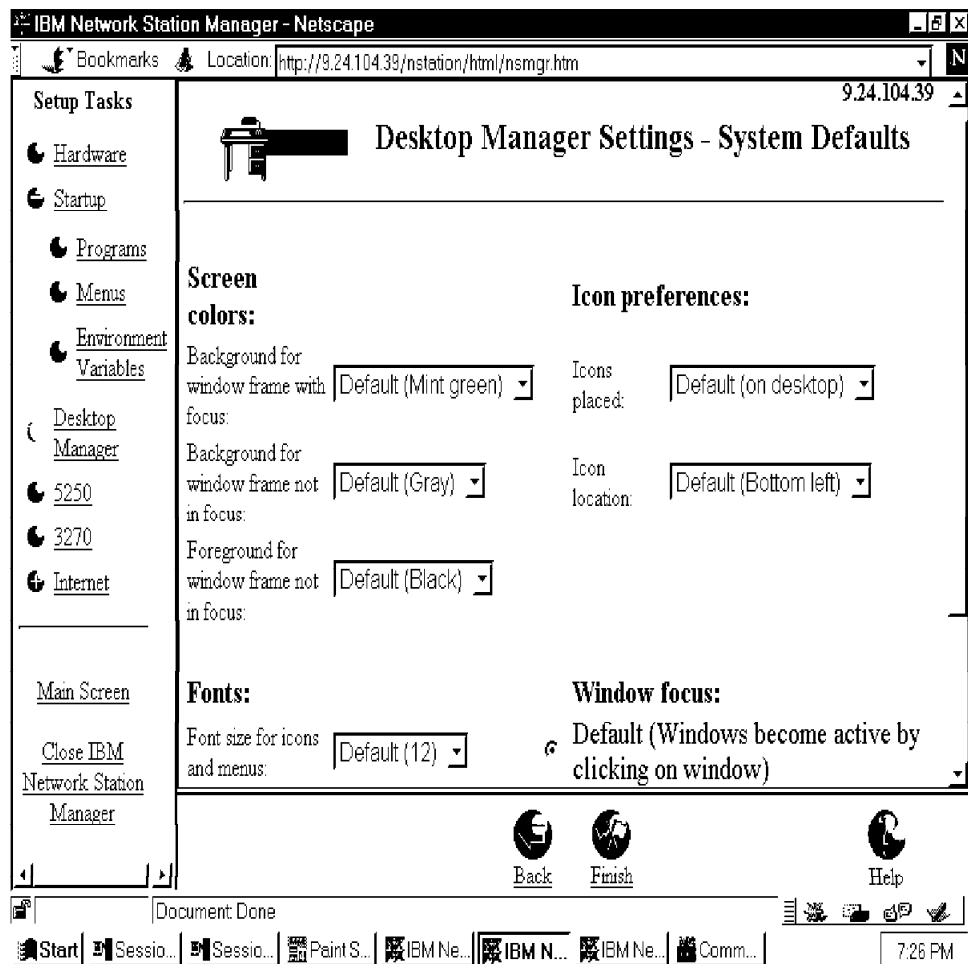


Figure 50. The Desktop Manager - System Default Settings

The following is a list of all the parameters you can update from this windows (if you scroll down to see all the items).

- The screen color (for window borders).
  - Background color for window border with focus. The default is Mint green.
  - Background color for window(s) border(s) not in focus. The default is Gray.
  - Foreground color for window(s) border(s) not in focus. The default is Black.

For best results, the border's color should contrast with the color chosen for the background color.
- Icon preferences.
  - Where icons are placed.
 

Values allowed are: in window or on desktop. The default is desktop.
  - Where icons are located
 

Values allowed are: top left, bottom left, top right, or bottom right. The default is bottom left.
- Fonts.



Specifies font sizes for icons and menus. Valid font sizes range from 8 point (small) to 24 point (larger). The default is 12 point.

- Window focus.

Specifies how a window becomes active. The default is to click on the window you want active but you can change that setting to "when mouse moves over window".

Click on **Finish** to complete the Desktop Manager setup.

### 7.2.1 Files Created by NSM for Desktop Manager Settings

- We made the following changes to the System Default:

Screen color: Back Ground for Windows frame with focus...0live

As a result, the file drive:\nstation\userdata\systdef\NCDwm\pref was updated to contain:

NCDwm.highlightColor: #808000

- Then we selected user **wilma** from the Desktop Manager User Default and we specified:

Windows become active when mouse moves over window

The file drive:\nstation\userdata\wilma\NCDwm\pref now contains:

NCDwm.keyboardFocusPolicy: pointer

These were just a few examples to show how different configuration files get updated by the Network Station Manager as you make changes in the configuration panels. We recommend that the user always use the configuration interface, as opposed to updating the files manually with an editor, in order to avoid mistakes. Only when the desired parameter is not supported by the NSM configuration interface should the file be manually updated.



---

## Chapter 8. Network Station Applications and User Services

The intent of this chapter is to focus on the facilities available to the user from the network station's desktop, mainly the menu bar and the Network Station console. We also look at some of the configuration changes required to customize the menu bar.

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 disposal:

- His primary tool is a 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.

---

### 8.1 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 to trigger the start of 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 certain 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 can be 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.

- 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 is 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 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 is away from his 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 can elect to use a new password each time he uses the Lock function.

- 3270 or 5250

When the user clicks on the default 3270 or 5250 button, a small box appears asking for your 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; the host address, and the characteristics of the session such as graphics and screen size, etc., can all be preconfigured.

- IBM Browser or Navio Browser

These are two other buttons that you get by default, and they cause the IBM Network Station browser or the Navio browser to start.

**Note:** In the case of the browsers, there are a few mandatory settings that must be done before they can be used successfully. The mandatory settings are:

- A Socks or Proxy server defined via the Network Station Manager
- A Domain name server address configured in one of the configuration files (unless you are using DHCP and this was configured in DHCP).
- You also need to have configured the default domain name (this currently has to be done manually by editing one of the configuration files. See Chapter 10, “Network Station Browsers” on page 119 for details).

See Chapter 10, “Network Station Browsers” on page 119 for additional details.

- New X session

This is also a default button. A click on this button causes the station to send a broadcast requesting all IP hosts, which are capable of supporting an X session, to reply.

The result is the display of a Login Chooser screen, with a list of hosts which have responded to the broadcast. This is the default, but there are configuration parameters that can be set to determine which hosts will actually appear in this list.

Choosing one of the entries in the list, or manually typing an IP address or IP host name in the Host field causes the station to send a request for an XDMCP (X display Management Control Protocol) session.

The typical use of this function is for an AIX user to log on to an AIX system as a CDE user (Common Desktop Environment) for example, or for a user to log on to a WinCenter server in order to get a Windows desktop and use Windows applications.

**Note:** If you start an X session to a an AIX system to use the CDE desktop, make sure you stop the local window manager, by using the WindowMgr pull-down on the console, before you start the X session. The reason is that CDE uses its own window manager, which conflicts with the local windowm

manager. If you fail to stop the local window manager, you will only get a black screen, with an hourglass displayed.

Let us now take a look at how the user environment can be customized either by autostarting applications or by customizing the menu bar to fit specific needs.

### 8.1.1 Creating a New Menu Bar Item

A new menu item can easily be added to the menu bar by using the Network Station Manager.

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 you want that menu item to appear on the menu bar for all users. The procedure to follow is:

- Log on to the NSM
- Use a username which is part of the NSMAdmin group
- Select the **Startup** task
- Select the **Menu** subtask
- Select **System defaults**
- Scroll down to 3270 menu item
- Add a 3270 session, call it WTSCPOK, and specify the host as 9.12.14.1

The result should be the following statement added to the startup.nsm file in \nstation\userdata\sysdef:

```
MENUITEM "WTSCPOK" ns3270 9.12.14.1
```

- Log Out and log back in to have the new configuration data read by the Network Station
- You should now have an additional menu item on the menu bar called WTSCPOK
- Click on this new item to start your 3270 session

### 8.1.2 Autostarting an Application

Assume that you want to have a 3270 application autostarted after the user logs in, and you want this to be applicable to all users. The S/390 host address is 9.12.14.1, you want the session to be titled "WTSCPOK", a 32x80 screen size and to be enabled to do graphics.

The procedure to follow is:

- Log on to the NSM as an administrator
- On the Setup tasks, select **Programs**
- Select **System defaults**
- Scroll down to the 3270 autostart item
- Under System/390, enter 9.12.14.1
- Under session title, enter WTSCPOK
- Select **32x80** under screen size, **enabled** under graphics and **finish**
- At the Network Station, Log Out and log back in as any user
- The 3270 session should start automatically after the user login

You should also see that the \nstation\userdata\sysdef\startup.nsm file has been updated with the following statement:

```
RUN ns3270 -title "WTSCPOK" -cols 80 -rows 32 -graphics 9.12.14.1
```

### 8.1.3 MENU Item for Remote Applications (X Session)

Assume that you need a menu bar button to start an aixterm application on a rs/6000 and reroute the display output to your Network Station's monitor.

This time, let's make this applicable only to a specific user.

The procedure to follow is:

- Log on to the NSM as an administrator
- On the Setup Tasks, select the **Startup** task
- Select the **Menu** task
- Select a specific user (through browse or entering the name)
- Add a Menu item called "aixterm", the target host name is rs600026.itso.ral.ibm.com, the command is aixterm, and optional parameter is -display \${IP}:0

The -display \${IP}:0 instructs the application to export its display to the host represented by the IP address specified; the \${IP} here is a variable which will be replaced with the IP address of the Network Station when it issues the command. This way, this command is valid for any IP address that the workstation might be using.

The following statements are added to the startup.nsm file in \nstation\userdata\userxx, where userxx is the user name you used.

```
RUN xhost rs600026.itso.ral.ibm.com
MENUITEM "aixterm" rsh rs600026.itso.ral.ibm.com aixterm -display ${IP}:0
```

- Log out your Network Station and log in with the user name you used
- Your menu bar should now have the additional menu item

### 8.1.4 Starting a Java Applet

Let's put 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 JDK, and let's make it available to all users.

The procedure would be:

- Log on to the NSM as an administrator
- Under the Setup Tasks, select **Startup**
- Select the **Menu** subtask, and **system defaults**
- Scroll down to the Java Applets menu
- Add an item, calling it "java-blink"
- Specify the application and path as  
/nstation/java/classes/demo/blink/example1.html (or use /netstation/ instead of /nstation/ if you prefer to use NFS instead of TFTP to access this file)
- You should get the following statement in the startup.nsm file in \nstation\userdata\sysdef:  

```
MENUITEM "java-blink" appletviewer  
/nstation/java/classes/demo/blink/example1.html
```
- Create a demo/blink directory under /nstation/java/classes
- 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 network station).
- Now log out and log back in as any user

- Click on the java-blink menu item to start the java applet

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.

### 8.1.5 Starting a Java Application

Now, instead of an applet, let's take the same example as above but make it a Java application.

The procedure is similar as the procedure for an applet:

- Log on to the NSM as an administrator
- Use the **Startup** task, the **Menu** subtask, and **System defaults**
- Scroll down to the java application menu
- Add an item, calling it "java-appl"
- Specify the class name; we used "Claude" (case sensitive) which was a simple application printing out Hello World
- Specify any arguments, if the application requires it
- Specify the classpath. In our case, we put our class in a directory called \nstation\java\classes\claudio, and the standard java classes are in \nstation\java\classes.zip, so we entered the classpath as /netstation/java/classes.zip:/netstation/java/classes/claudio

#### TFTP vs NFS

Remember that there are two ways of accessing the \nstation\java\ subdirectory; either through TFTP, in which case you use the alias /nstation/ to give you access to the \nstation\ directory, or through NFS, in which case you use the alias /netstation/ which gives you NFS access to the same \nstation\ directory.

In many cases, it does not really matter whether you use TFTP or NFS, but in this case, it is probably preferable to use NFS in order to handle the reading of the classes.zip file, which cannot be done when using TFTP.

Using TFTP will still work because the same classes that are in the classes.zip file are also available on the server in unzipped format. So, when TFTP finds out it cannot use the ZIP file, it goes on to read the individual required classes from the expanded directory on the server.

The conclusion is that it is probably more efficient, in this case, to use NFS, and therefore to use the /netstation/ alias instead of /nstation/.

- You should get the following statement in the startup.nsm file in \nstation\userdata\sysdef:

```
MENUITEM "java-appl" java -classpath
/netstation/java/classes.zip:
/netstation/java/classes/claudio:NCDCLASSES -verifyremote
Claude
```

(The above line has been broken to fit on this page, but may be all in one line in your startup file. The classpath is not broken like it is in this example).

**Note:** The NCDCLASSES path was added automatically by the NSM; it is an internal variable which points to the default classpath. Since we have already specified /netstation/java/classes.zip in our classpath, this NCDCLASSES is

redundant here and not necessary. It does not do any harm to leave it there but it could be removed, in this case.

- Create a claude directory under \instation\java\classes
- Copy the Claude.class application (or whatever yours is) to the above directory you just created
- Now log out and log back in as any user
- Click on the java-appl menu item to start the Java application

---

## 8.2 The Network Station Console

The Network Station console, although available to the user, should normally not be used by the typical user, because it is not required to launch user applications but rather, most of the time, to do problem determination.

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 which can be changed to use the Pause key instead, for example, by using the set pref-console-key-sequence = "Pause".

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.

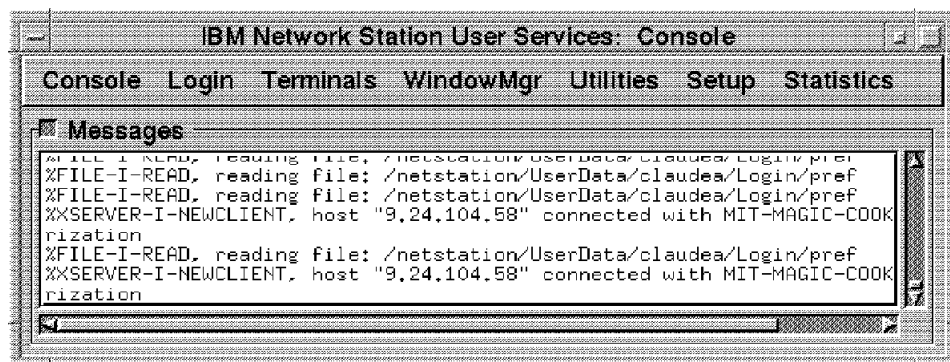


Figure 51. IBM Network Station Console

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.

### 8.2.1 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 following four entries:

- Show Version

This is a very useful panel to identify the version level of the software and the boot monitor program running on the Network Station. This also shows the built-in and current token-ring addresses, the TCP/IP address, memory, and a few other useful pieces of information, as illustrated below.



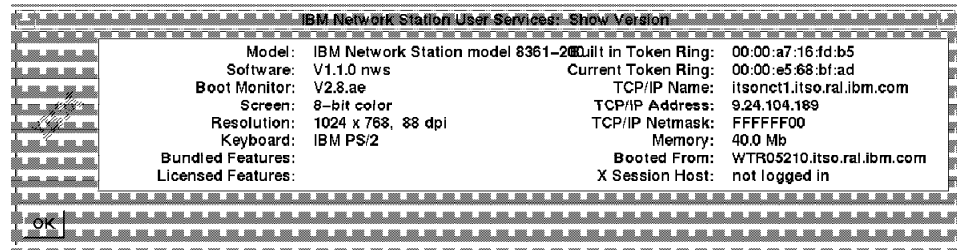


Figure 52. IBM Network Station Console - Version

- 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.

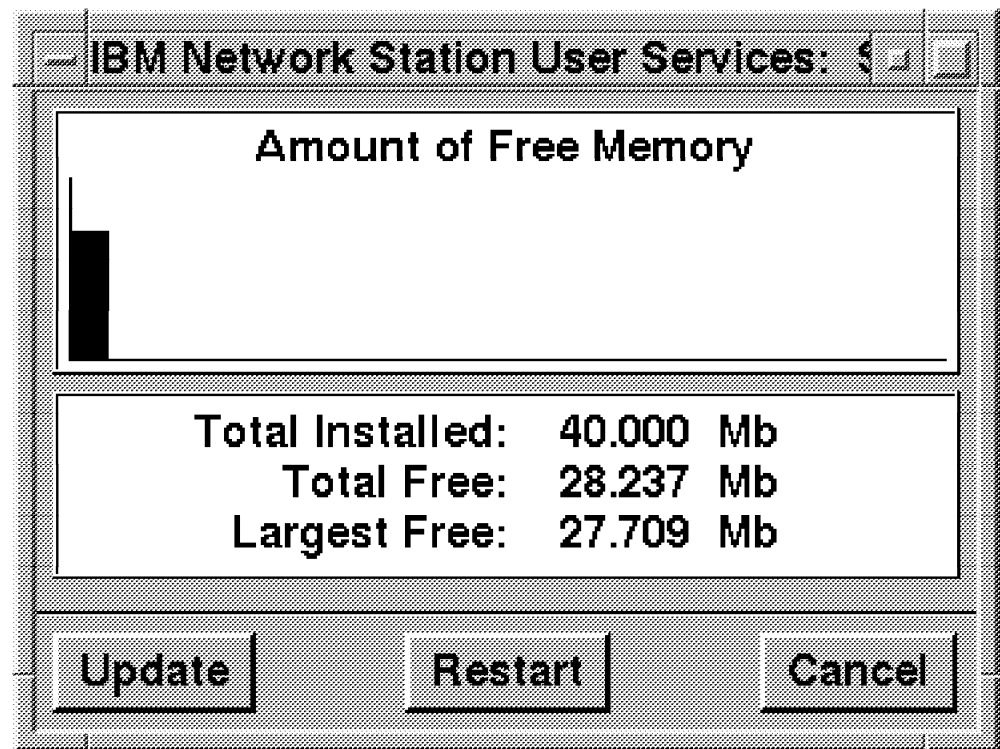
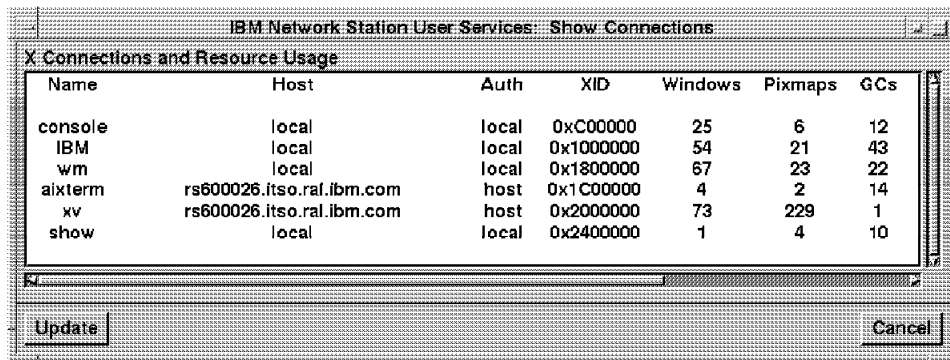


Figure 53. IBM Network Station Console - Memory

- 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.



IBM Network Station User Services: Show Connections

X Connections and Resource Usage

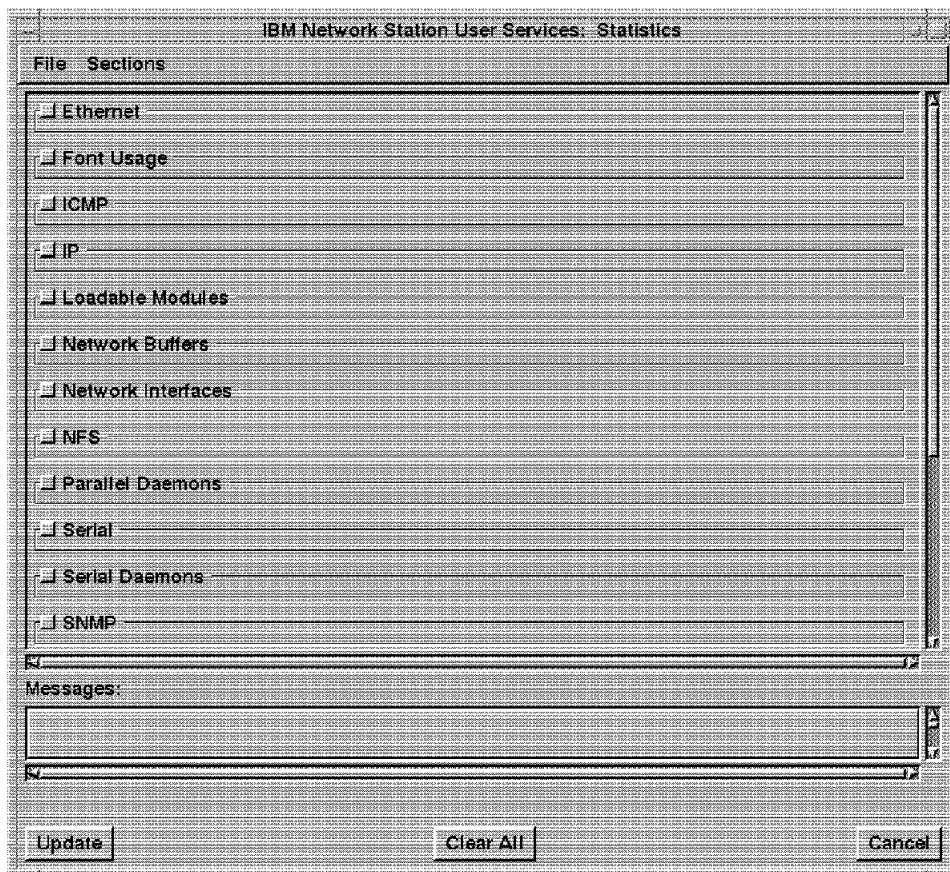
Name	Host	Auth	XID	Windows	Pixmap	GCs
console	local	local	0xC00000	25	6	12
IBM	local	local	0x1000000	54	21	43
wm	local	local	0x1800000	67	23	22
aiXterm	rs600026.itso.ral.ibm.com	host	0x1C00000	4	2	14
xv	rs600026.itso.ral.ibm.com	host	0x2000000	73	229	1
show	local	local	0x2400000	1	4	10

Update Cancel

Figure 54. IBM Network Station Console - X Connections

- 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.



IBM Network Station User Services: Statistics

File Sections

- ☐ Ethernet
- ☐ Font Usage
- ☐ ICMP
- ☐ IP
- ☐ Loadable Modules
- ☐ Network Buffers
- ☐ Network Interfaces
- ☐ NFS
- ☐ Parallel Daemons
- ☐ Serial
- ☐ Serial Daemons
- ☐ SNMP

Messages:

Update Clear All Cancel

Figure 55. IBM Network Station Console - Statistics

## 8.2.2 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:

- Change Quick Setup

This deals mainly with boot parameters. These are essentially some of the same parameters which are available from the Network Station Setup utility.

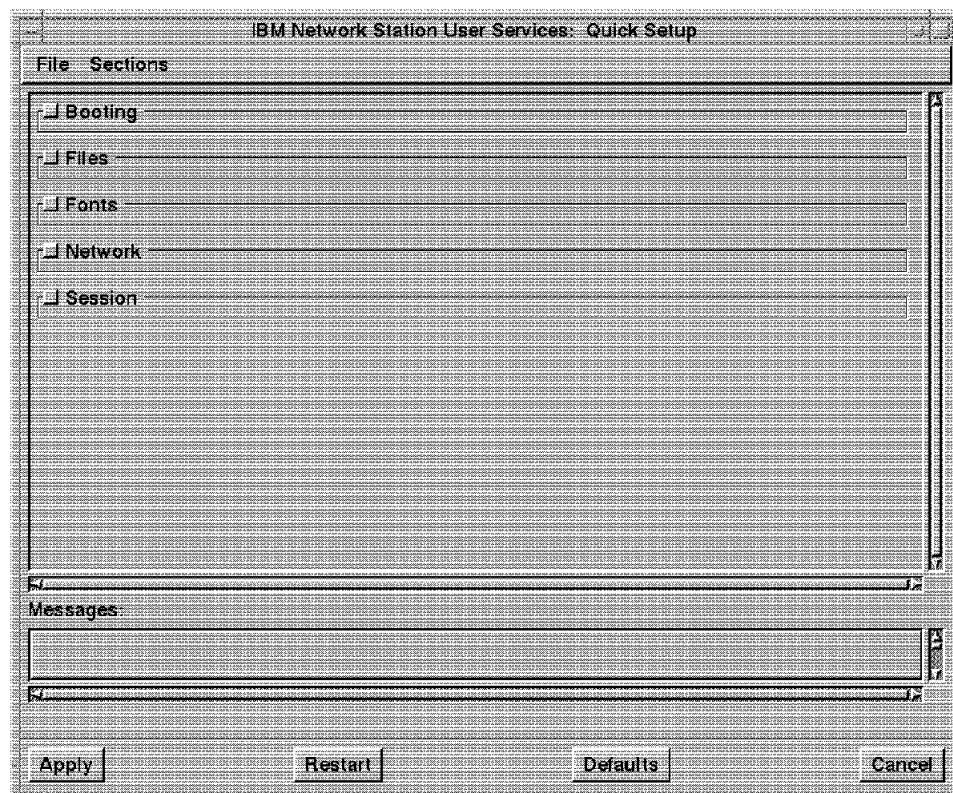


Figure 56. IBM Network Station Console - QuickSetUp

- Change Setup Parameters

The Setup parameters deals with all the main configuration parameters, as shown below:

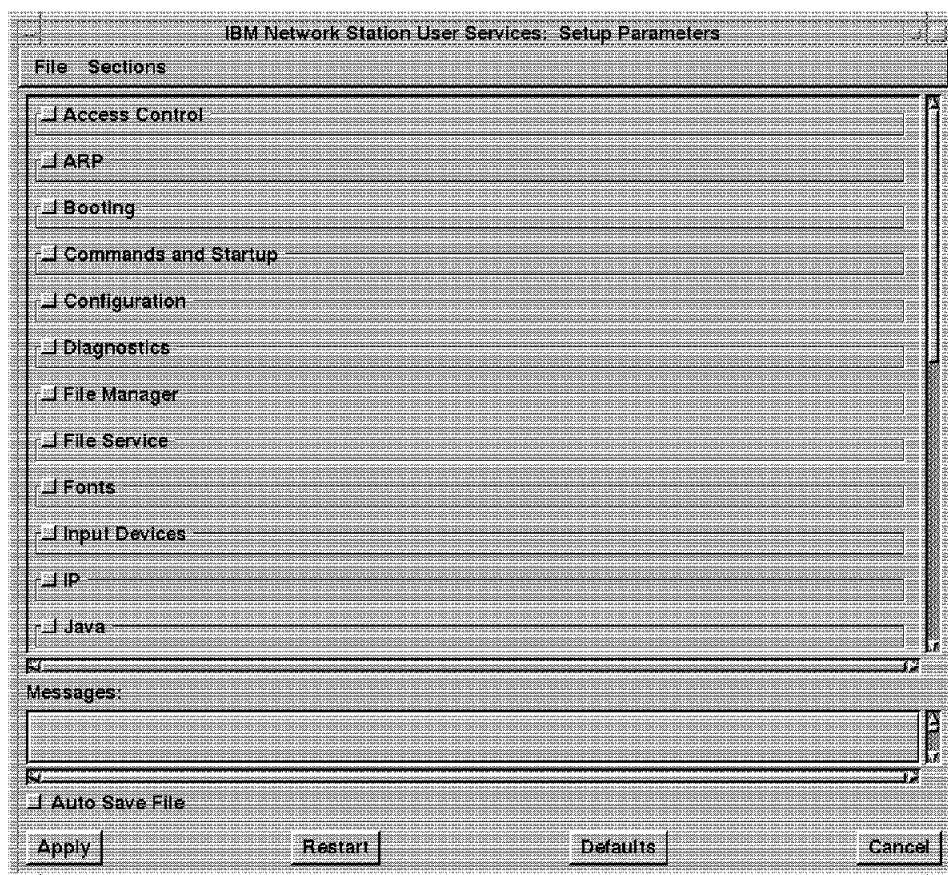


Figure 57. IBM Network Station Console - Setup Parameters

Notice the 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 Network Station to read again 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:

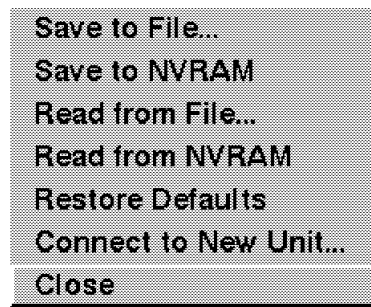


Figure 58. IBM Network Station Console - Setup - File Pull-Down

- Save to File - CAUTION - The Network Station has no knowledge of the hierarchical structure of the configuration files on the server which were loaded 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 which 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 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.
- 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:

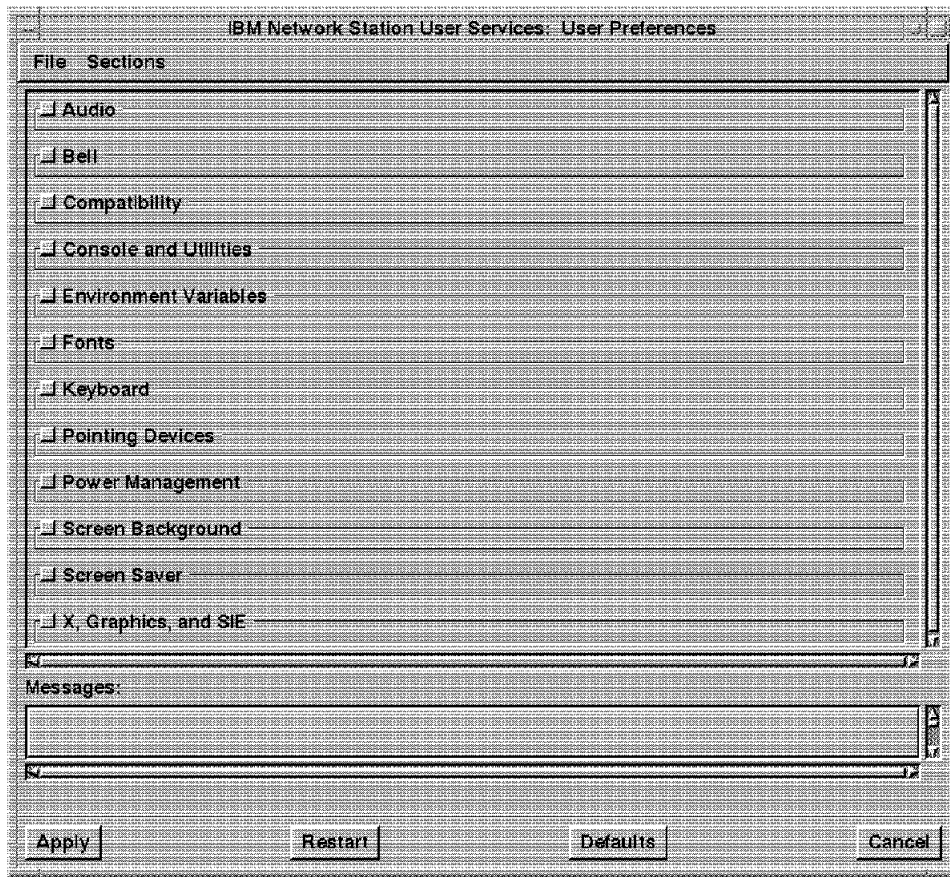


Figure 59. IBM Network Station Console - User Preferences

### 8.2.3 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:

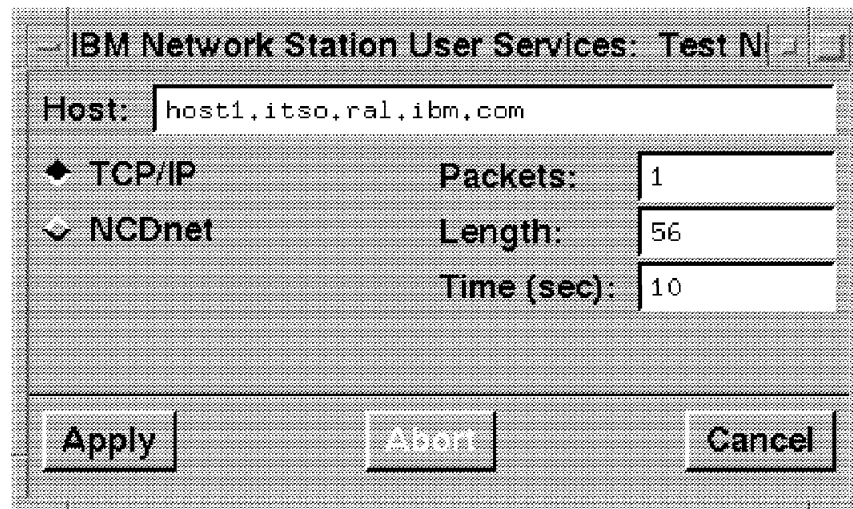


Figure 60. IBM Network Station Console - Test Network

## 8.2.4 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 CDE (Common Desktop Environment). This is because CDE uses its own window manager, which conflicts with the local window manager.

## 8.2.5 Terminals

The items on this pull-down are used to start a telnet session, for example, or to start a few of the services such as the diagnostic service (this is similar to the console messages), the configuration daemon or the file services daemon.

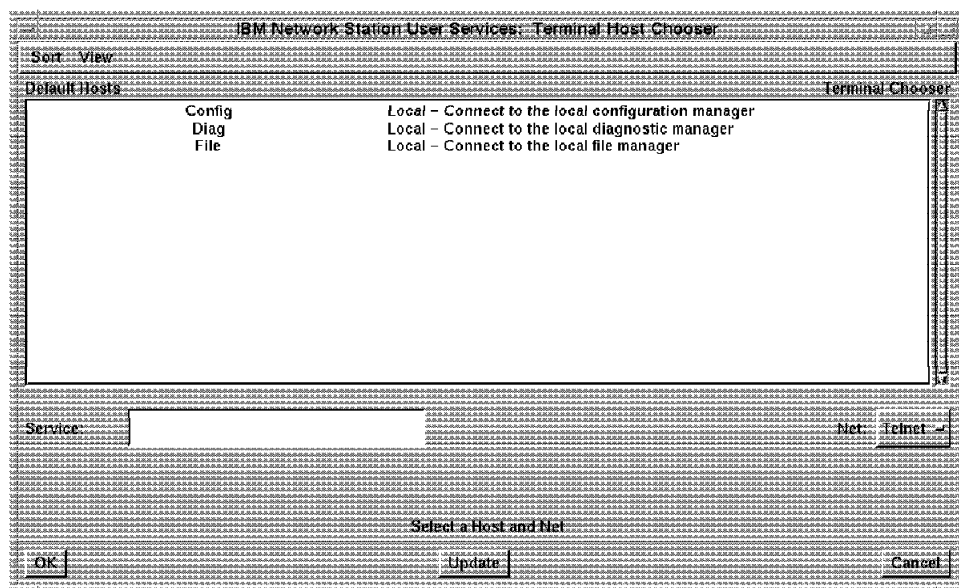


Figure 61. IBM Network Station Console - Terminal/Telnet



## 8.2.6 Login

Under this pull-down is the Login Chooser, which, when started, lists all the hosts which are capable of an X session. The items, or hosts, which appears on this list depend on how this has been configured, but, by default, the hosts listed will be those hosts that respond to a broadcast asking hosts which are capable of an X session to respond.

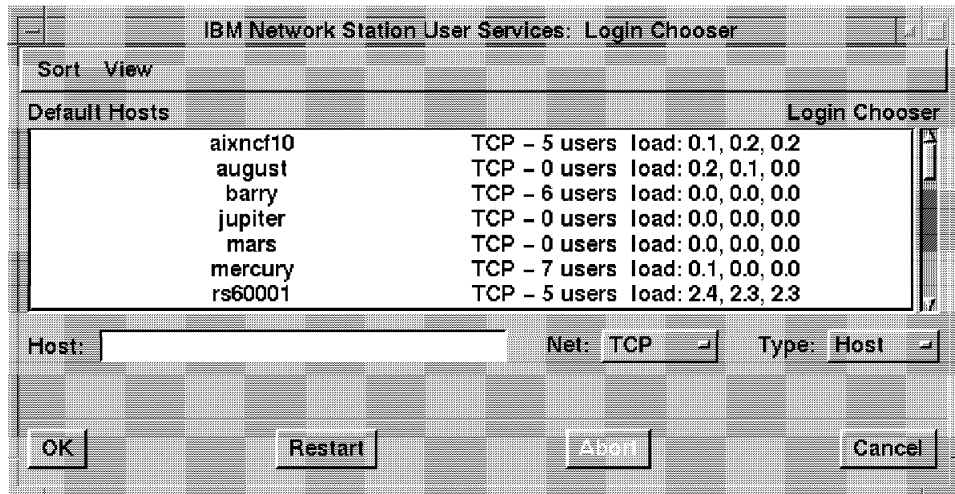


Figure 62. IBM Network Station Console - Login Host Chooser

## 8.2.7 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 in the log
- Reboot - Is equivalent to power off/power on
- Close - Closes the console

## 8.2.8 Messages

A click on the Messages checkbox opens up the display of console messages. This is your primary problem determination tool and the first place to look for error messages.



---

## Chapter 9. Network Station Emulators

The IBM Network Station provides two terminal emulators:

- The IBM Network Station 3270 Emulator, for accessing S/390 hosts running OS/390, MVS/ESA, VM/ESA, VSE/ESA, or TPF.
- The IBM Network Station 5250 Emulator, for accessing AS/400 hosts running OS/400.

The protocols used by these emulators are TN3270 and TN5250 respectively. Therefore, the target hosts must be configured with TCP/IP.

You can also use a TN3270 gateway (for example, the IBM Communications Server for Windows NT or for OS/2 Warp) to convert from TN3270 to SNA if the host is configured only for SNA.

The Network Station Emulators are specifically designed to be used on the IBM Network Station. They are loaded from a boot server and run (execute) on the IBM Network Station as native applications.

Because the Network Station has no local disk storage, all the configuration data for the emulator, such as color preferences, etc. is stored in files residing on the boot server.

We take a look here at some of the emulator parameters that can be configured using the Network Station Manager and the resulting changes that are produced in the configuration files.

---

### 9.1 Configuring the IBM Network Station 3270 Emulator using NSM

Select **3270** from the Setup Tasks menu in the IBM Network Station Manager home page.

This displays a new page where you can choose from **System defaults** or **User defaults**. Every parameter available for system defaults is also available for user defaults.

Select **System defaults**, then click on **Next** to display the panel shown below:

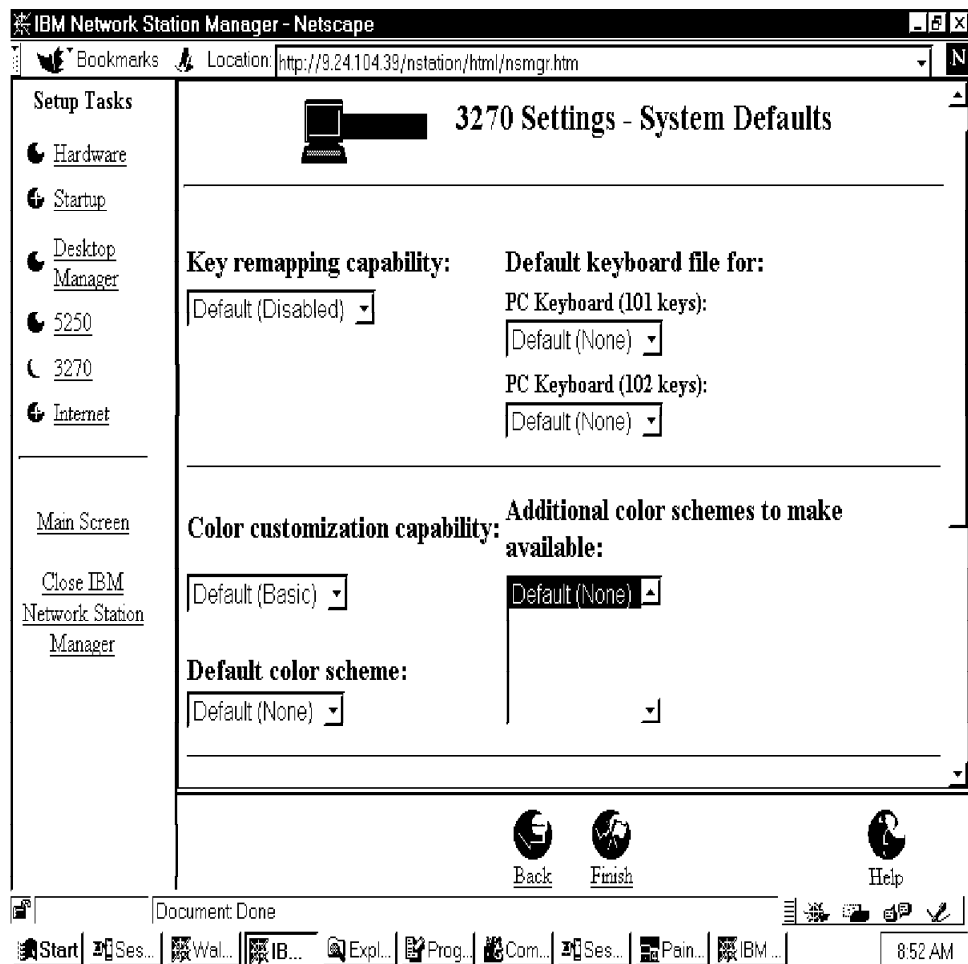


Figure 63. The IBM Network Station Manager. 3270 emulator settings.

The following is a list of all the parameters you can update from this windows (use scrolling to see all the items).

- **Key remapping capability.**  
Determines if you want the user to have the ability to remap keys or to restrict the user to the 3270 default (or system default). This function is made available to the user through the Option pull-down in the task bar of the emulation session. The default is Disabled, which means that the user can see the Keyboard Remapping selection but cannot select it (grayed out). "Hidden" means that the user will not see the Keyboard Remapping selection in the Options pull down.
- **Default keyboard file.**  
You can select a default keyboard file for the 101 or 102 keyboards. Which keyboard file is used depends on the type of keyboard being used with the 3270 emulation session.
- **Color customization capability.**
- **Additional Color schemes to make available.**
- **Allow use of keypad.**  
Specifies if users can use the pop-up keypad. The pop-up keypad represents PF keys 1 through 24. If a particular keyboard has some PF keys mapped to

perform functions different from the regularly mapped PF keys, users could access the pop-up keypad and press a PF key and the function the PF key is mapped to perform is run. The default is No, meaning you cannot use the pop-up keypad to select PF keys.

- Allow use of graphics

Enables/disables the capability of the 3270 session to display graphics. Graphics is only available with a 32 X 80 screen size.

- Key for Enter function

You can choose the 3270 Enter key to be the keyboard Ctrl key or the keyboard Enter key.

- Auto action

The Auto action function allows the user to highlight a text string and use this string as a command to be executed. For example, if the user selects the string "PF10" which appears on the screen, a double click on the string acts just like pressing the corresponding function key. The default is No, meaning Auto action is not enabled.

- Screen size

Use to select the size (number of rows and columns) of the 3270 session display. If you select the 27 rows by 132 columns size, the data displayed could become very small and hard to read (depending on the size of the monitor).

- Telnet 3270 port to connect to

Specifies which TCP/IP port on the destination host is used to establish a 3270 session. The default is 23. Other valid values range from 5001 through 65535. To use a port number other than the default, you should contact the system administrator of the remote host for the correct port number for that machine.

Click on **Finish** to complete the 3270 setup.

### 9.1.1 Files Created by NSM for 3270 Settings

- In the 3270 System defaults page in Figure 63 on page 106, we entered:

Allow use of keypad.....Yes

Use auto action.....Yes

The file drive:\nstation\userdata\systdef\NS3270\pref contains, as a result:

NS3270\*autoAction: true

NS3270\*buttonBox: true

- Then we select the user Gessica from the 3270 User defaults page and we enter:

Allow use of graphics.....Yes

The result is the file drive:\nstation\userdata\gessica\NS3270\pref, which contains:

NS3270\*Graphics: true

---

## 9.2 Starting the IBM Network Station Emulators

A Network Station user has basically two ways to start an emulator session:

- Autostart the emulator session

This assumes that the administrator has configured the startup files such that an emulator session is automatically started after the user logs on. The session can be autostarted with a specific host or can be autostarted in general, requiring the user to enter the desired destination host.

- Use the menu bar

This requires that the administrator has placed an item on the menu bar called 3270 to allow the user to start a session. This menu bar item can also be configured to be general, that is the user still has to enter a destination host, or it can be specific to a prespecified destination host (or both).

Here is an example of using the Network Station Manager to configure an emulator session to be on the menu or to be autostarted.

If you click on the **Startup** setup task in the Network Station Manager window shown in Figure 64 on page 109, it expands into the following three items:

- Programs (to specify programs to autostart)
- Menu (to configure items on the menu bar)
- Environment variables (to set variables)

Select **Menu**, then **System defaults**, then click on **Next** to display a panel as shown below:

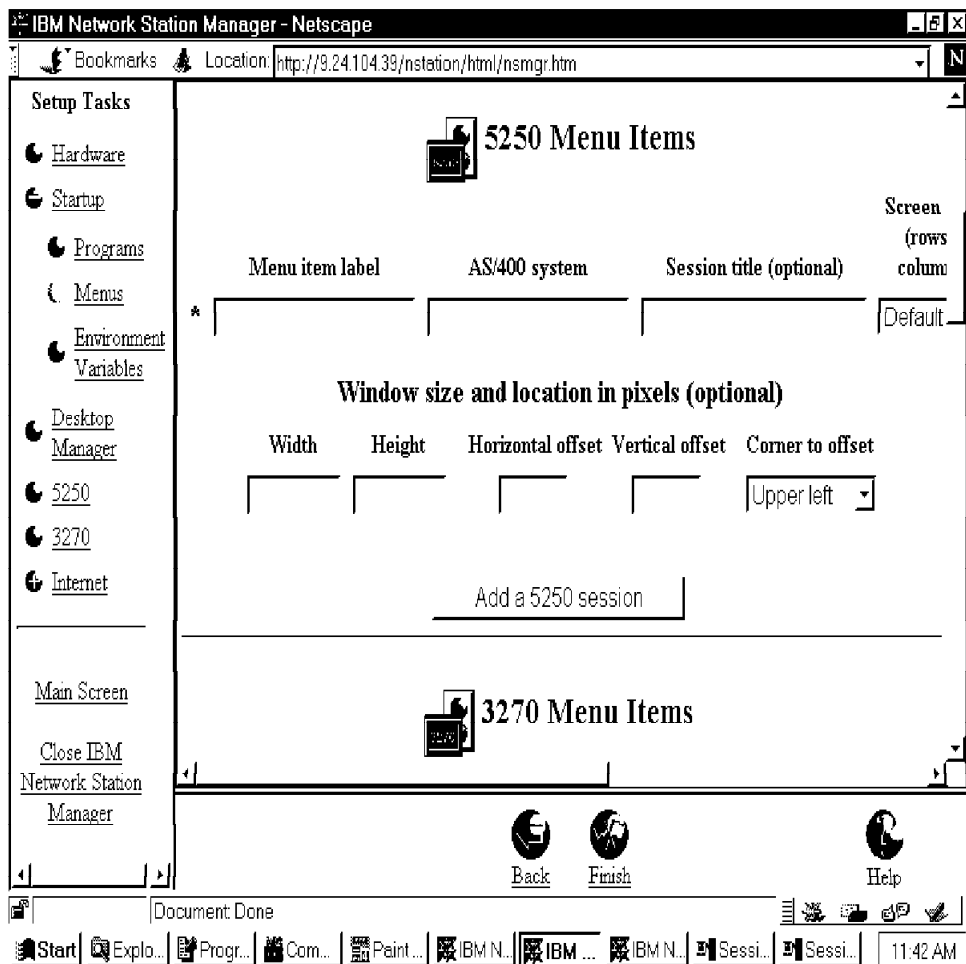


Figure 64. The IBM Network Station Manager - Startup menu settings.

The following is a list of the parameters you can update from this window (use scrolling to see all the items).

**Note:** The selections here are nearly all the same as those in the Setup Programs, because you are defining essentially the same information; in one case, it is to start a session using a menu item, in the other, it is to start the same session automatically at login time.

- 5250 Sessions

- Autostart a session with defaults

This field only appears if you select the Programs function of the Startup Setup Tasks. If this box is checked, a 5250 session will be started using defaults set in the 5250 function of the Programs Setup Task.

- Menu Item label

This is the text string that you want displayed on the button on the menu bar. This should be long enough for a good description but also short enough so that the menu button does not require too much space. If all the menu buttons take more space than the horizontal width available, a scroll bar is added to the menu bar in order to accommodate all buttons.

- AS/400 System

The name of the AS/400 system from which your 5250 session originates. The name can be the IP address or the IP hostname. This is an optional field if you are working from the Menus panel; in that case, the user is prompted for the host name at the time that he starts a session by clicking on this menu item. If you are working from the Programs panel, because you are defining an autostart session, then this is a required field.

- Window size and location in pixel (optional)

This function, if used, allows you to specify the size (width and height) and the location (Horizontal and Vertical offset and Corner to offset) of the 5250 window on your Network Station display.

- Other Parameters

For national language support.

- Add a 5250 Session

A click on this button opens up another set of input fields to enter a second 5250 session, etc.

- 3270 Sessions

- Autostart a session with defaults

This field only appears if you select the Programs function of the Startup Setup Tasks. If this box is checked, a 3270 session will be started using defaults set in the 3270 function of the Programs Setup Task.

- Menu Item label

This is the text string that you want displayed on the button on the menu bar. This should be long enough for a good description but also short enough so that the menu button does not require too much space. If all the menu buttons take more space than the horizontal width available, a scroll bar is added to the menu bar in order to accommodate all buttons.

- 390 System

The name of the System/390 system from which your 3270 session originates. The name can be the IP address or the name used in the domain name server table. This is a required field. Note that this does not have to be an actual S/390 if you are using a gateway to reach the S/390 host.

- Session Title

This text string appears on the 3270 sign-on screen as the session name. This field is optional and is case sensitive.

- Screen Size

This sets the size (width and height) of your 3270 session window. The choices are displayed by clicking on the down arrow in the list box. This selection determines the number of rows and columns displayed on your screen. For example, if you choose 43 X 80 instead of 24 X 80, more rows of data will be displayed, which generally means a smaller font with characters very close together and somewhat harder to read. Size of your display is also a factor to consider. Possible values are Default, 24 by 80, 32 by 80, 43 by 80, and 27 by 132.

- Graphics

This chooses whether to allow graphics capability with this 3270 session. Graphics is only available with a 32 X 80 screen size.

- Telnet port

The port number on the destination host to which this 3270 session connects. The default is 23. Other valid values range from 5001 through 65535.

- Other Parameters

For national language support.

- Add a 3270 Session

Clicking this button provides another set of input fields in which you can enable another 3270 session.

Some of the other settings that can be changed are:

- IBM Network Station Browser
- Sessions
- Navio NC Navigator
- Sessions
- Java Applets
- Java Application
- Remote Programs

## 9.2.1 Files Created by NSM for Startup Terminal Emulators

Here again are examples of the entries created by NSM in some configuration files as a result of the data we enter:

- We specify one 3270 Emulator to autostart for all the users, so we enter the following in the Startup Program System Defaults:

```
Autostart session with default.....Check box
System/390.....9.12.14.1
Session Title.....ITSO
```

The startup file drive:\nstation\userdata\sysdef\startup.nsm is updated to contain:

```
RUN ns3270 -title "ITSO" 9.12.14.1
```

- We also choose to give Mary a user button to start 5250 emulator with the ITSO's AS/400. We select user Mary from the Startup Menus User Defaults and we enter the following:

```
5250 Menu Items
Menu item label.....Start ITS0400
AS/400 System.....9.24.104.162
Session Title.....ITS0400
```

The file drive:\nstation\userdata\mary\startup.nsm now contains:

```
SOURCE /nstation/UserData/SysDef/startup.nsm
MENUITEM "Start ITS0400" ns5250 9.24.104.162 -title "ITS0400"
```

### 9.3 Using the IBM Network Station 3270 Emulator

Here is an illustration of a 3270 session started on a Network Station.

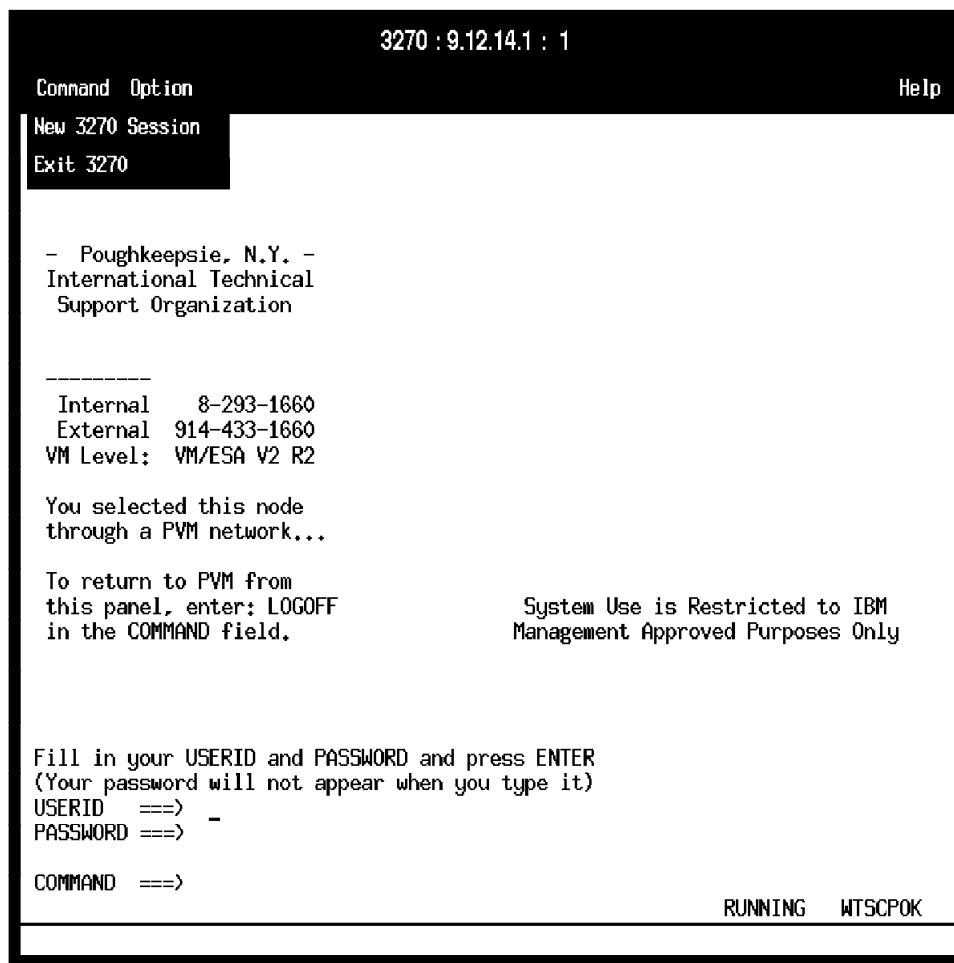


Figure 65. The IBM Network Station 3270 Emulator. The VM/ESA logon screen.

We do not explain here every detail of the IBM Network Station 3270 Emulator, as this has already been done in one of the other available redbooks, so we only highlight a few of the important aspects here.

- New 3270 session

Allows the start of additional 3270 sessions. There is no theoretical limit to the number of sessions that can be started simultaneously, but the limit will be a factor of the memory available on the IBM Network Station.

The user gets prompted for a host name. It can be a symbolic name or the numeric IP address of the host. You can also choose from several options for the screen size.

- Fonts
- APL2
- Bracket

This causes the left and right bracket characters to be translated to their correct ASCII representation. This function is particularly useful for C language programmers.



- Keypad
- Auto Action
- Block Cursor

This changes the cursor to a block or underscore character.

- Keyboard remapping

### 9.3.1 Copy and Paste

A useful facility of the 3270 Emulator is the possibility to copy data from a 3270 session in a clipboard buffer and then paste it in a different application and vice versa. This is true for every window on the IBM Network Station.

---

## 9.4 Configuring the IBM Network Station 5250 Emulator

Select **5250** from the Setup Task on the IBM Network Station Manager panel.

This brings up a new page where you can choose from **System defaults** or **User defaults**. Every parameter available for system defaults is also available for user defaults.

Select **System defaults**, then click on **Next** to display the window as shown in the figure below:

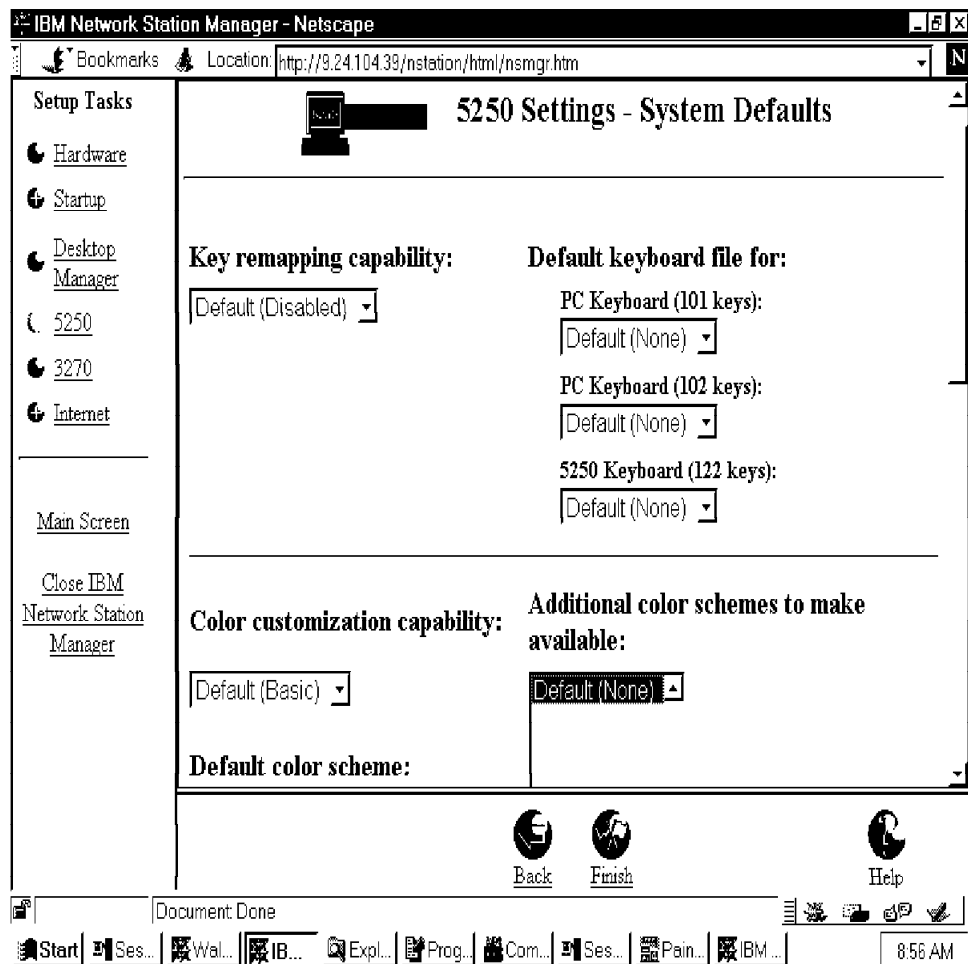


Figure 66. The IBM Network Station Manager. The 5250 emulator settings.

The following is a list of all the parameters you can update from this windows (use scrolling to see all the items).

- Key remapping capability

Determines if you want the user to have the ability to remap keys from the Option pull-down in the task bar of the emulation session. The default is Disabled. Note: "Disabled" means the user can see the Keyboard Remapping selection but cannot select it (grayed out). "Hidden" means the user will not see the Keyboard Remapping selection in the Options pull-down.

- Default keyboard file

Used to select which key remapping will be used with the 5250 session. You can select a default keyboard file for each of the three different types of keyboards: the 101, 102, or the 122. Which keyboard file gets used depends on the type of keyboard being used with the 5250 emulation session. The default for all three types of keyboards is None, meaning the default 5250 key mapping will be used.

- Color customization capability

Determines whether the user has the capability to create new color schemes (Advanced), use color schemes created by others (Basic), or be limited to

the default color scheme (use 5250 default or system default). The default is Basic.

- Additional color schemes

Determines the color schemes that will be available to users with basic or advanced color customization capability. If the system administrator has created additional color schemes, and made them available, they will appear in the pull-down list to select. The default is None, meaning not to use any color scheme.

- Default color scheme

Indicates which color scheme should be used when the 5250 emulation session is started. Users with basic or advanced color mapping capability may choose a different color scheme through the 5250 emulator menus. Also, if a default color scheme is specified within the 5250 emulator itself, it will override the specification of a default color scheme from the IBM Network Station Manager.

- Record/Playback capability

Determines if the user can use the 5250 emulator function of recording a series of keystrokes and then playing them back. The record and playback functions are located in the Options pull-down on the tool bar of the 5250 Emulation screen. On input-capable areas of the display screen, you can position your cursor and then access the record and playback functions. The value Playback only would let the user select preset playback sequences. The preset playback sequences are listed under Playback. The value Hidden would exclude this field from being presented to users. The default is Enabled.

- Playback sequences to make available

Contains the Playback sequences that will be made available to users with enable or playback only capability. The Record function is available in the Options pull-down on the tool bar of the 5250 Emulation screen for users with enabled playback capability. The default is None, meaning you don't want to make any playback sequences available.

- Screen size

Used to select the size (number of rows and columns) that you want your 5250 session to use. Possible values are 24 by 80 and 27 by 132. The default value is 27 by 132. Whatever value is selected, that value becomes the default when working with 5250 sessions in the Programs or Menus function of Startup.

**Note:** Selecting 27 x 132 does not give you 27 x 132 unless the monitor screen is capable of supporting that size.

- Image/Fax

This increases the memory requirements for a 5250 Emulation session. The default is Disabled, meaning you cannot display image files or faxes.

- Column separators

Enables or disables displaying column separators between certain types of fields. The default is Disabled.

- Allow use of the pop-up keypad

Specifies if users can use the pop-up keypad. The pop-up keypad contains PF keys 1 through 24. If a particular keyboard has some PF keys mapped to perform functions different from the regularly mapped PF keys, users could access the pop-up keypad and press a PF key and the function the PF key is mapped to perform is run. The default is No.

- Allow use of the control menu

Allows you to enable or disable the menu bar Control choice. Selecting a key within the Control option from the menu bar performs the same function as if you pressed this key on your keyboard. The default is Yes, meaning you can select from the Control pull-down.

- Allow use of the Edit menu

Allows you to enable or disable editing (copy, cut, and paste) functions. The default is Yes. Copy data using the Edit menu, in two steps. First mark the data by placing the mouse pointer on the first character; while holding the left mouse button down, drag the mouse to the last character to be copied and release the button. Then, click on **Copy** in the **Edit** menu to copy the marked data to the clipboard buffer. The data in the buffer can later be pasted into this or a different session.

- Allow use of the Command menu

Allows you to enable or disable the menu bar Command choice. The default is Yes. If the Command function is disabled (No), users will not be able to access new 5250 sessions or exit a 5250 session using the 5250 Command menu.

- Show New Session Window

When Yes is the specified value, users will see the New 5250 Session dialog box. When No is specified, the New 5250 Session dialog box will not be presented.

- Allow use of Local Print

The Local Print function determines if users can access the Local Print function. The default is Yes. Local Print, when used, prints the contents of the current screen. Local Print is accessed by clicking on the **Print** pull-down and selecting **Local...**

Click on **Finish** to complete the 5250 setup.

### 9.4.1 Files Created by NSM for 5250 Emulator Settings

- In the 5250 System Default, we entered:

Image/Fax display.....Enabled

This updated the file drive:\nstation\userdata\sysdef\NS5250\pref with:

NS5250\*ImageView: enable

- Then we selected user sarah on the 5250 User defaults page and entered:

Key remapping capability.....Enabled

The file drive:\nstation\userdata\sarah\NS5250\pref is updated with:

NS5250\*KeyRemap: enable

## 9.5 Using the IBM Network Station 5250 Emulator

Here is an illustration of a 5250 session started on the Network Station:

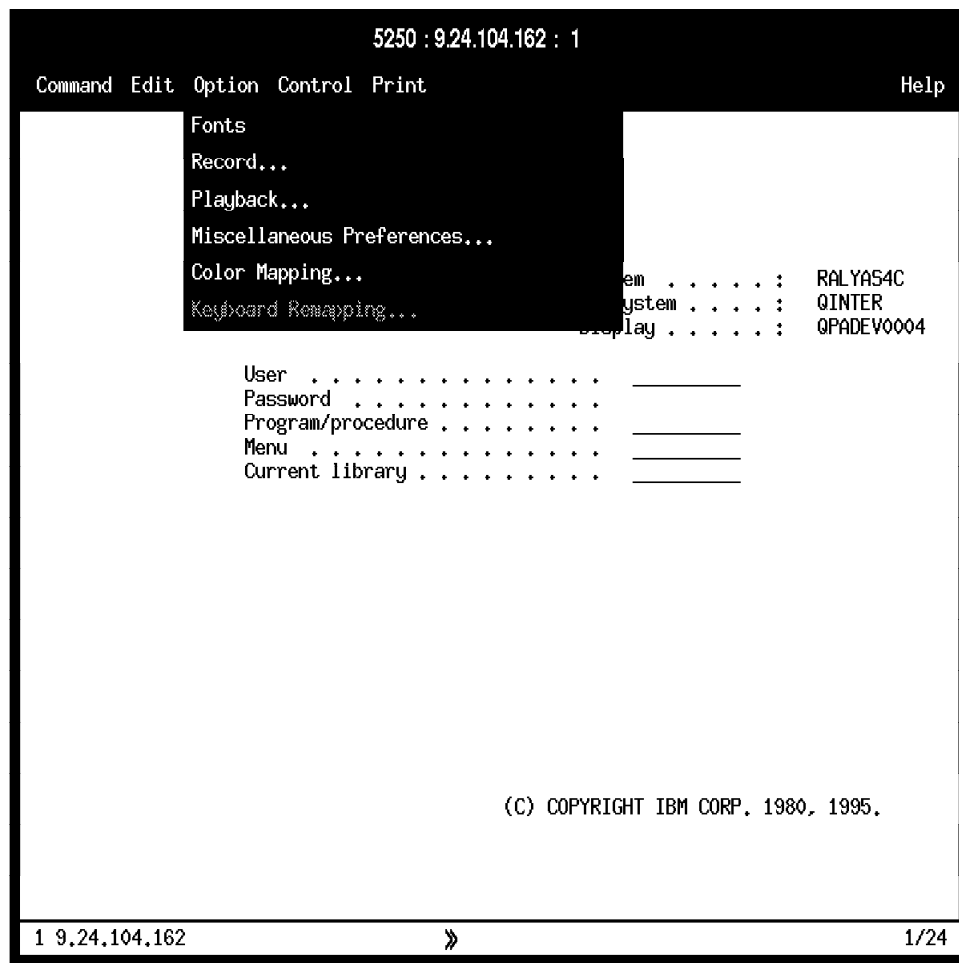


Figure 67. The Network Station 5250 Emulator. The Options menu.

Here are some of the options available from the pull-down menus:

- New 5250 session.

Allows the start of additional 5250 sessions. There is no theoretical limit to the number of sessions; this is limited by the amount of memory available on the IBM Network Station. You are prompted for host name; it can be a symbolic name or the numeric IP address of the host.

- Edit.

From this menu you can choose Paste, Copy and Cut.

- Option

From this menu you can choose Fonts, Record, Playback, Miscellaneous Preferences, Color Mapping and Keyboard Remapping.

- Control.

From this menu you can choose Reset Key, System Request Key, Attention Key, Help Key and Enter Key.

- Print.

From this menu you can choose Local or System.

### **9.5.1 Copy and Paste**

A useful facility of the 5250 emulator is the possibility to copy data from a 5250 session to the clipboard buffer and than paste it into a different application and vice versa. This is true for every window on the IBM Network Station.

---

## Chapter 10. Network Station Browsers

The IBM Network Station provides two native Web browsers:

- The IBM Network Station Browser
- The Navio NC Navigator

A typical administrator would likely install only one browser for use on the IBM Network Station, but we chose to install both in order to compare them.

These Web browsers are specifically designed to execute on the IBM Network Station as native applications after they are initially loaded from a boot server. Both browsers are Java and Javascript-enabled and have most features of the popular browsers.

The Navio NC Navigator is a special version of the Netscape 3.0 browser which has been modified to run on the IBM Network Station, so its operation is equivalent to its well-known Netscape counterpart. The IBM Network Station Browser is a simpler browser based on Mosaic.

Because the IBM Network Station has no local disk storage, the local data, such as bookmarks for example, are stored in files residing on the boot server.

We discuss here a few of the important configuration elements necessary to get these browsers to work on the IBM Network Station.

---

### 10.1 Configuring for Using the Browsers

In order for the Network Station browsers to function properly, they require some configuration parameters to be set properly.

First, the traditional IP parameters such as the IP address of the Network Station, the network mask and the default router must have been properly defined. These are usually obtained from the setup utility in NVRAM, if using the NVRAM method of booting, or from a DHCP server.

In addition to these, there are three parameters that must be set:

- The Domain name server(s) address

In order to properly resolve URLs, your Network Station must have access to a domain name server.

This currently cannot be configured using the Network Station Manager and must therefore be supplied to the Network Station through either:

- A DHCP server, if one was used for booting the Network Station
- Manually including the following statements in one of the configuration files (we recommend default.dft or hosts.nsm)

```
set tcpip-name-server-protocol = dns
set tcpip-name-servers = {
    {9.24.104.108}
    {9.24.104.209}
}
```

- The default domain name

At the moment, this parameter cannot be set using the Network Station manager or DHCP. Therefore, this statement should also be included in your configuration file, as we did for the DNS server address.

```
set tcpip-dns-default-domain = itso.ral.ibm.com (as an example)
```

- The SOCKS or proxy server address (if required in your network).

In most cases, a SOCKS server or proxy is required to go from your intranet to the World Wide Web.

The preferred way to configure this is to use the Network Station Manager. This parameter is located in the Internet Setup task, under the Network subtask.

The statements that are added to the startup files by the Network Station Manager would be similar to the statements below:

```
SET SOCKS_HOST socks1.server.ibm.com
SET SOCKS_PORT 1080
```

If you configured the above statements at the system level, applicable to all users, these statements would be added to the  
\\nstation\\userdata\\sysdef\\startup.nsm file.

Here is an example of using the IBM Network Station Manager to set these parameters:



Figure 68. The IBM Network Station Manager - Internet Menu



A click on **Internet** in the setup tasks of the IBM Network Station Manager (see figure above) opens up the following subtasks:

- Network
- IBM Browser
- Navio NC Navigator
- Applet Viewer

Selecting **Network** brings you the panel below, where you can choose from **System Defaults** or **User Defaults**. Every parameter available for System defaults is also available for User defaults.

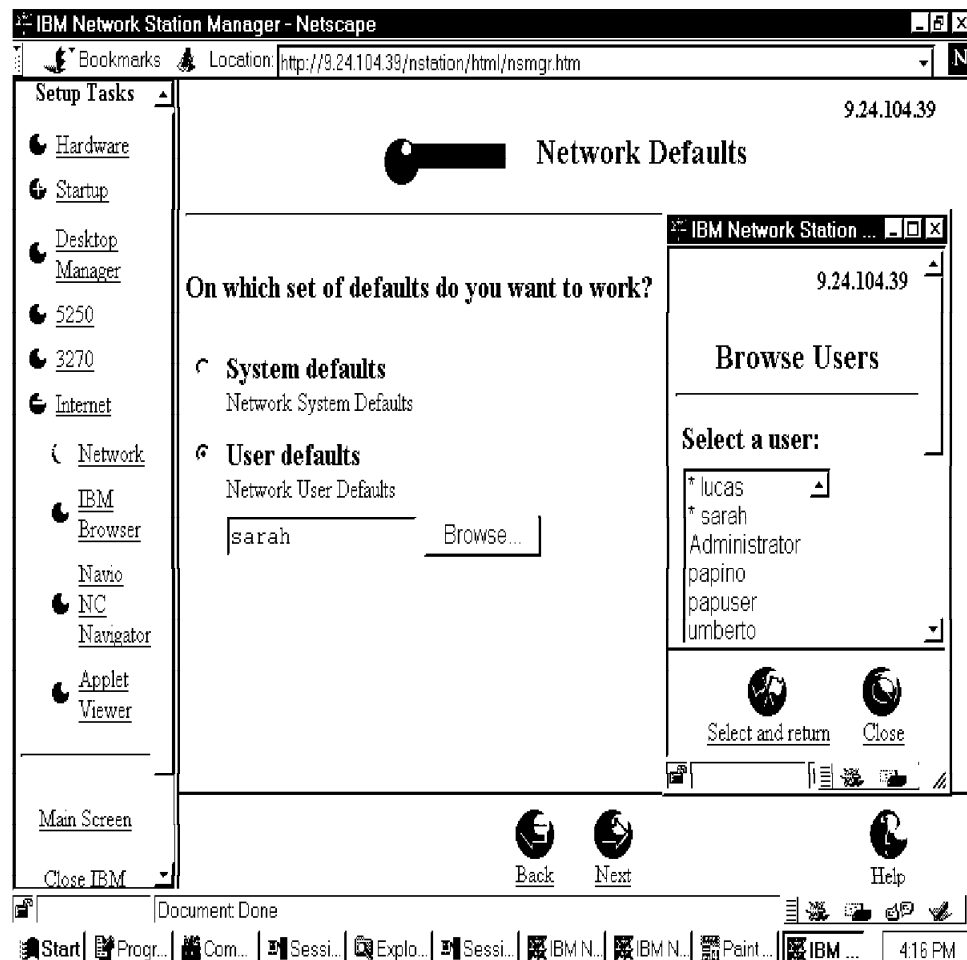


Figure 69. The IBM Network Station Manager - Network Default Settings

Select **System Defaults** then click on **Next** to get the panel shown below, where you can specify your SOCKS server or proxy server.

Please note that these settings can be viewed using the pull-down menus on the Network Station browser but they cannot be changed from the browser; they can only be changed in this Network Station Manager panel or by manually editing the resulting startup file.

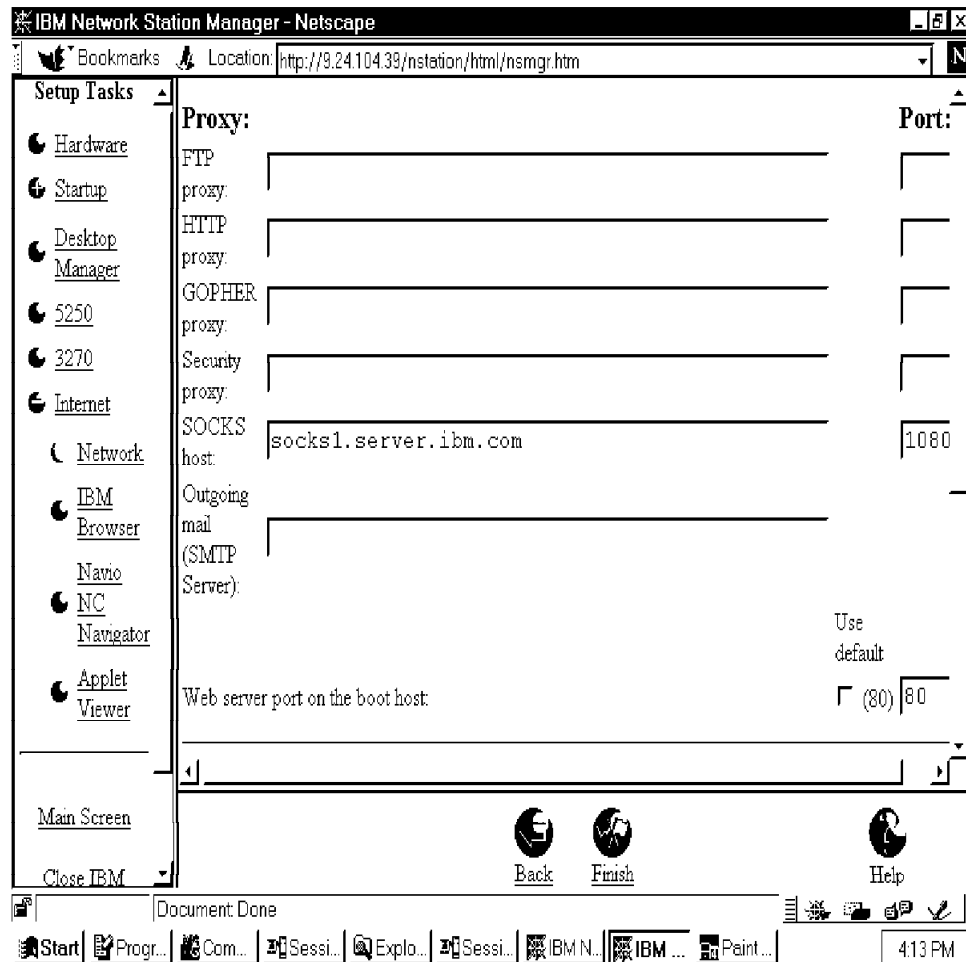


Figure 70. The IBM Network Station Manager - Network Customization

**Note:** The network settings specified on this panel are shared with other Internet-related applications such as Java and the IBM Network Station browsers.

The following is a list of the parameters you can update from this windows (scrolling to see the other parameters).

- User's name  
This would normally only be used when specifying user defaults.
- e-mail address  
The e-mail address field is used for specifying the Internet e-mail address of the user; should also be used only on a user default specification.
- Reply to address  
Specifies an e-mail address at which this user can receive e-mail as an alternative to the users regular EMail address. Typically this would be the same as EMail address.
- Home page
- FTP proxy
- HTTP proxy

- GOPHER proxy
- Security proxy

Proxy servers are used to enable selective access to services. The main purpose of proxies is to break the TCP/IP connection and hide the internal network information from outside access and intervention. Using proxies provides security to your system but does have a performance cost by having requests routed through the proxy.

If you are not using proxies of any kind, then there is no need to define them in the Network settings.

- SOCKS host

The SOCKS host field is used to specify the name of the SOCKS host and port to be used. The SOCKS security application running on the SOCKS host allows applications which have been SOCKS enabled to successfully access TCP/IP services beyond the SOCKS host. The services can include telnet, Web browsing, FTP, and other applications that have been SOCKS enabled.

- Outgoing mail (SMTP Server)
- Web server port on the boot host
- No FTP proxy
- No HTTP proxy

The No proxies configuration function means that no proxies will be used for the browser users. If you have a firewall in place, users will not be able to connect to any URLs outside of your network's firewall.

- No GOPHER proxy
- Applet launcher port
- IBM Network Station Browser Version

The IBM Network Station browser version field is used to specify which version of the IBM Network Station browser will be used. You can choose encrypted or nonencrypted. The difference between the versions is the level of encryption. The level of encryption determines the security level of transactions performed by users of the IBM Network Station Browser. The default is nonencrypted. Encrypted provides a 40-bit security algorithm for Internet transactions.

Click on **Finish** to complete the network setup.

### 10.1.1 Files Created by NSM for Network Settings

- The data we entered in Figure 70 on page 122 added the following statements

```
SET SOCKS_HOST socks1.server.ibm.com
SET SOCKS_PORT 1080
```

to the drive:\nstation\userdata\sysdef\startup.nsm file.

- We then selected the user **sarah** on the Network - User Default page, and we entered data in home page filed, as shown in the figure below:

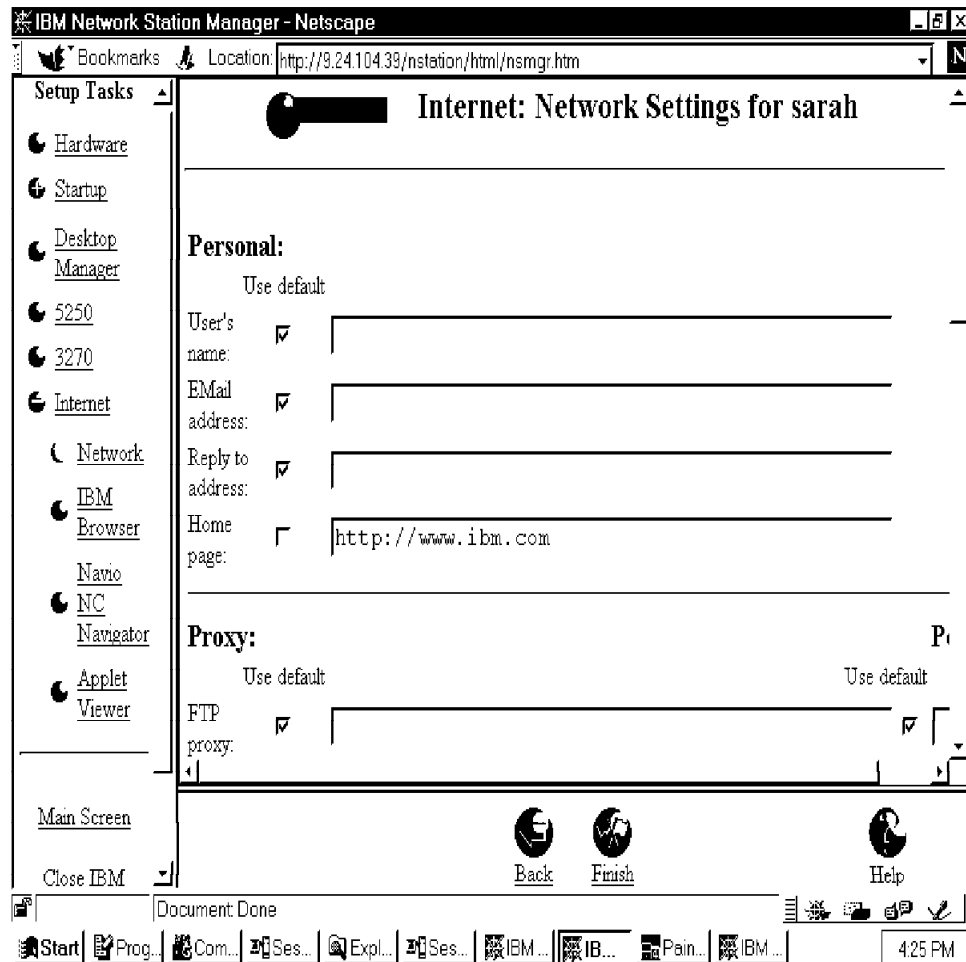


Figure 71. The IBM Network Station Manager - User Setting - Network

This causes the above URL to be automatically searched when the user Sarah starts the IBM Network Station browser.

The file drive:\nstation\userdata\sarah\startup.nsm is updated with the following entry:

```
SET HOME_PAGE http://www.ibm.com
```

## 10.2 Configuring the IBM Network Station Browser Using the NSM

Each of the available browsers on the Network Station should be configured first using the Network Station Manager. Note that there are some configuration that can be done on the browser itself, by the user, when he uses it, but this is more a setting of user preferences than a base browser configuration.

Select **IBM Browser** in the Internet Setup task in the Network Station Manager, select **System Defaults** and click on **Next** to display the panel shown below:

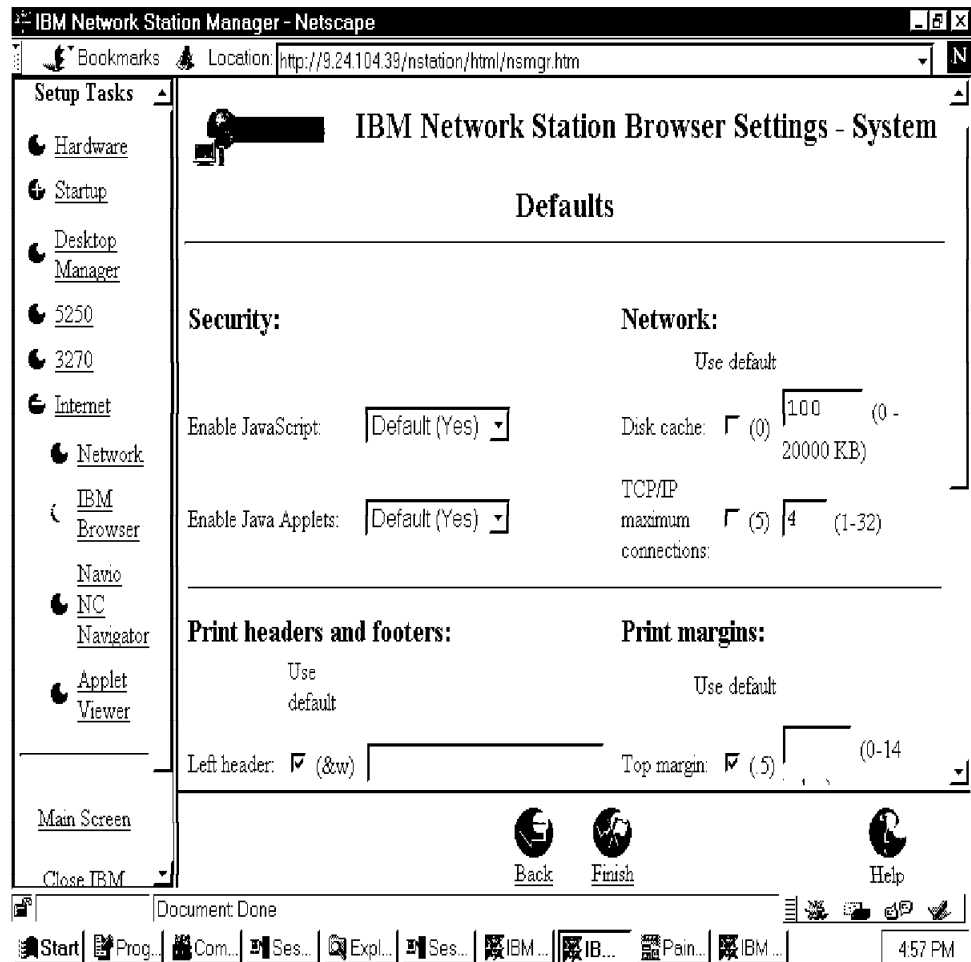


Figure 72. The IBM Network Station Manager - NSB Customization Page

The following is a list of the parameters you can update from this windows.

- Security:
  - Enabling Java Script
  - Enabling Java Applet
- Network:
  - Specifying disk cache size

The Disk cache function specifies the size, on the NT system, in kilobytes, of the disk space available for caching. The default is 0 kilobytes. When a document (text and images) is displayed on the monitor attached to the IBM Network Station, the document is cached on the host system (in our case the Windows NT Server if Disk cache function is being used).

From a disk space management perspective, keep in mind that whatever size you specify is multiplied by the number of IBM Browser users. For example, if you have 10 browser users and the Disk cache value specified is 2000 KB, you may use up to 20,000 KB or 20 MB of disk space on the NT Server for caching purposes.

We elected to supply 100 KB of disk cache for every user, and to monitor this value and to adjust it during performing session.

- Specifying the number of TCP/IP connections.

Specifies the maximum number of simultaneous TCP/IP connections that the IBM Network Station Browser can use. This is equivalent to the number of simultaneous sessions or windows of the browser.

- Miscellaneous:
  - How the images will be handled by the browser.
  - Whether to allow a toolbar for users.
- Print headers, footers, and paper size:
  - Determining the position and the composition of headers and footers.
  - Determining the paper size on which to print.

- Print margin.

- Preference settings.

Enables the System Default settings for the IBM Network Station Browser to be overridden for a specific user ID.

Overriding the Preference settings can be done by either the IBM Network Station administrator (using the IBM Network Station Manager program), or by an end user through the User Preferences menu item on the Edit pull-down menu of the IBM Network Station Browser.

- Determining print margins (top, bottom, left and right).

Click on **Finish** to complete the IBM Network Station Browser setup.

## 10.2.1 Files Created by NSM for IBM Network Station Browser Settings

Here are a few examples of the updates to the configuration files produced by the NSM when updating data relative to the IBM Network Station browser.

- For example, we elected to supply 100 KB of disk cache for every user; we specified, in the IBM Network Station Browser Setting System Default page:

```
Disk cache:                100 KB
TCP/IP maximum connection:    4
```

As a result, the drive:\nstation\userdata\sysdef\nsb\pref file contains:

```
NSB*Disk_CacheAAAenable_disk_cache: TRUE
NSB*Disk_CacheAAAmain_cache_kb_size: 100
NSB*Unix_TCPAAAmx_connections: 4
```

- Then we selected the user sarah from the IBM Network Station Browser Setting User Default page, and we specified:

```
Show toolbar:    No.
```

The file drive:\nstation\userdata\sarah\nsb\pref was updated with:

```
NSB*NSBAAAShow_Tool_Bar: FALSE
```

## 10.3 The Java Applet Viewer

**Note:** You might notice some slight differences in the display of an HTML page when displaying on an Intel-based platform such as Windows and when displaying on an IBM Network Station, which has a UNIX base.

The reason is that the Java Development Kit (JDK), which is the basis for all the Java environments, has a different version for Intel and for UNIX, and there are some slight inconsistencies between the two versions.

If you create code on Windows 95 or Windows NT and it works differently on the IBM Network Station, in many cases it will also work differently on any UNIX based operating system including IBM's AIX and Sun's Solaris.

Notice, in the figure below, the look of the choices, that is text, surrounded by a rectangular box with a small rectangle on the right-hand side of the box for the user to click on.

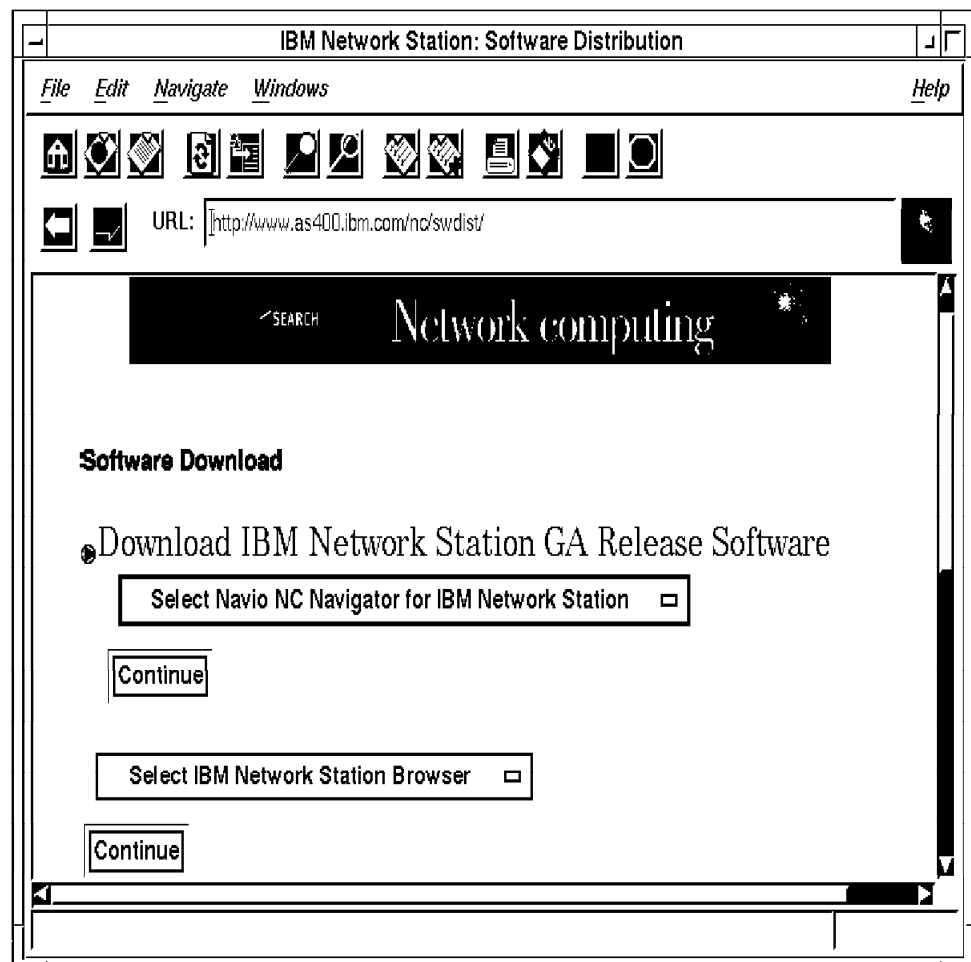


Figure 73. A Web Page on the IBM Network Station

Now compare the figure above with Figure 1 on page 14 in the installation chapter, where we used a browser on a Windows NT server to download the software. Notice the slight difference in the user interface components such as buttons and entry fields. This is due to the fact that the native operating

environment's windowing system is called to display the user interface with a "native look and feel".

This means that from a UNIX base, the user interface components call the Motif library routines, but on a Windows base, the Windows library routines are called.

For example, in the figures we just referenced, the selection menus (using the Choice class) on UNIX based systems display with a square box with a line in the middle, and clicking the square displays the choices. On a Windows based systems, the selection menu is displayed with a down arrow, where clicking the arrow displays the selection list.

### 10.3.1 Configuring the Java Applet Viewer

Select **Applet Viewer** in Internet Setup tasks, and **System Defaults**, then click on **Next** to display the figure below:

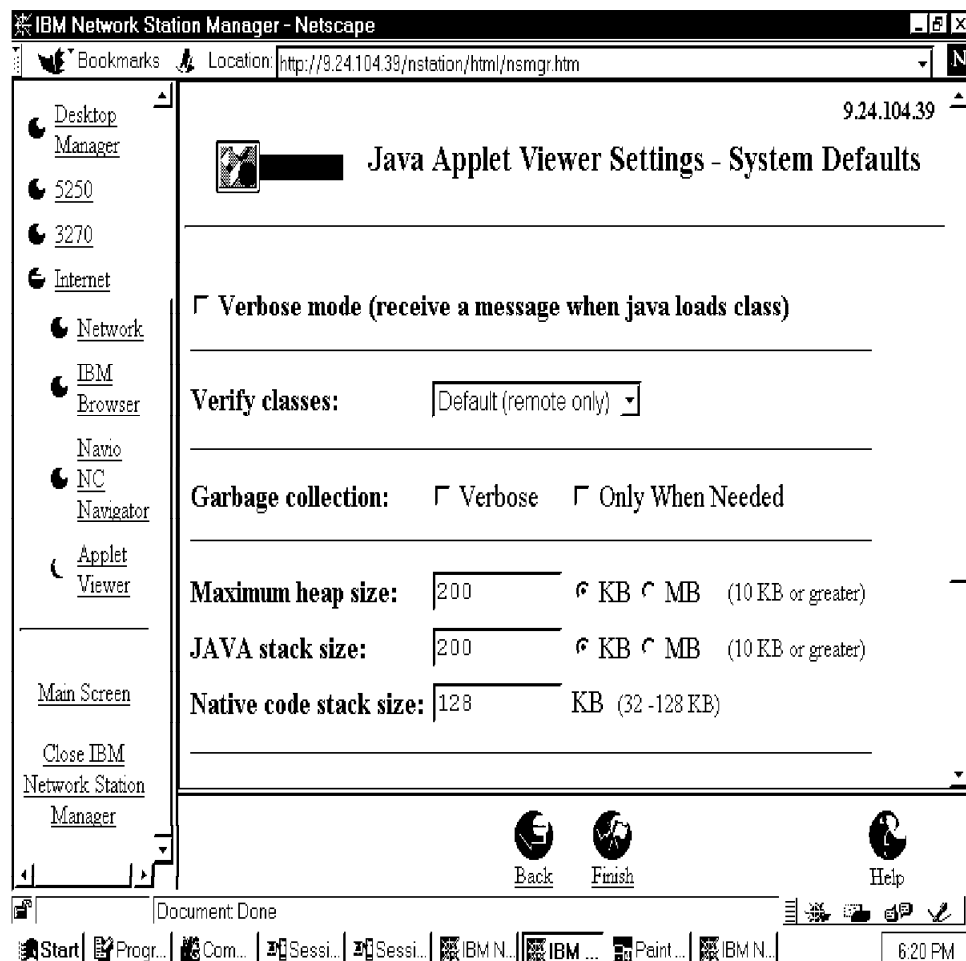


Figure 74. The IBM Network Station Manager - Java Applet Viewer

The following parameters are available on this window:

- Verbose Mode.
- Verify classes.

The Verify classes function ensures that the byte code for each class being loaded is constructed to Java language semantics requirements. By



verifying the byte code, you ensure that Java applications do not access information they are not authorized for.

- Garbage collection.

The Garbage collection function is the process of identifying and reclaiming the memory of freed Java objects. Garbage collection may be initiated by the system at unspecified intervals even though memory may be currently available. In order to disable this behavior, select the option **Only When Needed**; in this case, garbage collection will only occur when the system is out of heap space.

- Maximum Heap Size.

Specifies the maximum size of the memory allocation pool the interpreter uses for dynamically allocated objects and arrays.

- Java Stack Size.

The Java stack size function specifies the maximum size of the stack for running Java code for each thread.

- Native Code Stack Size.

The native code stack size function specifies the maximum size of the stack for running native C or C++ code for each thread.

- Properties.

**Note:** Assigning storage to parameters above affects the amount of memory available on the IBM Network Station to run non-Java applications.

Click on **Finish** to complete the Java Applet Viewer System setup.

### 10.3.2 Files Created by NSM for Java Applet Viewer Setting

We configured the following data for the Applet Viewer:

Maximum heap size:.....200 KB

Java stack size:.....200 KB

Native code stack size.....128 KB

The result, in the drive:\nstation\configs\default.nsm file is:

```
set java-appletviewer-command="java -oss200k -ss128k -mx200k
ncd.applet.NCDAppletViewer"
set pref-screensaver-enable=true
set pref-screensaver-time=3000
```

---

## 10.4 Starting the IBM Network Station Browser

As with the other applications already discussed, you have the choice of autostarting a browser or putting an item on the menu bar to let the user launch the browser when he needs it.

- Autostarting an IBM Network Station Browser

In the Network Station manager Setup tasks list, select **Programs**, then **System Defaults**, then click on **Next** and scroll down to where you see the entries for the browsers, as shown below:

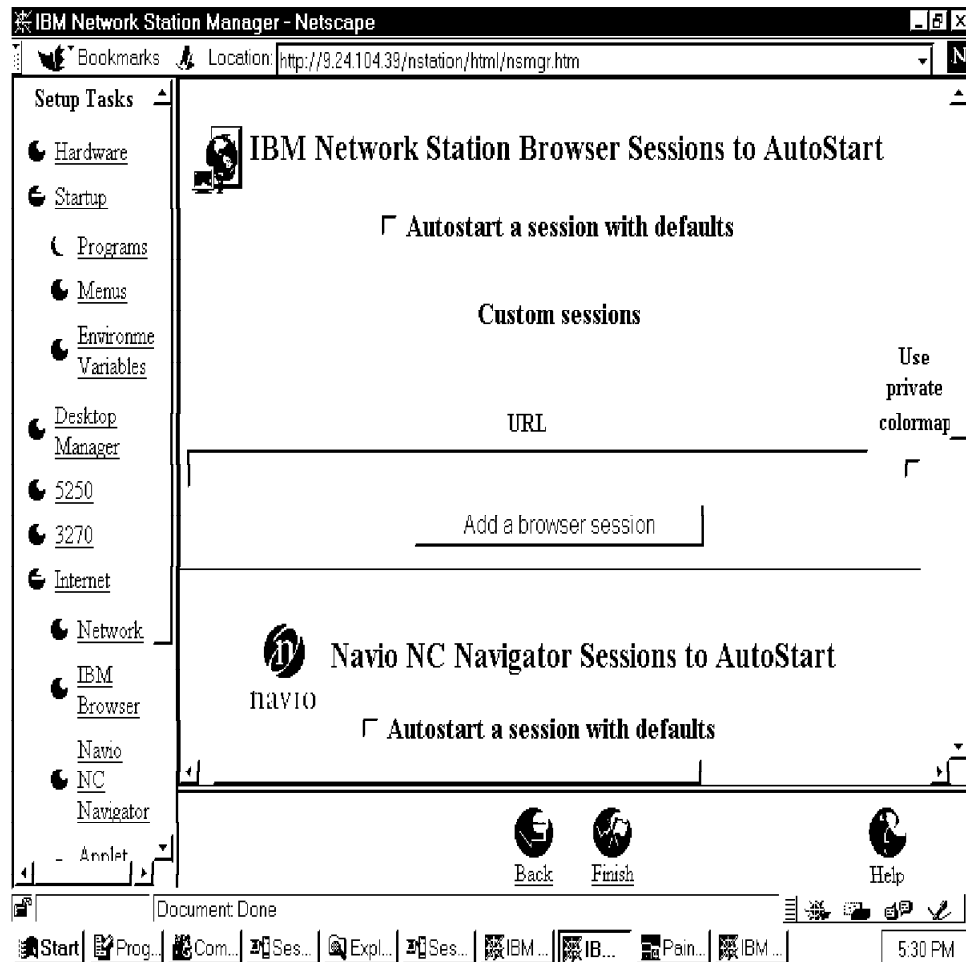


Figure 75. The IBM Network Station Manager - Startup Programs - Browsers

On this panel, all that is required is to check the checkbox labeled **Autostart a session with defaults**. The defaults used will be the ones which have been previously configured in the Network Setup task.

If you do not want to use these defaults, you can then specify here the URL desired for this session to be autostarted.

The private colormap field enables the browser to allocate its own color table. This allows the browser to display more colors than are typically available. By default, all applications share the same color table. The private colormap function can have unpredictable side effects when used. This function should only be used when specific color problems occur while viewing the contents of the browser.

The Add a browser session button provides another set of input fields in which you can enable another IBM Network Station Browser session.

For the Navio browser, the fields are the same as the IBM Network Station Browser, but it also has a field to specify the window size and location.

- Setting up a menu item to start a browser

To set up a menu item for a browser, click on **Startup**, then on **Menus**, select **System Defaults**, then click on **Next** and scroll the window down to where you see the browser entries, as shown below:

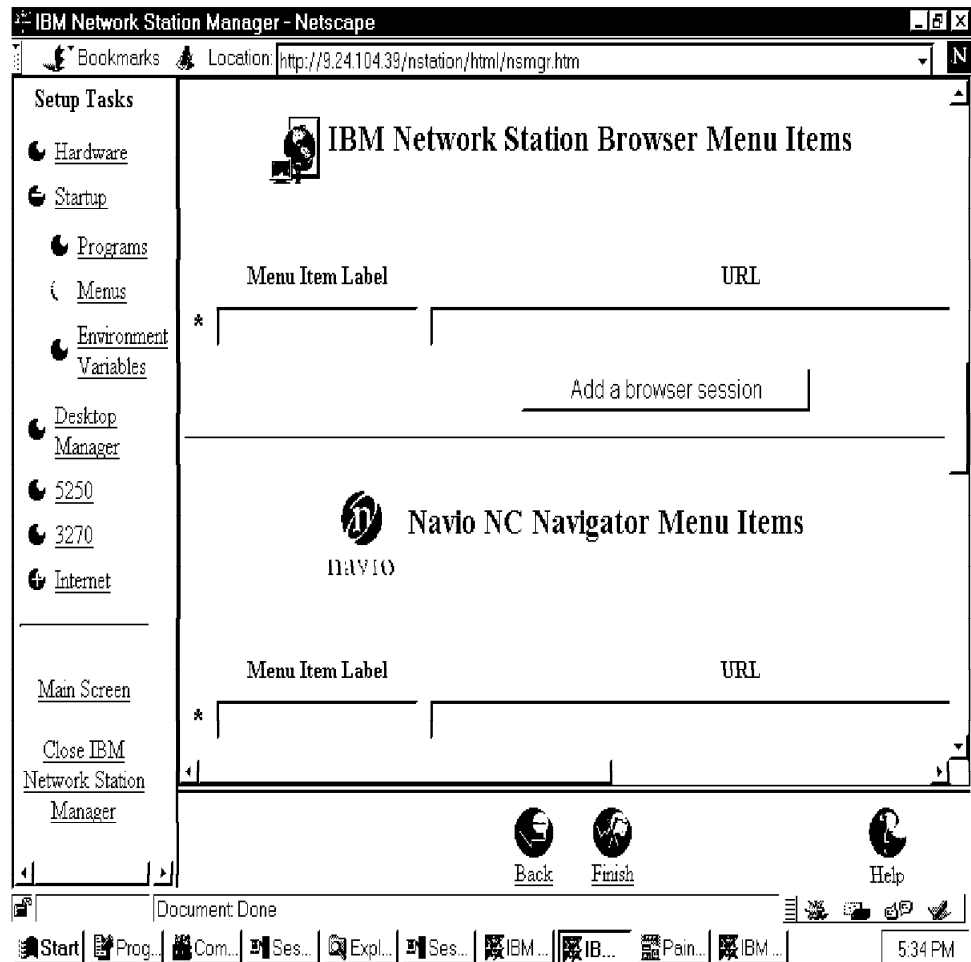


Figure 76. The IBM Network Station Manager Startup - Startup Menu - Browser

The parameters available here are similar to those we just saw above in the autostart specifications. The only field that is different is the Menu Item Label where you specify the text string that you want to appear on the button on the menu bar.

#### 10.4.1 Files Created by NSM for the Browsers Startup Settings

We have entered, in the above panels, for both the startup and the menu items, entries to autostart one session for each browser (with a URL of WWW.IBM.COM and WWW.NAVIO.COM respectively), and entries to have a button on the menu bar labeled IBM Browser and Navio browser.

For the system defaults, the file drive:\nstation\userdata\sysdef\startup.nsm was updated with the following statements:

```
MENUITEM "IBM Browser" loadb nsb
MENUITEM "Navio" loadb navio
RUN loadb nsb -url http://www.IBM.com
RUN loadb navio -url http://www.NAVIO.com
```

If we had entered the same data at the user defaults level for a user named sarah, the same above lines would have been added to the drive:\nstation\userdata\sarah\startup.nsm file.

## 10.5 Using the IBM Network Station Browser

As previously stated, a browser can either be autostarted after the user logs in, or started by the user from the menu bar.

Once started, the operation of these browsers is similar to any typical browser on other platform. However, one main difference is the absence of local disk storage to store user preferences, and bookmark entries for example. Such user preferences and bookmarks are stored in files that reside on a server.

We will take a look here at some of the files used by these browsers to store preferences.

Note that a browser, once it has been started on the Network Station, can continue to operate even if the boot server from which it was loaded is down. However, the browser would be unable to store new bookmarks, or store new preferences until the server was available again.

Let's take a look at some common tasks.

To customize User Preferences, choosing **User Preferences** from the **Edit** pull-down menu brings up the panel below:

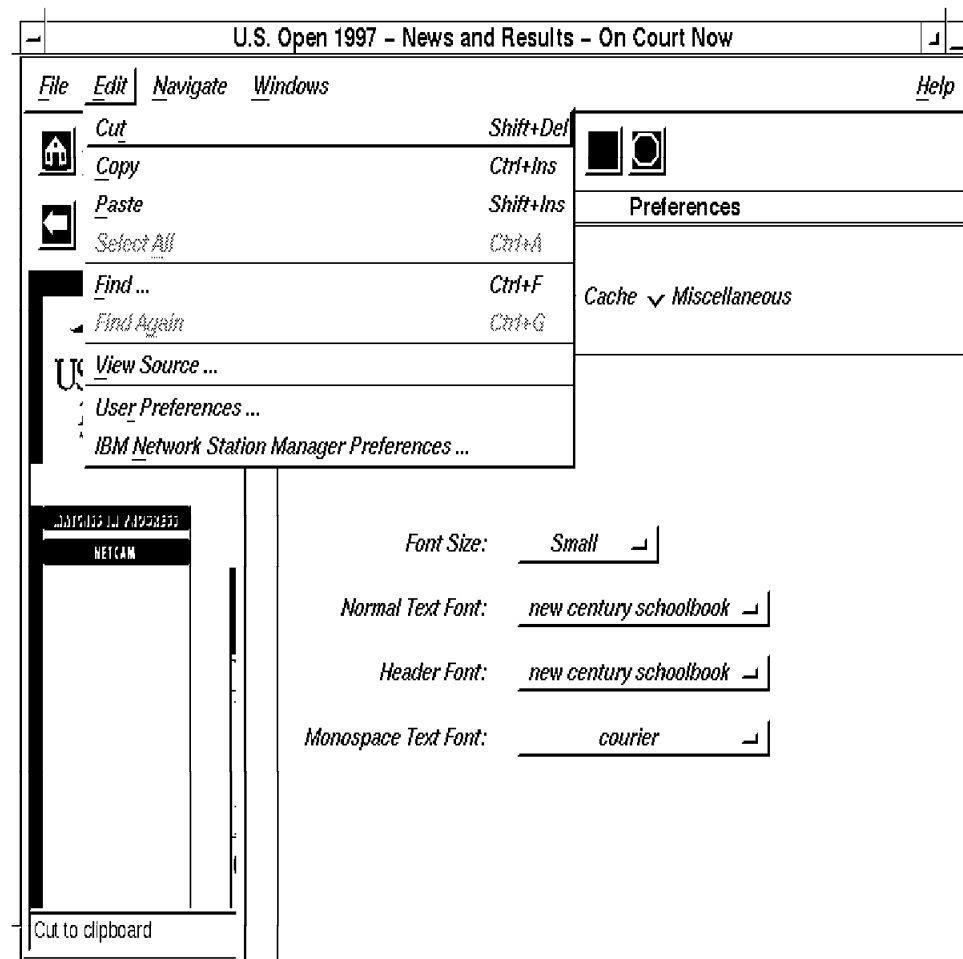


Figure 77. The IBM Network Station Browser. The User's Font Preferences.

There are five categories of preferences that can be selected on that panel:

- Fonts
- Colors
- Printing
- Cache
- Miscellaneous

The fonts preferences is pre-selected as the first choice (as shown in the panel above). Most of the options here may be changed by the user; however, there are some that require authorization from the administrator through the Network Station Manager.

**Note:** When you are configuring the IBM Network Station Browser using the IBM Network Station Manager, there is an entry for Preference settings. The Preference settings function enables the System Default settings for the IBM Network Station Browser to be overridden for a specific user ID.

- The Fonts Panel

From this panel the user can change the size and type of fonts for three types of text. There are five different sizes of fonts. They are: Very Small, Small, Medium, Large, and Very Large. There are seven font types: Courier, Helvetica, Lucida, Lucidabright, Lucidatypewriter, New Century Schoolbook, and Times. The three different types of text are: Normal Text, Header, and Monospace Text.

- The Colors Panel

From this panel the user can set the colors of the document text, background, links, and visited links. The user can also choose to ignore document attributes. This causes the documents that are loaded to take on the colors set by the user, not the ones specified in the document.

- The Cache Panel

This panel has information about the cache size limit, which is set by the IBM Network Station Manager, and the current cache size. The user can flush the cache and set the browser to verify the cache: Always, Once Per Session (the default), or Never.

- The Printing Panel

This panel has information about the margins and headers. These values may be changed only if the IBM Network Station Manager sets the override; otherwise they are read-only. In addition, there are two values which may be changed by the user. They are the Header Font Size and the Paper Size.

- The Miscellaneous Panel (shown below)

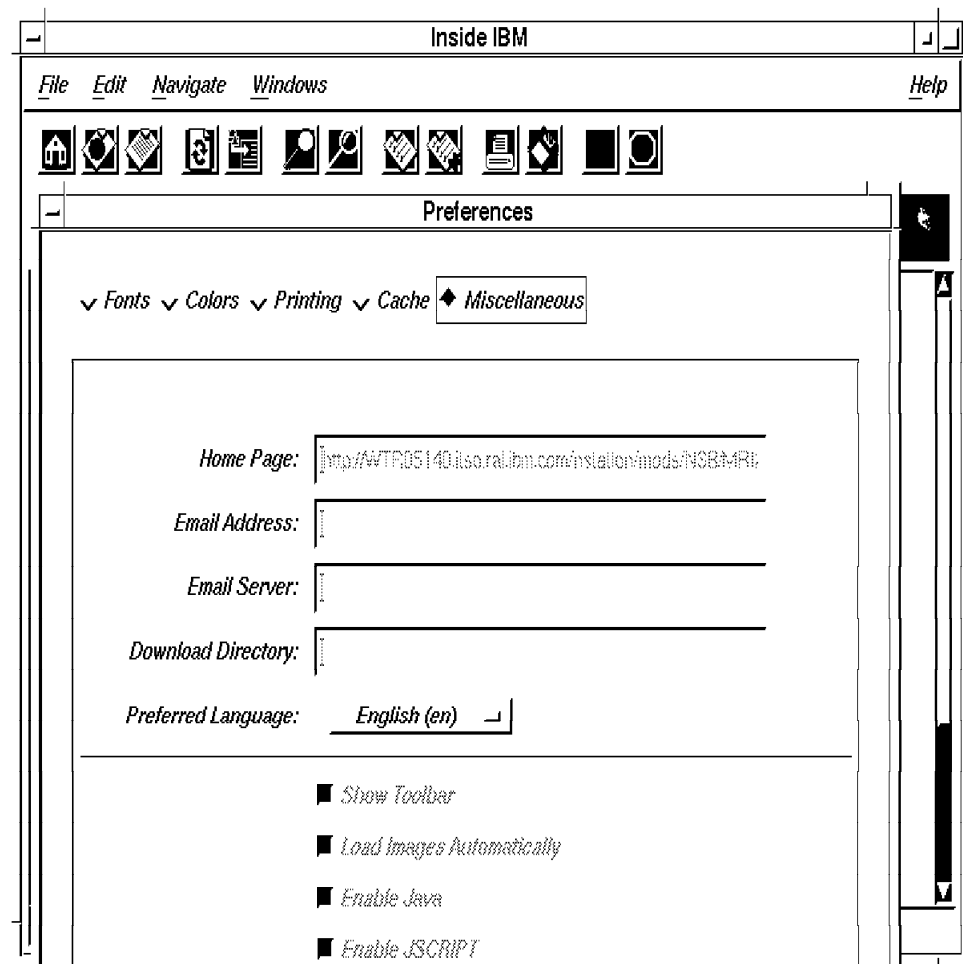


Figure 78. The IBM Network Station Browser - User's Preferences

In this panel there is a variety of information such as:

- Home Page.

This may be changed only with authorization of the administrator through the IBM Network Station Manager.

- Email address.
- Email server.
- Download directory.

The download directory is defaulted to the user's home directory, but may be changed by the user.

- The Preferred Language.

Finally there are four check boxes at the bottom. They are: Show Toolbar, Load Images Automatically, Enable Java, and Enable JSCRIPT. These are set by the Network Station Manager unless the override is set for the user to select.

## 10.5.1 Hot List

The hotlist is where you can save the titles and URL's of your favorite Web documents.

To add the current file to the hotlist, click on **Navigate**, choose **Add Current to Hotlist** or click the **Add Current to Hotlist Toolbar Button**.

## 10.5.2 Saving Files

To save the current document:

1. Click **File**, choose **Save As** or click the **Save** icon.
2. Specify the name and location of the saved file.
3. Set the file type format to Plain Text, or HTML if you want to include the HTML tags.
4. Choose the **OK** button.

To save an Inline image:

1. Click the image with the right mouse button.
2. From the pop-up menu, choose **Download Image to Disk**.
3. In the Unknown Type pop-up, specify the path and file name.
4. Choose the **OK** button.

## 10.5.3 Starting Multiple Network Station Browser Windows

To start multiple IBM Network Station Browser windows, within the browser select **File** and then select **New Window**.

The number of multiple browsers are limited by:

Max TCP/IP connections

which was set in the browser configuration.

## 10.5.4 Files Created by the IBM Network Station Browser Operations

We have set some user preferences and saved them from the IBM Network Station Browser in order to verify where the browser stores these changes on the server.

- When a user logs on to the IBM Network Station, a folder with his user ID as a name is created (if doesn't exist) on drive:\users\userid. In our example, we logged on as user umberto, so a drive:\users\umberto file was created.
- After starting the IBM Network Station Browser, a file called drive:\users\umberto\nsb\nsb-viewers-default is created, which contains the following entries:

```
# eMosaic Viewers 2.0
MIME: audio/x-wav
Description: WAVE Files
Suffixes: .wav
Encoding: binary
ViewerApp: VOID
Present: SAVE
MIME: image/tiff
Description: TIFF Images
```

Suffixes: .tiff .tif  
 Encoding: binary  
 ViewerApp: VOID  
 Present: SAVE  
 MIME: application/postscript  
 Description: PostScript Files  
 Suffixes: .ps .eps .ai  
 Encoding: 8bit  
 ViewerApp: VOID  
 Present: SAVE  
 MIME: video/mpeg  
 Description: MPEG Files  
 Suffixes: .mpeg .mpg  
 Encoding: binary  
 ViewerApp: VOID  
 Present: SAVE  
 MIME: video/quicktime  
 Description: QuickTime Files  
 Suffixes: .qt .mov  
 Encoding: binary  
 ViewerApp: VOID  
 Present: SAVE  
 MIME: video/x-msvideo  
 Description: Microsoft Video Files  
 Suffixes: .avi  
 Encoding: binary  
 ViewerApp: VOID  
 Present: SAVE  
 MIME: application/pdf  
 Description: PDF Files  
 Suffixes: .pdf  
 Encoding: binary  
 ViewerApp: VOID  
 Present: SAVE  
 MIME: application/zip  
 Description: Zip Files  
 Suffixes: .zip  
 Encoding: binary  
 ViewerApp: VOID  
 Present: SAVE

- Then we went to Yahoo Web site and saved the home page as yahoo.htm. This created a file called drive:\users\umberto\nsb\yahoo.htm.
- We then added this page to our hot list; this action created a file called drive:\users\umberto\nsb\.\nsb-hotlist-default-html which contains:
 

```

<title>Hotlist</title>
<h1>Hotlist Page</h1>
<a href="http://www.yahoo.com/">Yahoo!</a><br>

```
- We then chose to set a user preference, and we changed the Font Size from very small to small; this created a file called drive:\users\umberto\nsb\.\nsb-prefs with the following entries:
  - IBM;NSB User\_Text\_Size=1
  - IBM;NSB Main\_Font\_Name=New Century
  - IBM;NSB Header\_Font\_Name=New Century
  - IBM;NSB Monospace\_Font\_Name=Courier
  - IBM;NSB Window\_Color\_Text=#000000000000
  - IBM;NSB Window\_BgColor=#bfbfbfbfbfbf



- IBM;NSB<sup>c</sup> Anchor\_Color=#00000000b0b0
  - IBM;NSB<sup>c</sup> Anchor\_Color\_Been\_There=#272705055b5b
  - IBM;NSB<sup>c</sup> Ignore\_Document\_Attributes=
  - IBM;NSB<sup>c</sup> Print\_Text\_Size=
  - IBM;NSB<sup>c</sup> Paper\_Size=0
  - IBM;NSB<sup>c</sup> Top\_Margin=.500
  - IBM;NSB<sup>c</sup> Left\_Margin=.500
  - IBM;NSB<sup>c</sup> Bottom\_Margin=.500
  - IBM;NSB<sup>c</sup> Right\_Margin=.500
  - IBM;NSB<sup>c</sup> Left\_Header=&w
  - IBM;NSB<sup>c</sup> Right\_Header=Page &p
  - IBM;NSB<sup>c</sup> Left\_Footer=&D
  - IBM;NSB<sup>c</sup> Right\_Footer=&t
  - IBM;NSB<sup>c</sup> Dcache\_Verify\_Policy=1
  - IBM;NSB<sup>c</sup> Home\_URL=http://WTR05140.itso.ral.ibm.com/nstation/mods/NSB/MRI2924/homepage.htm
  - IBM;NSB<sup>c</sup> Download\_Directory=
  - IBM;NSB<sup>c</sup> Accept\_Language\_Header=en
  - IBM;NSB<sup>c</sup> Show\_Tool\_Bar=TRUE
  - IBM;NSB<sup>c</sup> Auto\_Load\_Images=TRUE
  - IBM;NSB<sup>c</sup> jscript\_active=TRUE
  - IBM;NSB<sup>c</sup> applet\_active=TRUE
- Another file which is created automatically is drive:\users\umberto\nsb\nsb-global-history-html which contains a list of all the URLs which were accessed, for example:
 

```
<title>Global History</title>
<h1>Global History Page</h1>
<a href="http://WTR05140.itso.ral.ibm.com/nstation/mods/NSB/MRI2924/homepage.htm" name="10192">IBM Network Station Browser Help</a><p>
<a href="http://www.yahoo.com/" name="4565">Yahoo!</a><p>
```

---

## 10.6 Configuring the Navio NC Navigator in NSM

Select **Navio NC Navigator** in the setup task in the Network Station Manager, select **System Defaults**, and click on **Next** to display the figure below:

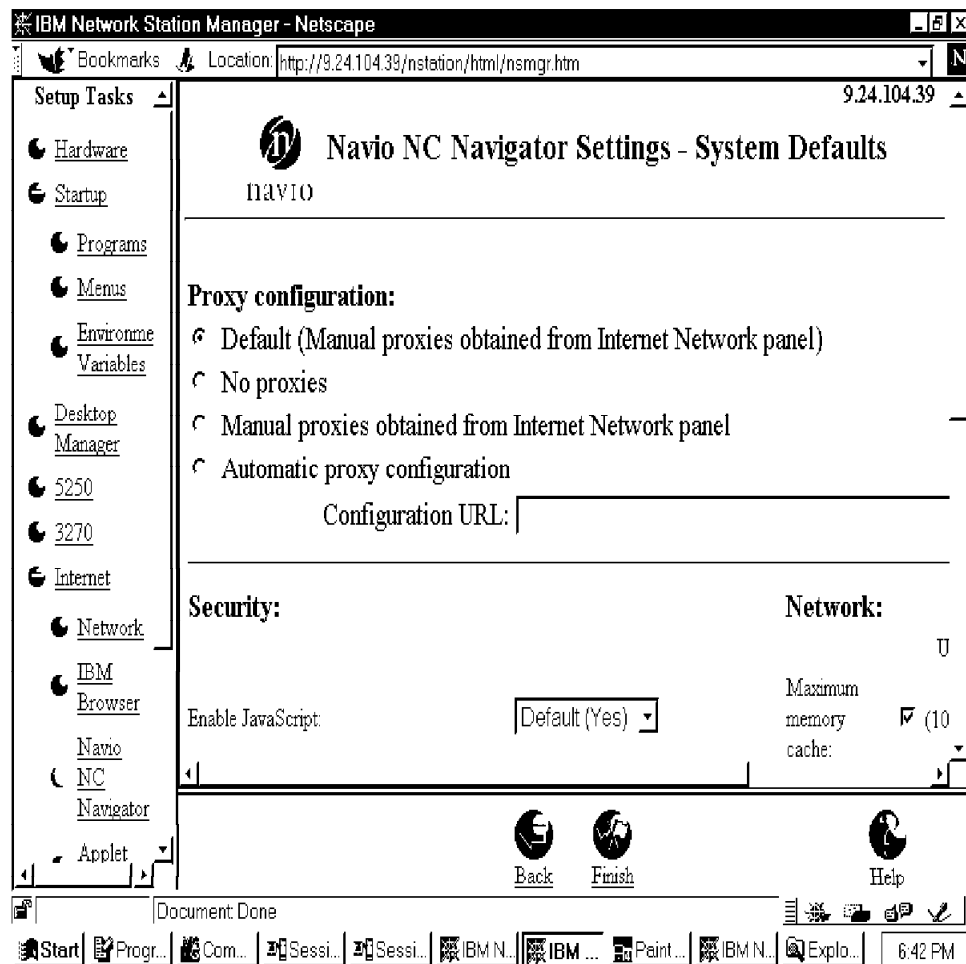


Figure 79. The IBM Network Station Manager - Navio Customization

The following parameters can be updated from this window.

- Proxy Configuration:
  - Default (Manual proxy obtained from the Internet Network panel).  
The Default proxy configuration function indicates that the proxy settings specified in the Network function of the Internet Setup Task will be used. At the system level (all of your IBM Network Station users), this is the same as specifying Manual proxies.
  - No proxy.  
The No proxies configuration function means that no proxies will be used for the Navio NC Navigator users. If you have a firewall in place, users will not be able to connect to any URLs outside of your network's firewall.
  - Manual proxy obtained from the Internet Network panel.
  - Automatic proxy configuration.
- Security:
  - Enable JavaScript.
  - Enable Java Applet.
  - Enable SSL 2.

The Enable SSL (Secure Sockets Layer) 2 and 3 functions allow Navio NC Navigator users to connect to servers utilizing SSL. SSL is an encryption function that works with applications and servers utilizing HTTPS-type URLs. The default for SSL 2 and SSL 3 is Yes.

- Enable SSL 3.
- Network:
  - Specifying maximum memory cache size.

The maximum memory cache function specifies the largest size, in kilobytes, of the memory in the IBM Network Station system unit available for caching Web pages and images. The default is 1024 KB. A smaller cache size reduces the performance of the browser. However, a smaller cache size will make more memory available for running other applications.
  - Specifying maximum TCP/IP connections.
  - Network buffer size.
- Navigator Directory button definition:
  - Name

Specifies the name of the Navio NC Navigator directory button. This text string appears inside the specified directory button. There are up to six Navio NC Navigator directory button input fields available. If used, these buttons are displayed near the top of the browser page (directly below the Location input field for URLs).
  - URL

Specifies the URL address that this directory button will link to when clicked.
  - Fly-over help.

Specifies the text that is displayed when the mouse pointer hovers over a Navio NC Navigator directory button.

Click on **Finish** to complete the Navio NC Navigator Setting.

### 10.6.1 Files Created by NSM for Navio NC Navigator Settings

- We configured, in the Navio NC Navigator Setting - System Default page, the following entry:

Maximum TCP/IP Connections	3
----------------------------	---

The file named drive:\nstation\userdata\sysdef\nav\pref was updated by the NSM with the entry

```
Navio.maxConnections: 3
```
- Then we configured, for user sarah,

Maximum memory cache:	2000 KB
-----------------------	---------

and this action created in the file named drive:\nstation\userdata\sarah\nav\pref the following entry:

```
Navio.memCacheSize: 2000
```

## 10.7 Using the NAVIO NC Navigator

Similar to the IBM Network Station browser, the Navio browser can either be autostarted after a user logon or it can be started by the user when required.

The figure below shows the main panel of the Navio browser.

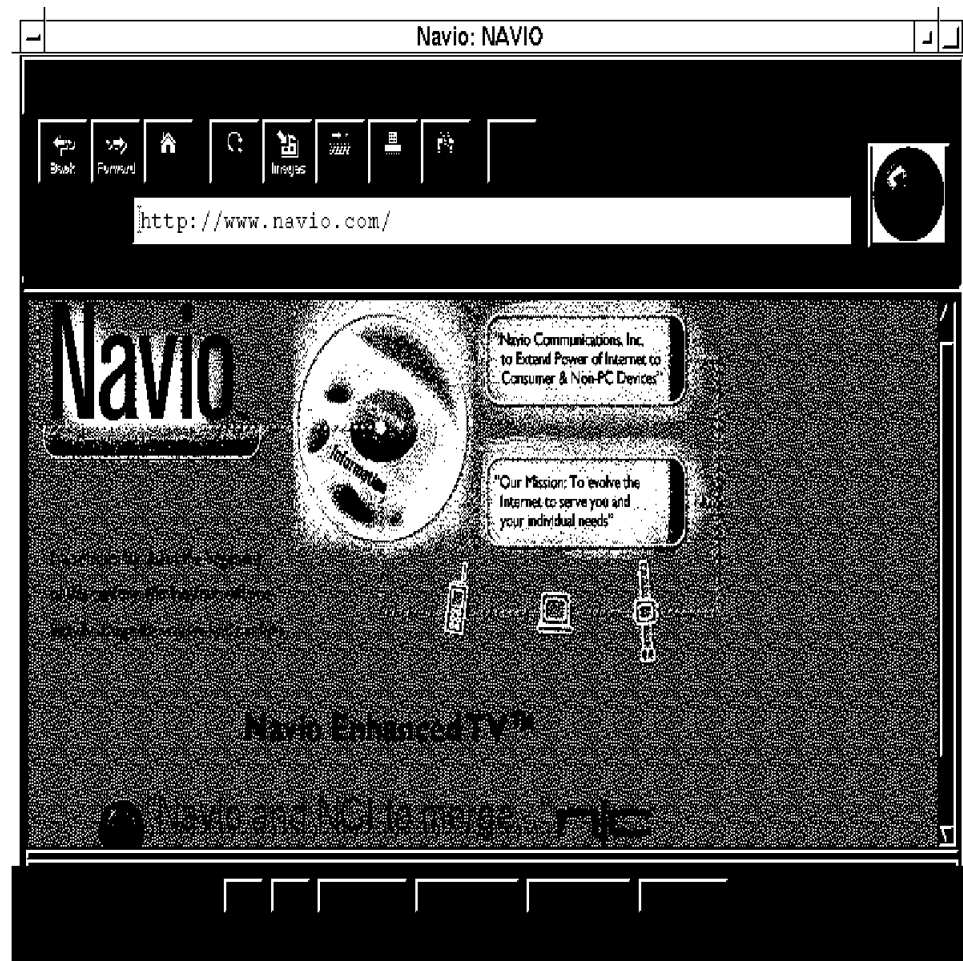


Figure 80. The Navio NC Navigator Home Page

### 10.7.1 Setting User Preferences

From the **Options** pull-down menu you can choose:

- General Preferences.

There are panels for Appearance, Fonts and Images

- Appearance Panel

From this panel the user can set how the toolbar is shown, what the browser tries to search when started, and link styles.

- The Fonts Panel

From this panel the user can change the size and type of fonts and for the encoding.

- The Images Panel

This panel has information about how colors are applied to images and if the images are displayed while or after loading.

- Mail and News Preferences.

There are panel for Compose, Server Identify.

- Network Preferences.

This panel is illustrated below. There are tabs for Cache, Connections, Proxies, Protocols and Languages.

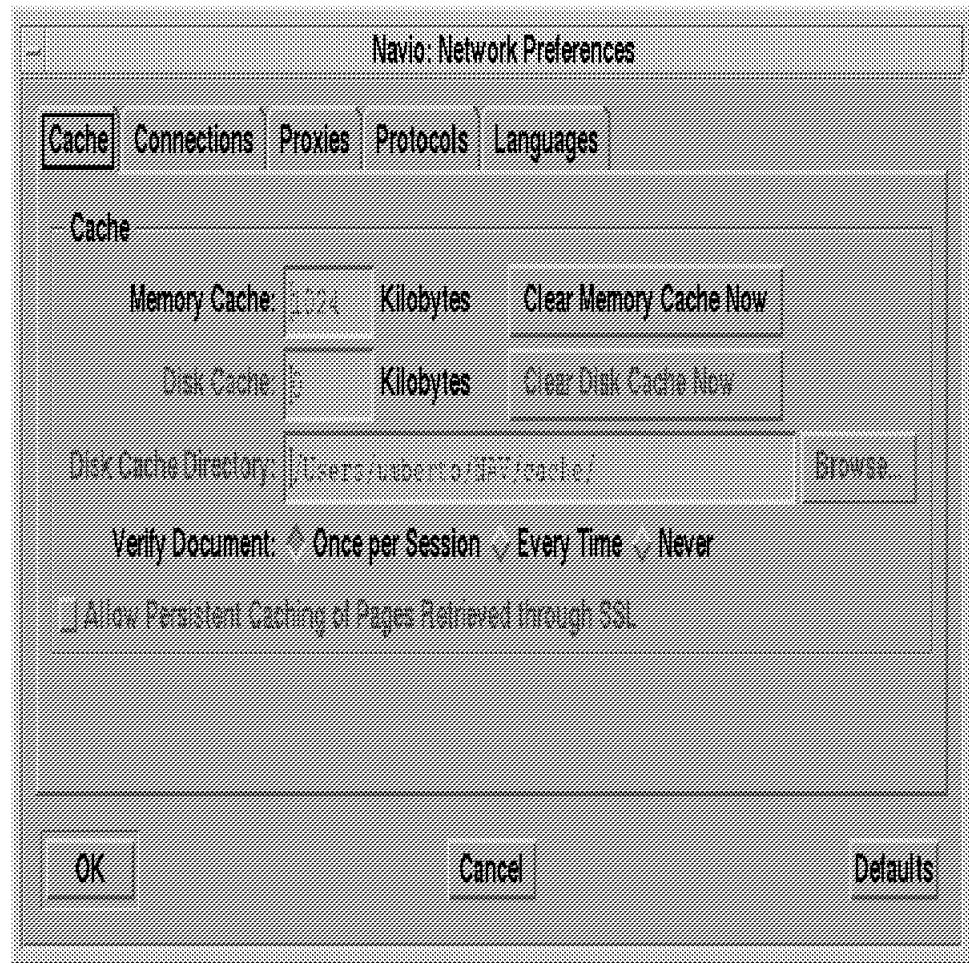


Figure 81. The Navio NC Navigator Network Preferences

Note that you can, using the Proxies tab, look at the setting of the proxies but they cannot be set from this panel. These are set using the Network Station Manager panels.

- Security Preferences.

There are panels for General, Password, Personal Certificates and Site Certificates.

## 10.7.2 Bookmarks

The bookmarks are where you save the titles and URLs of your favorite Web sites. To add the current file to the bookmarks, click on **Bookmarks**, and choose **Add Bookmarks**.

When we added the URL [www.altavista.com](http://www.altavista.com) to our bookmarks, this updated the file named `drive:\users\umberto\nav\bookmarks.html` which then contained the following entries:

```
<!DOCTYPE NAVIO-Bookmark-file-1>
<!-- This is an automatically generated file.
It will be read and overwritten.
Do Not Edit! -->
<TITLE>Umberto's Bookmarks</TITLE>
<H1>Umberto's Bookmarks</H1>

<DL><p>
  <DT><A HREF="http://www.altavista.com/"
ADD_DATE="872594156" LAST_VISIT="872593478"
LAST_MODIFIED="872593478">AltaVista Technology, Inc.</A>
</DL><p>
```

## 10.7.3 Saving Files

To save the current document:

1. Click on **File**, and choose **Save Frame as**.
2. Specify the name and location of the saved file.
3. Set the file type format to Plain Text, Source if you want to include the HTML tags or PostScript.
4. Choose the **OK** button.

To save an inline image:

1. Click the image with the right mouse button.
2. From the pop-up menu, choose **Save this image as**.
3. In the Save as pop-up, specify the path and file name.
4. Choose the **OK** button.

When we saved the home page from the Altavista site as `altavista.htm`, the file `drive:\users\umberto\nav\altavista.htm` was created on the server.

## 10.7.4 Starting Multiple Navio NC Navigator Windows

To start multiple Navio NC Navigator windows within the browser, select **File** and then select **New Web Browser**.

The number of multiple browsers are limited by the

Max TCP/IP connections

which was configured in the Network Station Manager panels.

## 10.7.5 Files Created from Navio NC Navigator User Settings

We have done some settings using the Navio NC Navigator to observe the files that get created on the server as a result of these actions.

- When we logged on to the Network Station as user umberto, a file called drive:\users\umberto\ is created.

- After starting the Navio browser, the following files are created:

```
drive:\users\umberto\nav\bookmarks.html
drive:\users\umberto\nav\cert5.db
drive:\users\umberto\nav\cookies
drive:\users\umberto\nav\history.db
drive:\users\umberto\nav\key.db
drive:\users\umberto\nav\lock
drive:\users\umberto\nav\preferences
```

You can only browse the preferences and lock files; the other files are not readable.

- Our file drive:\users\umberto\nav\preferences contains:

```
# Navio Preferences File
# Version: 3.01
# This is a generated file! Do not edit.

SHOW_TOOLBAR: True
SHOW_URL: True
SHOW_DIRECTORY_BUTTONS: True
SHOW_MENUBAR: True
SHOW_BOTTOM_STATUS_BAR: True
AUTOLOAD_IMAGES: True
FTP_FILE_INFO: True
SHOW_SECURITY_BAR: True
MEMORY_CACHE_SIZE: 1024
DISK_CACHE_SIZE: 0
CACHE_DIR: /Users/umberto/NAV/cache/
VERIFY_DOCUMENTS: 0
CACHE_SSL_PAGES: False
8BIT_MAIL_AND_NEWS: True
SEND_FORMATTED_TEXT: True
QUEUE_FOR_LATER: False
MAIL_BCC_SELF: False
MAIL_BCC:
MAIL_FCC: /Users/umberto/nsmail/Sent
TMPDIR: /tmp
BOOKMARKS_FILE: /Users/umberto/NAV/bookmarks.html
HISTORY_FILE: /Users/umberto/NAV/history.db
DOC_CSID: 2
FONT_CHARSET: iso-8859-1
FONT_SPEC: misc-nil-20-noscale-fixed-x-user-defined
FONT_SPEC: misc-nil-20-noscale-prop-x-user-defined
FONT_SPEC: misc-fixed-130-noscale-fixed-jis_x0201
FONT_SPEC: misc-fixed-130-noscale-prop-jis_x0201
FONT_SPEC: jis-fixed-230-noscale-fixed-jis_x0208-1983
FONT_SPEC: jis-fixed-230-noscale-prop-jis_x0208-1983
FONT_SPEC: adobe-courier-100-noscale-fixed-iso-8859-1
FONT_SPEC: adobe-new century schoolbook-100-noscale-prop-iso-8859-1
```

```

CITATION_FONT: 2
CITATION_SIZE: 0
CITATION_COLOR:
REAL_NAME: Umberto
EMAIL_ADDRESS: umberto
ORGANIZATION:
SIGNATURE_FILE: /Users/umberto/.signature
SIGNATURE_DATE: 0
DITHER_IMAGES: Auto
STREAMING_IMAGES: True
MAILHOST: localhost
MAIL_DIR: /Users/umberto/nsmail/
MAX_CONNECTIONS: 3
SOCKET_BUFFER_SIZE: 32
ACCEPT_COOKIE: 0
ASK_PASSWORD: 1
PASSWORD_TIMEOUT: 30
WARN_ENTER_SECURE: True
WARN_LEAVE_SECURE: True
WARN_MIXED_SECURE: True
WARN_SUBMIT_INSECURE: True
DISABLE_JAVA: True
DISABLE_JAVASCRIPT: False
DEFAULT_USER_CERT: do the default
ENABLE_SSL2: True
ENABLE_SSL3: True
CIPHER:
LICENSE_ACCEPTED: 0 3.01
TOOLBAR_ICONS: True
TOOLBAR_TEXT: True.0
TOOLBAR_TIPS: True
HOME_DOCUMENT: http://www.navio.com/
UNDERLINE_LINKS: True
HISTORY_EXPIRATION: 9
ADD_URLS:
BOOKMARK_MENU:
PRINT_COMMAND:
PRINT_REVERSED: False
PRINT_COLOR: True
PRINT_LANDSCAPE: False
PRINT_PAPER: 0

```

- And our file drive:\users\umberto\nav\lock contains:

```
00.00.a7.16.f6.28-9.24.104.236-59
```

This is our IBM Network Station's MAC and IP address. If the same user logs on to another IBM Network Station while already logged on to one Network Station (you can be concurrently logged on several IBM Network Stations), and he starts the Navio NC Navigator, he gets a warning message that this user is already running Navio from another IBM Network Station. He can continue to use the browser but without the ability to use the disk cache, global history and his personal certificates.

Note that this lock file is erased when the user terminates the browser in a *normal* way. If the user terminates the browser abnormally, (say by powering down the Network Station without first ending the browser) this lock file is not be erased and prevents the same user from storing preferences with this browser from any other physical Network Station; that is because this user is still considered active on another workstation.



- Then we changed the Font size from 10.0 to 8.0 by a click on **Options**, then **General Preferences**.

The file named drive:\users\umberto\nav\preferences then contains:

FONT\_SPEC: adobe-new century schoolbook-80-noscale-prop-iso-8859-1



---

## Chapter 11. IBM Network Station and Windows NT Security

In this chapter, we discuss a few Network Station security aspects as well as some Windows NT server-related security issues. This chapter is divided into two main sections:

- Network Station-specific security concerns regarding setup parameters, file service and access control to the Network Station.
- Windows NT-related security, including directory and file access.

---

### 11.1 Network Station Security

This section explains how to:

- Incorporate security into the Network Station setup utility panels
- Work with the Network Station's local file system
- Specify access control parameters

#### 11.1.1 Setup Utility Panels

The Network Station Setup Utility panels allow an administrator or user to update some of the configuration parameters residing in the NVRAM of the Network Station.

One way to access the setup utility panels is to press the Esc (escape) key when the Network Station is powering on. When you see the message:

NS0500 Search for Host System

press the Esc key to interrupt the boot sequence and provide you access to the setup utility configuration panels.

To prevent unauthorized users from modifying the parameter settings found in the utility menus, an administrator password can be enabled. When a password is set, the process of interrupting the boot sequence does not take the user directly into the setup menus, but rather, prompts for the administrator password.

To enable an administrator password using the Network Station Manager, start the NSM, log on as Administrator, select **Hardware, System Defaults**, click on **Next**, find the field under Miscellaneous Settings titled Administrator password and enter the password you wish to use, then select **Finish**. This updates the /nstation/configs/defaults.nsm file by adding the following statement:

```
set unit-global-password="<ENCODED>%7A%66%8A%F2%EA%88%49%C5"
```

The following figure shows where to set the Administrator password within the Network Station Manager.

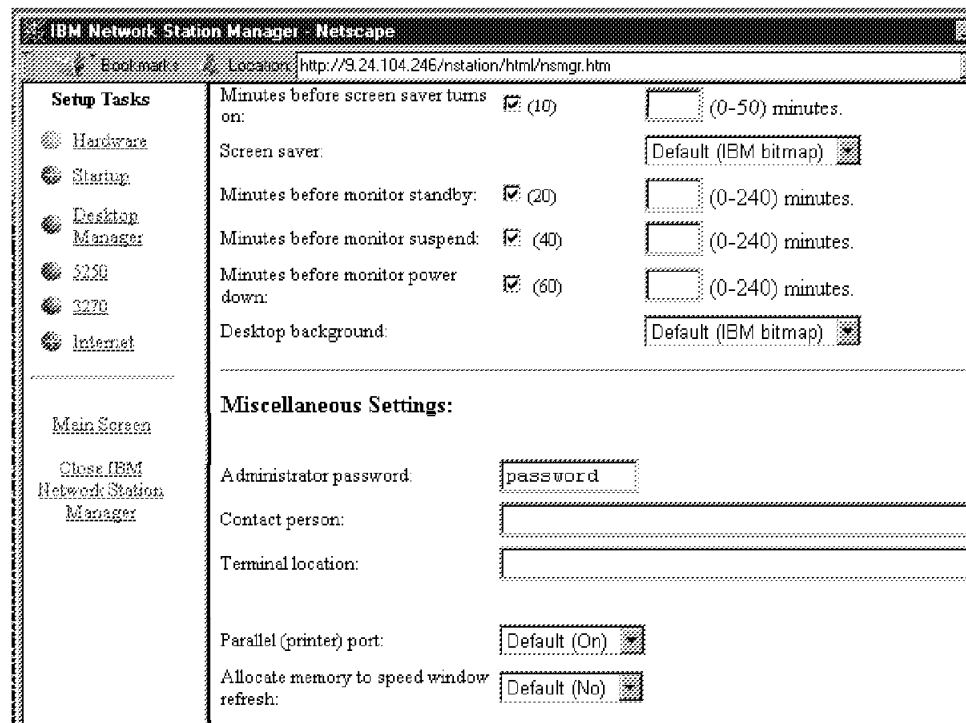


Figure 82. Using the NSM to Set the Network Station Admin Password

**Note:** If you set or change the administrator password for a specific Network Station using the NSM, that Network Station needs to go through the boot process once completely before the password is enabled on that particular system. This is required so that the Network Station reads and processes its configuration files.

After protecting the Network Station with an administrator password, a password panel is presented to the user when the Esc key is pressed during the boot process. This password is case sensitive.

If the user does not know the password, pressing the F12 key allows access to the information display panels, which are available to general users; with these panels, the user can view but not change the information.

The user is allowed three attempts to enter the correct password, after which he is assigned general user authority, which only allows him to view the setup parameters.

Another method to access the Setup Utility panels is to use the key sequence of Left Alt + Caps Lock + Pause after the Network Station has completed booting. This takes the user into the boot monitor program. From the boot monitor program, press the F1 key to enter into the Setup Utility panels. If the administrator password is enabled, the user is prompted for the password.

#### Tip

Note that this method is much faster than powering off and powering on, waiting for the power on self tests to complete and pressing the Esc key.

From the Setup Utility, it is possible to enter the boot monitor program. The boot monitor program is a facility from which you can set or test some Network Station hardware-specific values. To access the boot monitor program from the Setup Utility, use the Left Alt + Left Ctrl + Left Shift + F1 key sequence (this is for 101/102 keyboards). Note that if the administrator password is enabled, normal users will not be able to enter the boot monitor program from the Setup Utility panel.

The following table summarizes special key sequences for entering the Setup Utility Panels and the Boot Monitor Program.

<i>Table 6. Key Sequences to Access the Setup Utility and Boot Monitor Program</i>			
<b>Key Combination</b>	<b>Context</b>	<b>Action</b>	<b>Special Note</b>
Esc	Boot time	Stops downloading kernel and invokes Network Station Utility Main Menu	
Left Alt + Left Ctrl + Left Shift + F1	Network Station Setup Utility	Enter the boot monitor program	Only 101/102 keyboards
Left Alt + Left Shift + F1	Network Station Setup Utility	Enters the boot monitor program	Only 5250/3270 keyboards
F1	Boot monitor program	Switch to Network Station Setup Utility Panels	
Left Alt + Caps Lock + Pause	Window manager	Use keys in this sequence. Enters boot monitor program	All applications terminated and there is no chance to switch back to the Window Manager.

### 11.1.2 File Service - Local File System

The Network Station needs a file system structure from which to serve requests for access to data from local applications. This is called the local file system and is made up of mounts of other hosts' directories. This is required because the Network Station does not have its own hard disk or diskette drive.

During the Network Station initialization, the \nstation directory on the boot server is mounted using the TFTP protocol to the local file system. From this mount, the Network Station can access font directories, keyboard definition directories and loadable module directories.

Following user login, several other directories are mounted using the NFS protocol. These directories are specified in an NFS exports file, which is configured during the installation of IBM TCP/IP Services for Windows NT Server 4.0. The exports file is located on the server in /ibmtcpip/etc.

After the installation process, the exports file, by default, should contain the following entries:

```
x:\nstation alias=/netstation/ -ro
x:\nstation\userdata alias=/netstation/userdata/
x:\users alias=/users/
```

In some cases, you may want to run an application on the Network Station, which requires access to files stored on a remote server. Your application may therefore have variables that refer to the remote directory containing additional files. In order for the Network Station to be able to follow the path specified in the variable, a mount point must be defined to the local file system.

To add an additional mount point to the local file system, 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 filesystem 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`.

### 11.1.3 Access Control

Access control parameters allow you to specify how the 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 turned on, you then usually configure an access control table that lists the names or addresses of the hosts which are allowed access.

Access control can be enabled for the following areas or services:

- Xserver
- Config daemon
- User preference daemon
- Diagnostic daemon
- NFS
- File manager
- Local command execution daemon
- Serial and parallel daemon

Refer to the configd2.doc file located in /nstation/configs for the description of the parameters required to enable access control.

We cover here a few of the common parameters that you might wish to configure. Refer to the configd2.doc file for help in configuring parameters not discussed here.

#### 11.1.3.1 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 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 a RS/6000 AIX machine. From the 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 client 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 universal access to the Xserver, specify the following in the defaults.dft configuration file:

```
set xserver-access-control-enabled = false
```

To grant specific clients X server access, add the following to the defaults.dft file:

```

set xserver-access-control-enabled = true
set xserver-access-control-list = {
    { hostname family }
}

```

where hostname is the IP hostname or address of the x client and family is tcpip.

**Note:** This same type of access control list is used in many of the other settings where an access control list can be specified.

### 11.1.3.2 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 may choose to enable this parameter to prevent the general user from having access to the 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.

### 11.1.3.3 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. Use the following parameter to enable this function:

```
set config-enforce-passwords-locally = true
```

To do the same for user preferences, use the following:

```
set config-pref-enforce-passwords-locally = true
```

### 11.1.3.4 Diagnostic Access

A helpful problem determination source of information is the Network Station's message log. If you need to restrict access to the message log, use the following:

```
set diag-access-control-enabled = true
```

### 11.1.3.5 Remote Execution Access

You can cause the execution of commands on a 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.



---

## 11.2 Windows NT Server Security

This section focuses on how to incorporate Network Station-related security into the Windows NT Server. Because all of the configuration files reside on the server, it is important to understand how the files are protected and how the files are accessed by the Network Stations.

### 11.2.1 Directory and File Access

Because all of the Network Station and user data resides on a server, we must have a method to access this data. We must also have a method to secure the data. The Network Station utilizes two types of file access methods, TFTP and NFS.

By default, TFTP is the protocol is used to access files prior to the user login. For example, the Network Station kernel and the associated configuration files such as `standard.nsm` and all the other files called by `standard.nsm` are read using the TFTP protocol. Following the reading of the configuration files, the kernel activates the login process and the user must supply a valid user name and password.

After the user logs in, the kernel then switches to NFS as the preferred protocol used to access files. NFS is better suited to read/write operations on remote files than TFTP is. Before the user login, all file accesses are read-only, and therefore, the simpler TFTP protocol is more than adequate for these operations. However, after the user login, many file operations require write capabilities, such as storing user preferences for example, and NFS is then the preferred way.

Note however, that in many cases, the kernel may make an attempt to access one file using one protocol, and if unsuccessful, attempt access with the other protocol.

The NFS access protocol uses a UID number (user ID) for all access requests to the NFS server. This allows the NFS server to also work with the Windows NT Security and provide a stronger and more flexible security mechanism than can be provided with TFTP.

So why is TFTP used at all if NFS provides a more flexible and secure mechanism? The answer is that there are still occasions where TFTP has certain advantages over NFS; it is a simpler protocol, and its performance equals that of NFS when packet size negotiation is used (which it is in the Windows NT version), and it might lend itself better to the use of broadcast or multicast boots, which we might see in future functions.

#### 11.2.1.1 TFTP Security

The Network Station client code is loaded to the Network Station via TFTP. The TFTP server is implemented as a Windows NT service. The EPROM on the Network Station contains TFTP client code that allows the EPROM to load the operating system kernel from a boot server. After the kernel is loaded the TFTP client code is used to download the configuration information and the Network Station application code.

TFTP provides no means of authenticating. That is, TFTP has no concept of a user and if a directory is made available via TFTP, it becomes available to everyone. Furthermore, if a directory is to be accessed in read or write mode,

anyone will be allowed to read and/or write to the specified directory. This is fine for accessing read-only files and applications. However, it becomes a problem when you want to allow users to write to their own individual data directories, but prevent them from writing to other user's directories.

The TFTP configuration tab allows an administrator to specify directories that are to be available via TFTP. Here, you also specify the permissions on the directory, whether they be read, write or both. To access this configuration panel, select **Start**→**Programs**→**Network Station Manager TCP/IP**→**Configuration Utility** and the panel below is displayed:

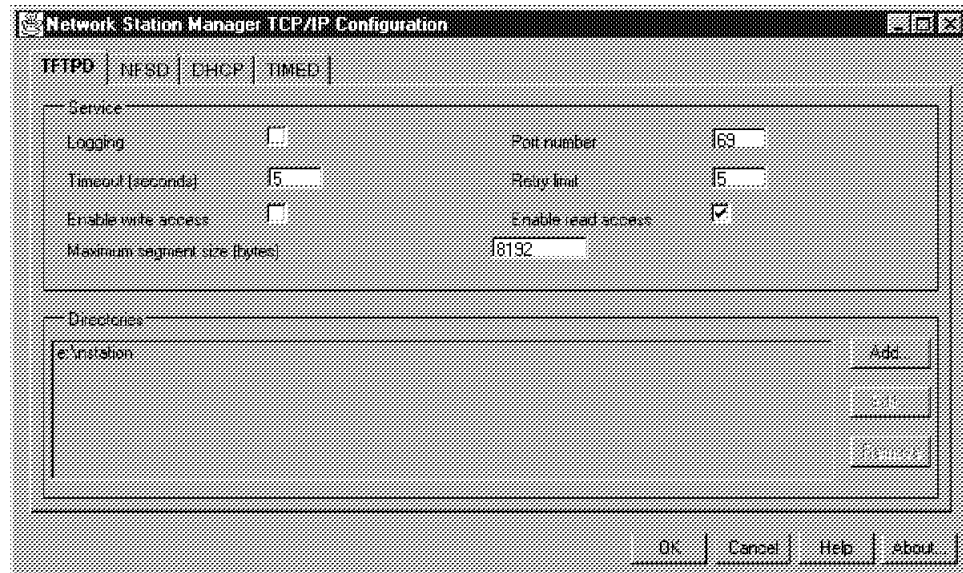


Figure 83. The TFTP Configuration Screen

In this example, the only TFTP accessible directory is e:\nstation. This must be made available via TFTP so that the Network Station can boot and initialize without authentication.

Note that only the Enable read access is selected. This permission (read, write, or both) apply to all directories specified. That is, you cannot specify one directory as read only and another as read/write; all directories are either read only or read/write.

#### 11.2.1.2 NFS Security

As stated earlier, NFS provides the concept of a user, allowing us to protect our data while still providing the access necessary for a user to have control over individual directories and/or files. The NFS Server is the NFS server that is installed on the NT server. Like the TFTP server, the NFS server is implemented as a Windows NT service.

Security and access control for the NFS server is provided in two ways:

- File system mount points
- Windows NT security user access

The Network Station kernel contains an NFS client to provide user and file specific security as well as a more enhanced filesystem. Once login occurs, NFS is used to provide authentication control as well as to provide applications with filesystem support.

If you examine the filesystem table after login, (from the Console select **Setup**→**Change Setup Parameters**→**File Service**) you will notice that the NFS exported directories are now listed. As discussed in the filesystem section, mount points are necessary for the Network Station to access data. NFS mount points (directories) are specified in the exports file located in /nstation/ibmtcpip/etc. The exports file contains the level of access to be granted (read, write, or both) to the entire directory tree that is specified. When a Network Station attempts to access an NFS server, the exports file is read to determine which directories can be exported.

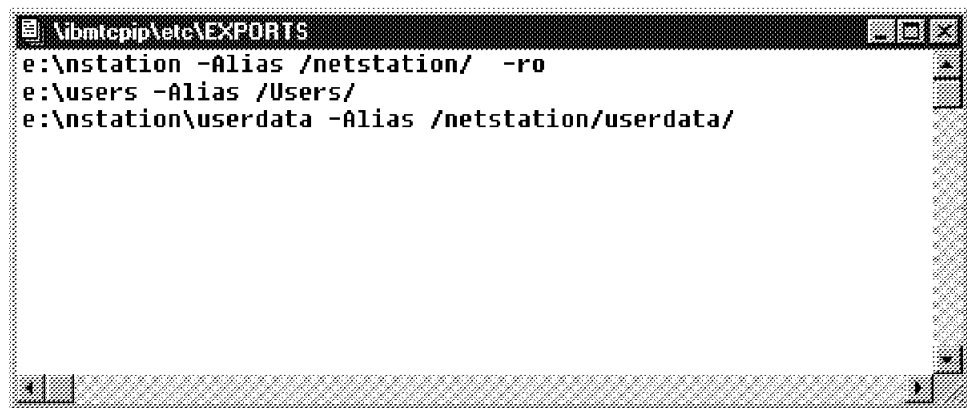


Figure 84. The /ibmtcpip/etc/exports File - NFS Exported Directories

The NFS directories are aliased for several reasons. The aliases help to isolate the Network Station from the physical NT server directory structure. For example, the Network Station does not understand backslashes, so if e:\nstation were exported without an alias the Network Station would have a hard time understanding that the backslash was not an UNIX-like special character.

Another reason for exporting e:\nstation as /netstation/ is to help clarify which directory is exported using TFTP and which is exported using NFS. To make it easier to understand which directory is an NFS connection and which directory is a TFTP connection, the alias for NFS connections is /netstation/.

Another method of enhancing security is to provide file and directory-specific control on a user or group level. This feature is provided by the Windows NT Security subsystem.

The Windows NT security subsystem does not have to be used along with the base NFS security, but it can be used to provide an additional level of security. The Windows NT security is implemented by selecting the **Use Windows NT security** box from the Network Station Manager TCP/IP Configuration NFS tab. To access the NFS configuration panel, select **Start**→**Programs**→**Network Station Manager TCP/IP**→**Configuration Utility**.

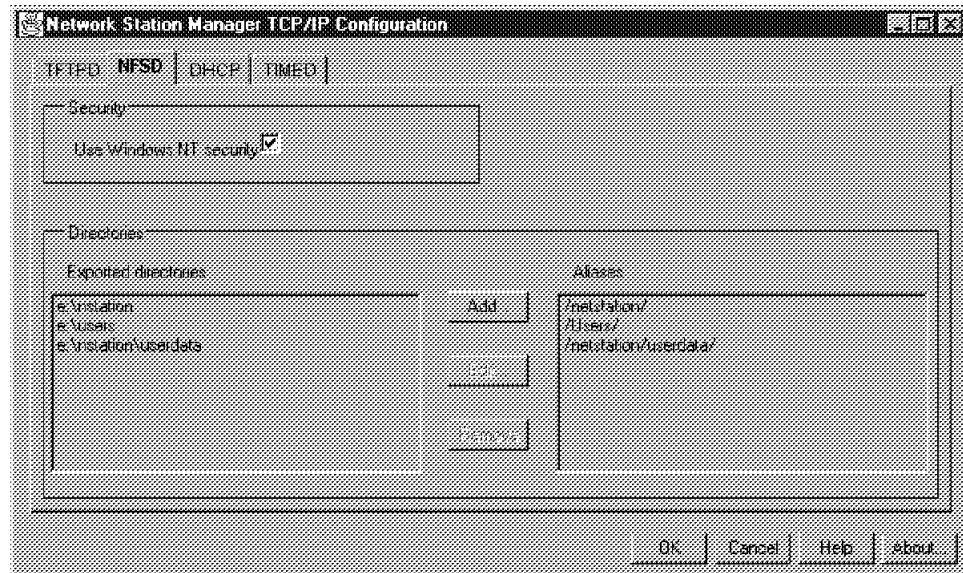


Figure 85. The NFS Configuration Screen

After enabling NT security, you may wish to define access control lists at a directory or file level. The access control list includes individual users and/or groups. These users or groups must be defined to the Windows NT server using the User Manager program. To access the User Manager for Domains program, select **Start**→**Programs**→**Administrative Tools**→**User Manager for Domains**. By default, the NSMAdmin and NSMuser groups have adequate permissions for all Network Station-related directories.

If you wish to change the access control on a file or directory perform the following:

1. Select **Start**→**Programs**→**Windows NT Explorer**
2. Highlight the directory or file you wish to work with
3. Click the right mouse button
4. Select **Properties**
5. Select the **Security** tab
6. Select **Permissions**
7. Specify the user or group name and type of access you wish to grant
8. Select **OK** to close the Permissions window
9. Select **OK** to close the Properties window

For the Windows NT security to work correctly, the NFS server maps the user ID in the NFS request with a corresponding Windows NT username. The NFS server then impersonates the user, (pretends to be this username) and logs on to the Windows NT security subsystem requesting access to all files and directories based on the Windows NT file permissions.

When using both NFS and Windows NT security, if conflicting permissions are set, the most restrictive access is the one that applies. For example, if a directory in the exports file is defined as read-write, while the same directory is defined as read-only in Windows NT, the read-only permission will dominate.

**Note:** For more information, refer to the help HTML file found at </netstation/ibmtcpip/help/ntcfghlp.htm>. The title of this help file is "IBM eNetwork Network Station Manager TCP/IP for Windows NT".

### 11.2.2 Network Station Manager Groups

The following Windows NT user groups are created when the Network Station Manager is installed:

- NSMAdmin
- NSMUser

These groups are used for directory and/or file access permission as well as by the Network Station Manager program.

The NSMAdmin group will allow rights to use the Network Station Manager program and allows any user in this group to change NSM settings for any Network Station user.

The NSMUser group allows any user in this group to log on as a Network Station user. Anyone in this group also has the ability to access the NSM at a user level and make changes to their own user environment.



---

## Chapter 12. 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
- 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

---

### 12.1 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:

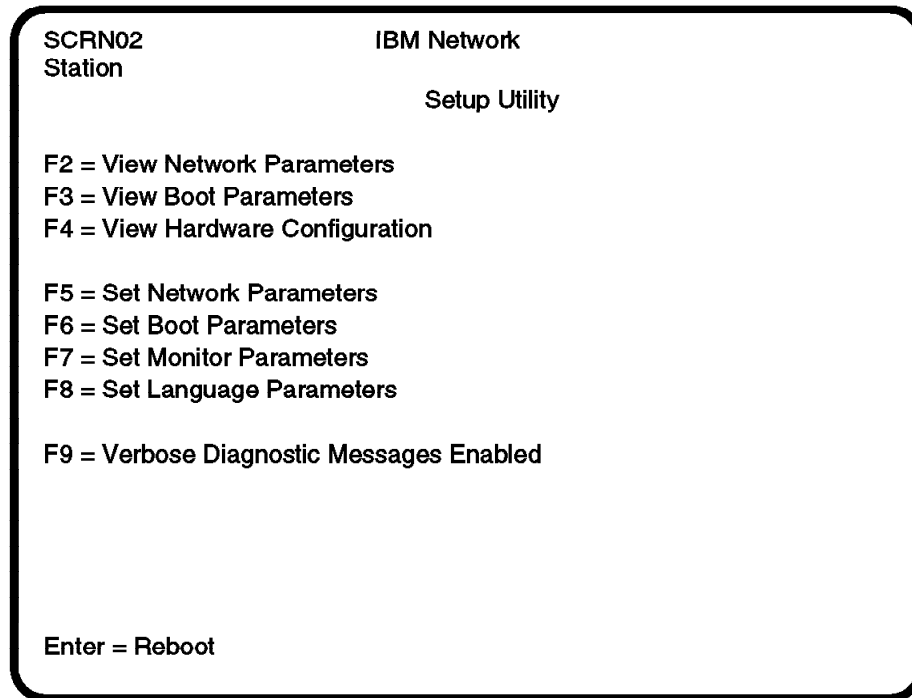
- On the IBM Network Station screen during the boot process
- Using the message log on the IBM Network Station console
- Using TELNET to port 5998 from the IBM Network Station itself
- Using TELNET to port 5998 from a remote host

We examine at each of these below.

#### 12.1.1 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 (F9) when configuring the IBM Network Station, on the main Setup Utility screen, as shown below.

## Main Setup Screen



The image shows a screenshot of the 'Main Setup Screen' for the 'IBM Network Station Setup Utility'. The screen is titled 'SCRN02 Station' in the top left and 'IBM Network Setup Utility' in the top right. Below the title, there is a list of function keys and their corresponding actions:

- F2 = View Network Parameters
- F3 = View Boot Parameters
- F4 = View Hardware Configuration
- F5 = Set Network Parameters
- F6 = Set Boot Parameters
- F7 = Set Monitor Parameters
- F8 = Set Language Parameters
- F9 = Verbose Diagnostic Messages Enabled

At the bottom of the screen, it says 'Enter = Reboot'.

cbechard-08/97

*Figure 86. IBM Network Station Setup Utility Display - 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 get displayed or not, they still get saved in the IBM Network Station memory and are available for display from the Network Station console.

### 12.1.2 Messages on the IBM Network Station Console

Shown below is the Network Station console. To display messages, the user clicks on the **Messages** checkbox situated right below the Console pull-down on the menu bar.



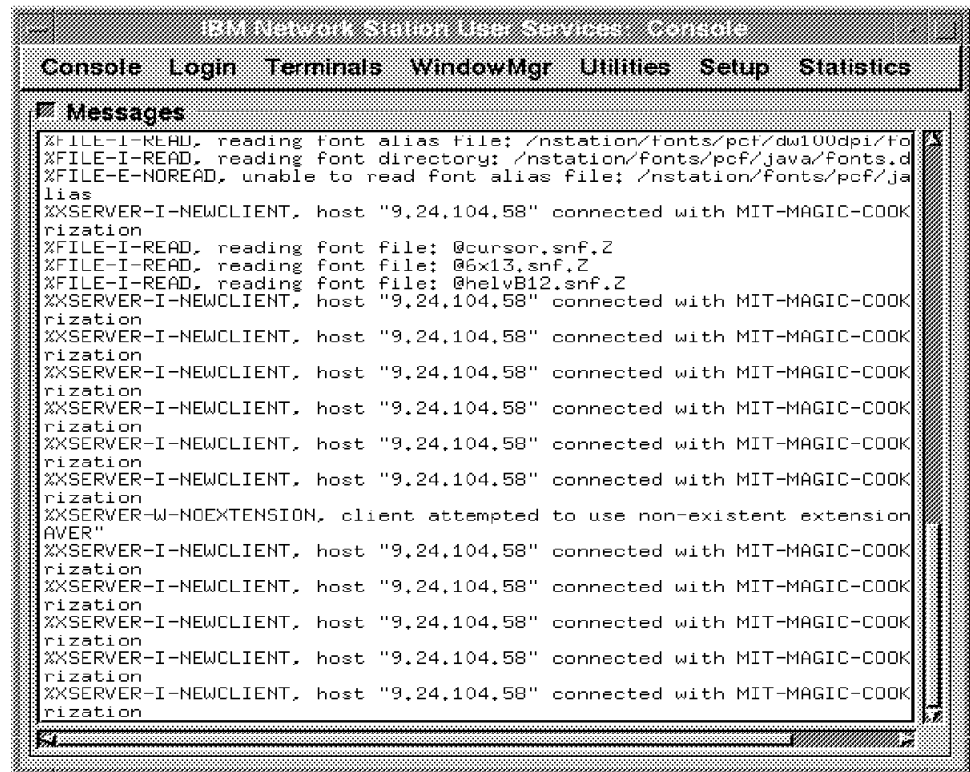


Figure 87. IBM Network Station Console Messages

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 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 at the commands are issued and executed.

### 12.1.3 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 loopback) 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 Figure 88 on page 162.

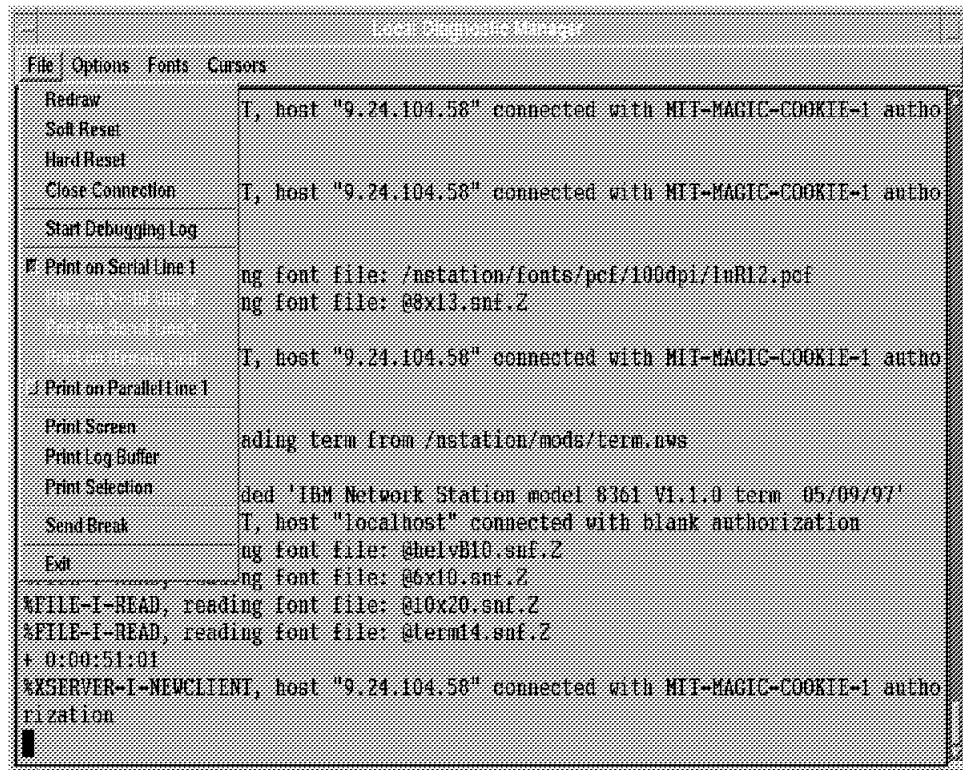


Figure 88. IBM Network Station Console Messages via Diag Port

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 also is fast, with good scrolling capabilities. The figure below illustrates the items available on the Options pull-down.

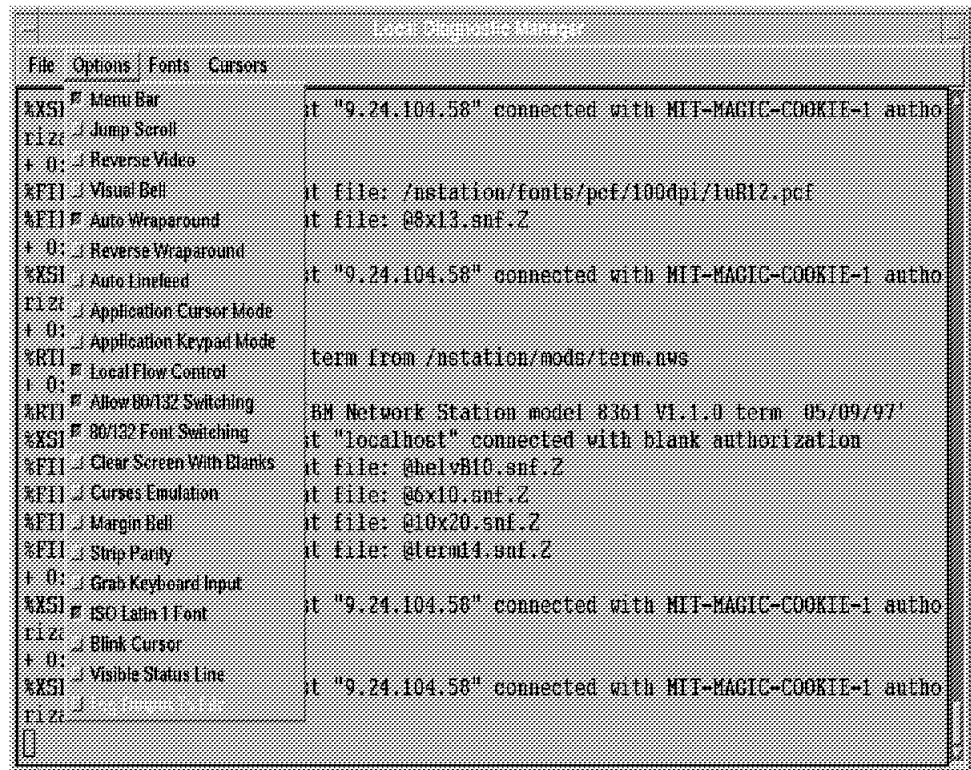


Figure 89. IBM Network Station Console - Options

#### 12.1.4 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.

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.

```

Telnet - 9.24.105.189
Connect Edit Terminal Help
%UI-I-READ      Preferences...  p file: /NStation/ProdData/SysDef/ibmwall.xbm
%UI-I-READ      Start Logging   p file: /NStation/ProdData/SysDef/ibmwall.xbm
%CONFIGD-E      Stop Logging    to read config file: /nstation/configs/hosts.nsm
%CONFIGD-I      config file: /nstation/configs/defaults.nsm
+ 0:20:44:51
%CONFIGD-I-READ, reading config file: /nstation/configs/defaults.dft
%CONFIGD-I-WROTE, wrote settings to NVRAM
+ 0:20:45:00
%CONFUI-I-STOP, setup: shutting down
+ 0:20:45:07
Special Command Check, command = rsh
rsh command for 9.24.104.58 server is AIXTERM -display 9.24.105.189:0
+ 0:20:45:08
Userinit.c: Couldn't set up rsh connection to host 9.24.104.58
+ 0:20:48:34
%NETSRV-I-ACCEPT, accepting EXECOD connection from wtr05319.itso.ral.ibm.com
%RTLD-I-LOADING, loading rsh from /nstation/mods/rsh.nws
%RTLD-E-ERROPEN, error opening module file for rsh
%RTLD-I-RETRY, module load failed, retrying from default location
%RTLD-I-LOADING, loading rsh from /rsh.nws
%RTLD-E-ERROPEN, error opening module file for rsh
%EXECOD-E-OPENMODFAIL, unable to open module rsh
+ 0:23:10:43
%NETSRV-I-ACCEPT, accepting DIAGD connection from WTR05210.itso.ral.ibm.com

```

Figure 90. IBM Network Station Console Messages via TELNET 5998

### 12.1.5 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
%KBM-I-READINGFILE, Reading file: /nstation/keyboards/AB83useng
%KBM-I-NUMERRORS, Total errors: 0
%RTLDD-I-LOADING, loading libx2 from /nstation/mods/libx2.nws
+ 0:00:00:09
%RTLDD-I-LOADED, loaded 'IBM Network Station Model 8361 V1.1.0 libx2 05/09/97'
%RTLDD-I-LOADING, loading libxt from /nstation/mods/libxt.nws
+ 0:00:00:10
%RTLDD-I-LOADED, loaded 'IBM Network Station Model 8361 V1.1.0 libxt 05/09/97'
%RTLDD-I-LOADING, loading libxm from /nstation/mods/libxm.nws
+ 0:00:00:17
%RTLDD-I-LOADED, loaded 'IBM Network Station Model 8361 V1.1.0 libxm 05/09/97'
%RTLDD-I-LOADING, loading libconf from /nstation/mods/libconf.nws
+ 0:00:00:18
%RTLDD-I-LOADED, loaded 'IBM Network Station Model 8361 V1.1.0 libconf 05/09/97'
%RTLDD-I-LOADING, loading actlogin from /nstation/mods/actlogin.nws
%RTLDD-I-LOADING, loading export from /nstation/mods/export.nws
%RTLDD-I-LOADED, loaded 'IBM Network Station Model 8361 V1.1.0 export 05/09/97'
+ 0:00:00:19
%RTLDD-I-LOADED, loaded 'IBM Network Station Model 8361 V1.1.0 actlogin 05/09/97'

%FILE-I-READ, reading font directory: @fonts.dir
%FILE-I-READ, reading font alias file: @fonts.alias
%FILE-I-READ, reading font directory: /nstation/fonts/pcf/misc/fonts.dir
%FILE-I-READ, reading font alias file: /nstation/fonts/pcf/misc/fonts.alias
%FILE-I-READ, reading font directory: /nstation/fonts/pcf/100dpi/fonts.dir
+ 0:00:00:20
%FILE-I-READ, reading font alias file: /nstation/fonts/pcf/100dpi/fonts.alias
%FILE-I-READ, reading font directory: /nstation/fonts/pcf/dw100dpi/fonts.dir
%FILE-I-READ, reading font alias file: /nstation/fonts/pcf/dw100dpi/fonts.alias
%FILE-I-READ, reading font directory: /nstation/fonts/pcf/java/fonts.dir
+ 0:00:00:21
%FILE-E-NOREAD, unable to read font alias file: /nstation/fonts/pcf/java/fonts.alias
%FILE-I-READ, reading font file: @10x20.snf.Z
%FILE-I-READ, reading font file: @cursor.snf.Z

```

Figure 91. Sample Messages in the Message Log

---

## 12.2 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 Chapter 8, "Network Station Applications and User Services" on page 91 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 using the Connect to New Unit from the File pull-down. See 12.9, "Accessing the Setup Panels from Another Network Station" on page 196 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.
- 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.

---

## 12.3 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. There are three types of event logs, which can all be examined by using NT's Event Viewer and 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 thru **Start→Programs→Administrative Tools→Event Viewer**

Below is an illustration of a typical Event Viewer display:

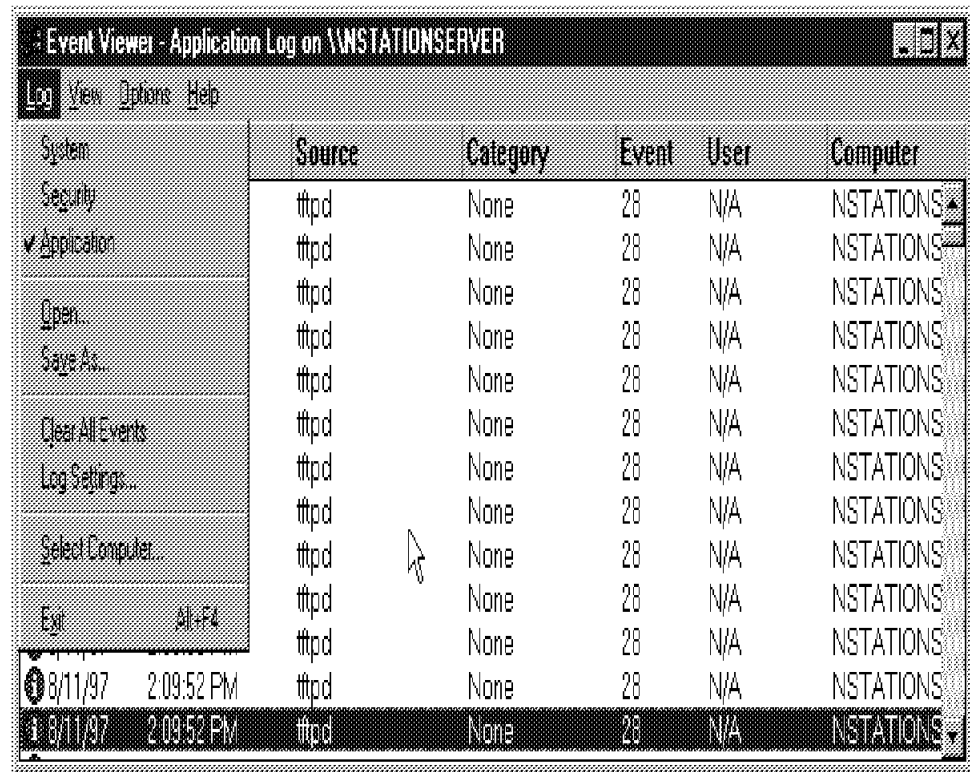


Figure 92. NT Event Viewer

When the IBM Network Station accesses the boot server to read its configuration files, all file accesses are logged to the application log. This log will therefore show the successes or failures incurred in accessing configuration files on the server.

For example, a double click on a specific event brings up additional details on the event. The one illustrated below shows the successful access to a font file.

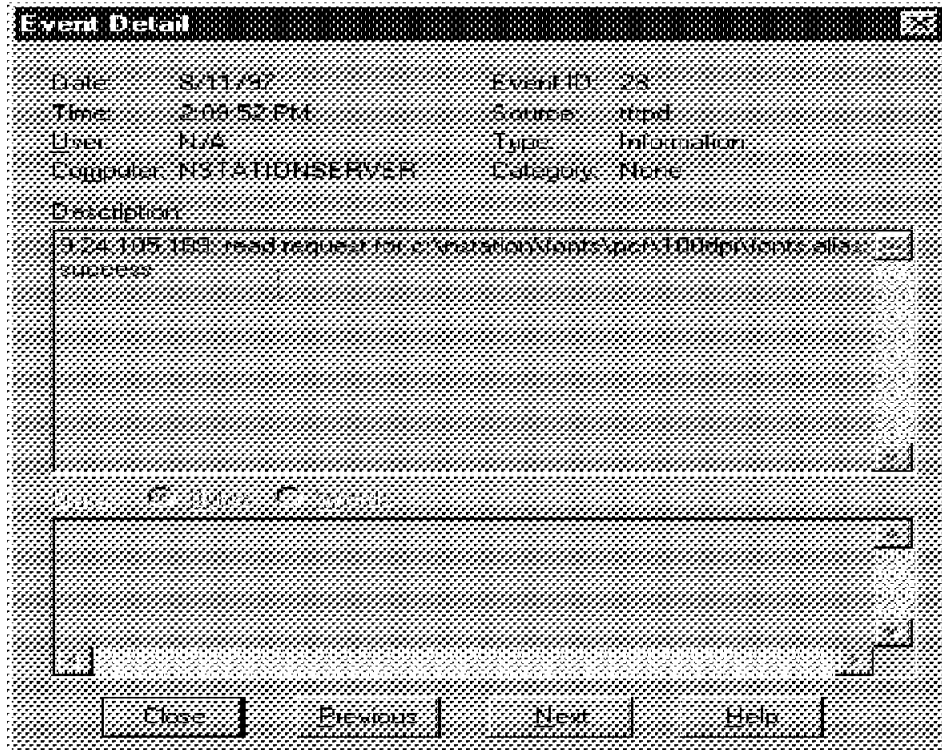


Figure 93. NT Event Viewer - Details of an Event

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 for example.

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 options pull-down, and is illustrated below:



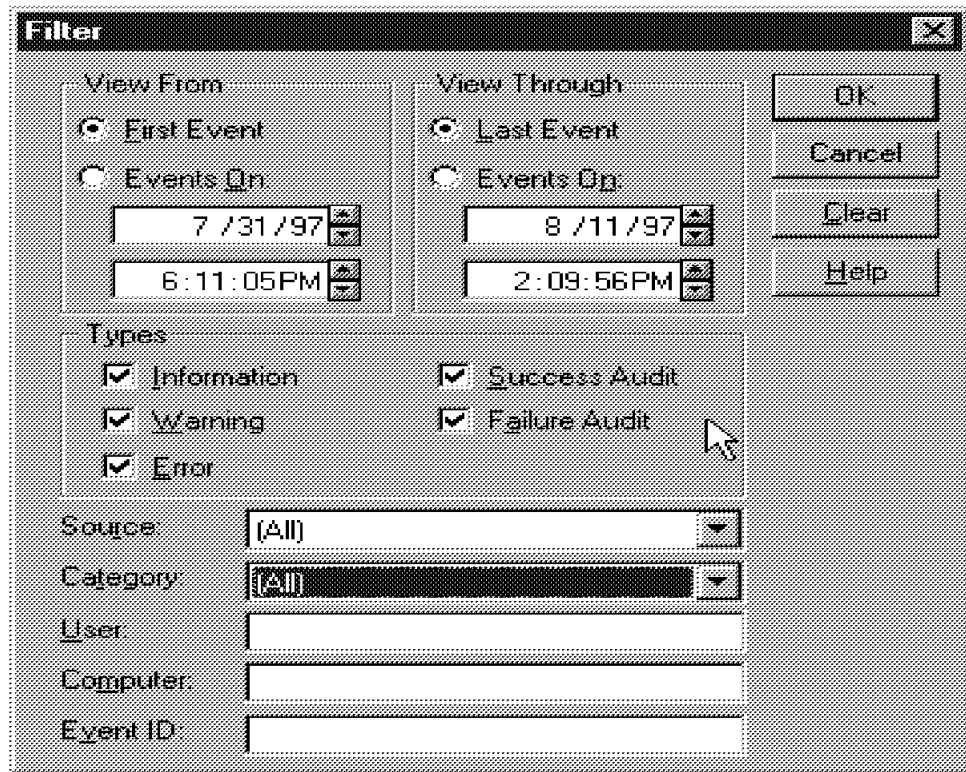


Figure 94. NT Event Viewer - Specifying a Display Filter

## 12.4 DHCP Server Log Files

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 selectable logging options are shown in the panel below.

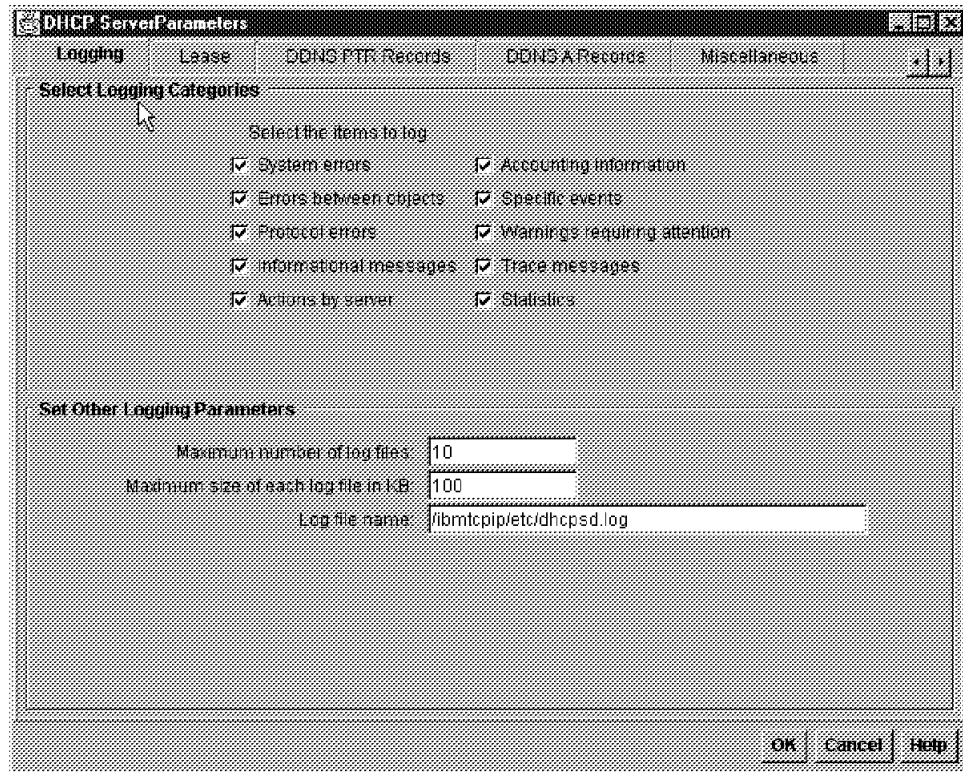


Figure 95. DHCP Logging Configuration Panel

The recommendation is to enable all selectable logging options when first implementing the DHCP server, and to reduce them once the system has been operational for a while without any problems.

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.

In order to get the DHCP server to start logging, the maximum number of log files must be set to 1 or greater. The size of each log can be set to a maximum size. What this means is that, once a log file reaches the maximum size set by the user, the log file is closed, renamed, and a new log files opened.

The log file name default is dhcpsd.log, but it can be changed by the user as shown in the panel above. If no path is specified, it will be placed in \winnt\system32.

The current log filename's extension is always .log. When it gets to its full size, the system renames the file to filename.001 and starts a new log file as filename.log. As more files are needed, up to the maximum specified, each file is renamed so that the oldest file always has the highest number for the extension (filename.004 for example).

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 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 *
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 DHCPPOFFER 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 96. DHCP Server Sample Message Log

## 12.5 Web Server Log Files

Another set of log files are the Web Server log files, showing accesses to the Web Server. This might not be a very significant log for problem determination, but it is one more source to look for clues.

To enable logging for the Web Server, click on **Start**→**Programs**→**Microsoft Internet Server**→**Internet Service Manager**

This brings up the main panel for the Web Server.

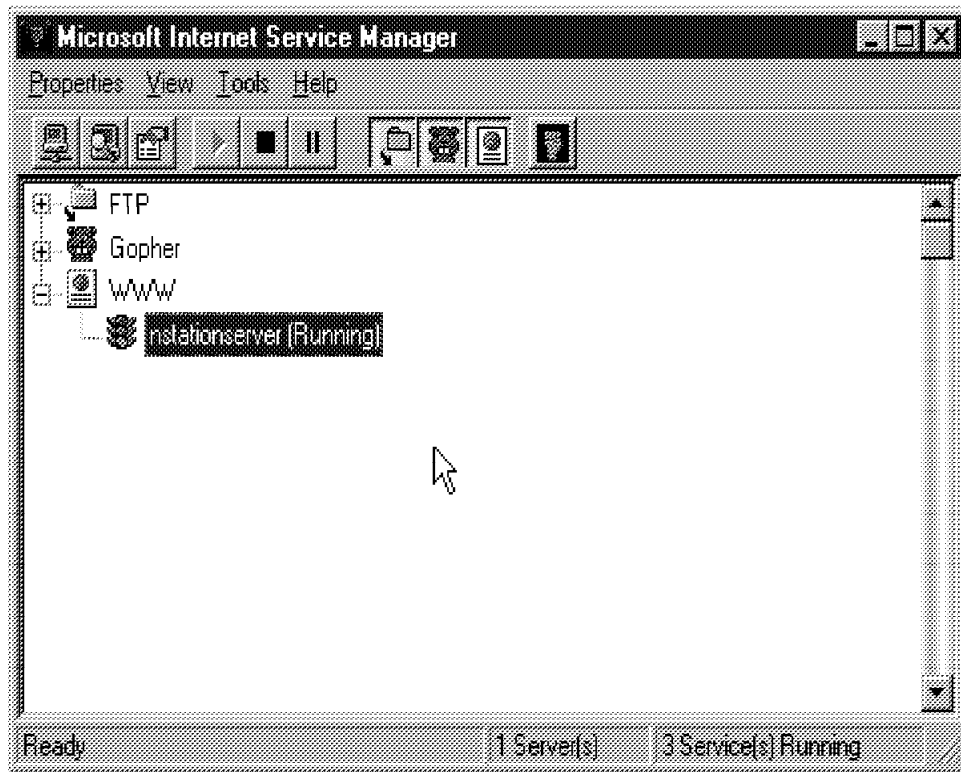


Figure 97. MS Internet Service Manager Panel

Double click the **WWW** service and select the **Logging** tab, to display the panel below:

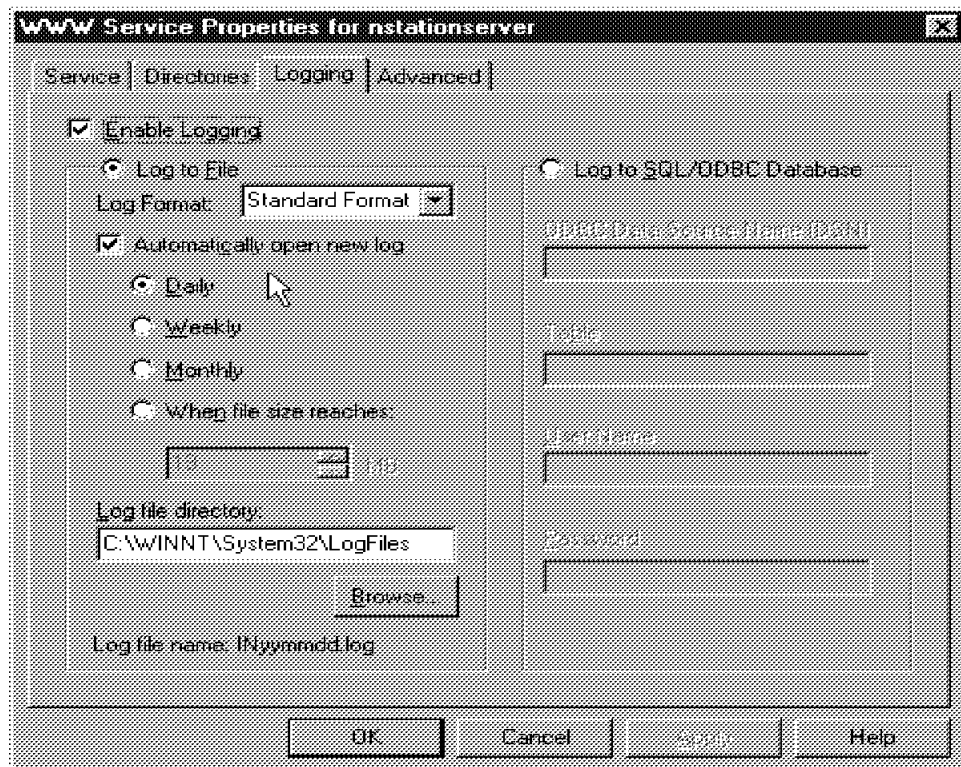


Figure 98. Web Server - Specifying Logging Options

The instructions on the panel are self-explanatory to set up logging as you require.

---

## 12.6 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.

At the moment however, 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 Allowing Promiscuous Copy Mode

Note that not all adapters can be set to promiscuous copy mode. A list of adapters that support this mode can be found at the following Web site:

<http://www.networking.ibm.com/nes/nesibase/default.htm>

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 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 <example> (My value was "Streamer1").  
  
    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  
    Data: 1
6. Choose **OK** and quit the Registry Editor.

Figure 99. Setting Adapter to Pmode

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 your own.

### 12.6.1 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.

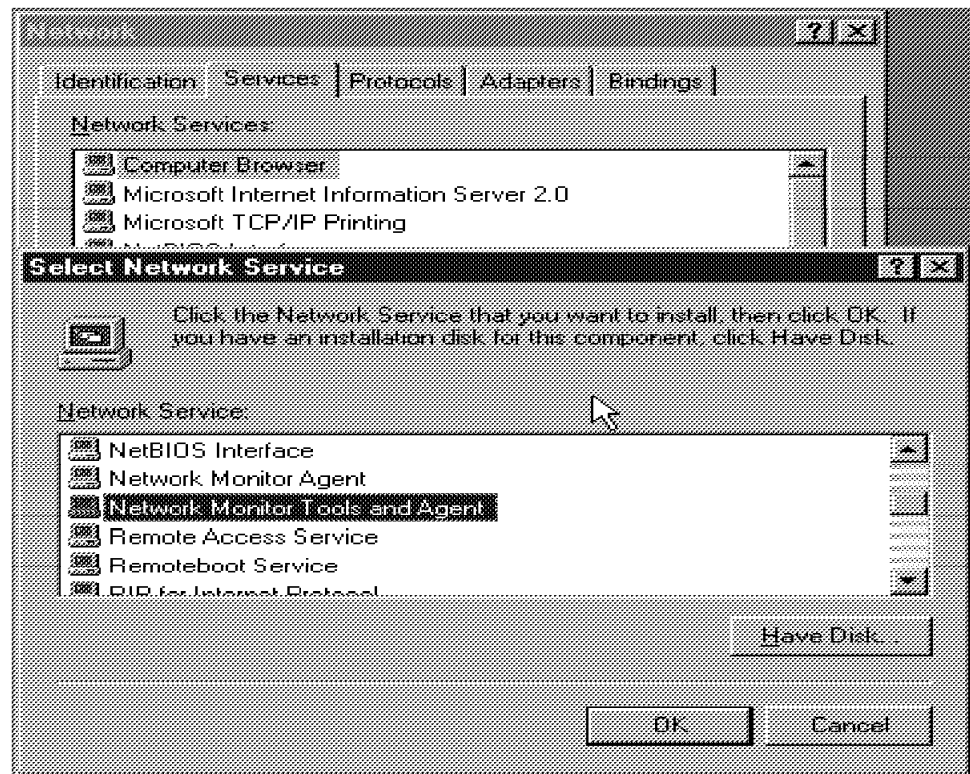


Figure 100. Network Monitor Tool Installation

## 12.6.2 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**.

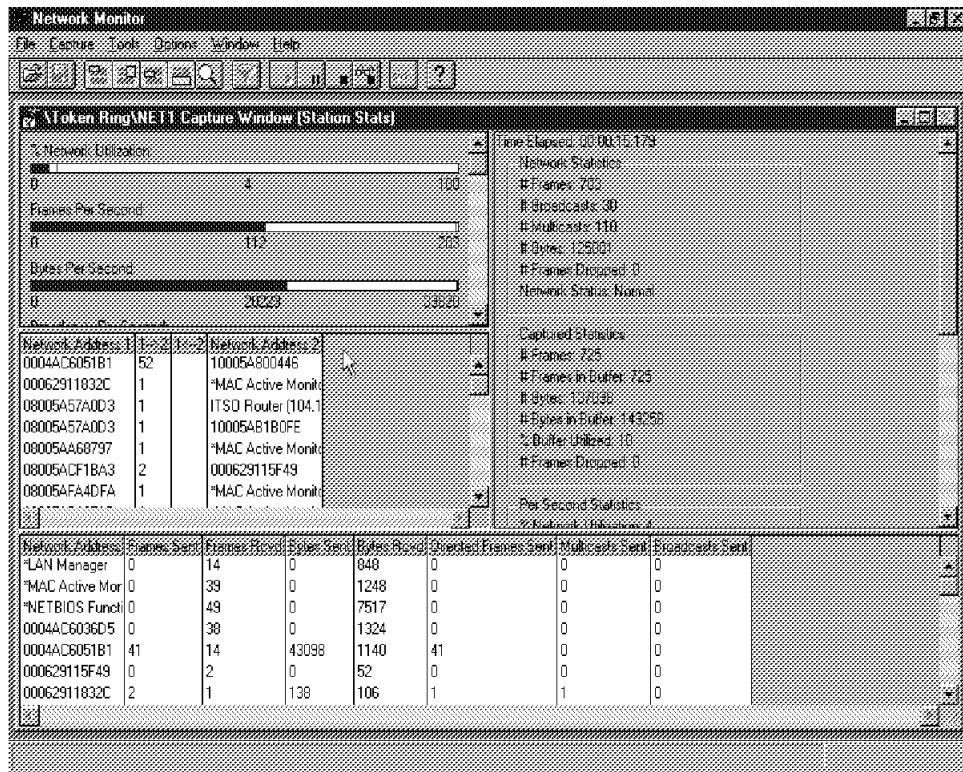


Figure 101. Network Monitor Tool - Main Panel while Capturing Data

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.

And in the bottom left hand corners 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.



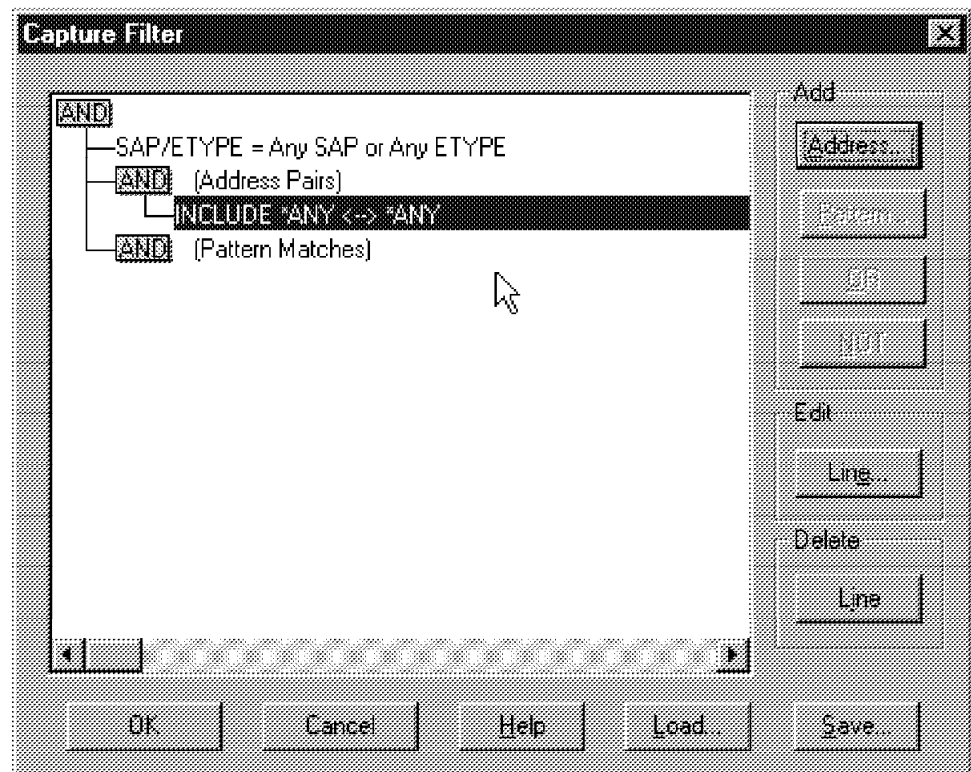


Figure 102. Network Monitor Tool - Capture Filters

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.

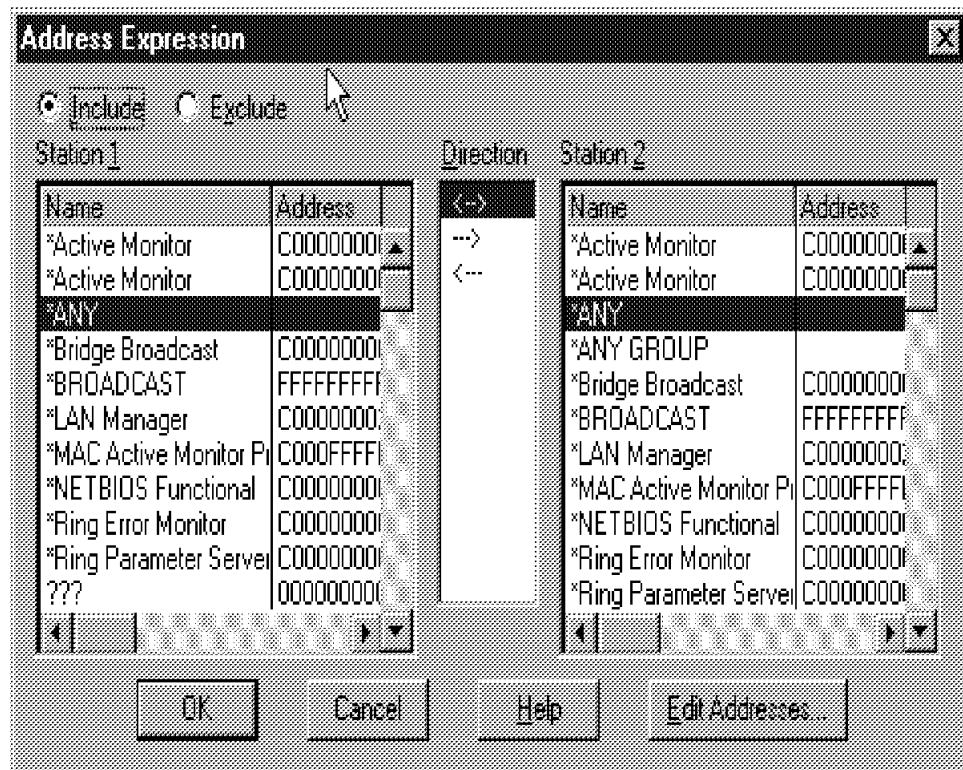


Figure 103. Network Monitor Tool - Filtering on Addresses

## 2. Displaying the captured data

Once the capture is stopped, the user can then display all the frames that have been captured. Below is a 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\W06CAPTURES\DHCPACKOK.cap [Summary]]						
Frame	Time	Src MAC Addr	Dest 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	ITSO Router	INS 1	ICMP	Echo, From 09.90.72.162 To 09.24.104.189	
28	46.493	ITSO 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	ITSO Router	ARP_RARP	ARP: Reply, Target IP: 9.24.104.1 Target Hdr Addr: 40005200501	
31	47.115	NT Boot Serve	INS 1	DHCP	Offer (xid=BA010000)	
32	47.476	ITSO 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	ITSO Router	ARP_RARP	ARP: Reply, Target IP: 9.24.104.1 Target Hdr 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 Hdr 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=0x70 SSAP=0x70 C N(R) = 0x4E POLL	
52	55.193	OPTICL005052	NT Boot Serve	LLC	RR DSAP=0x70 SSAP=0x71 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 104. 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.

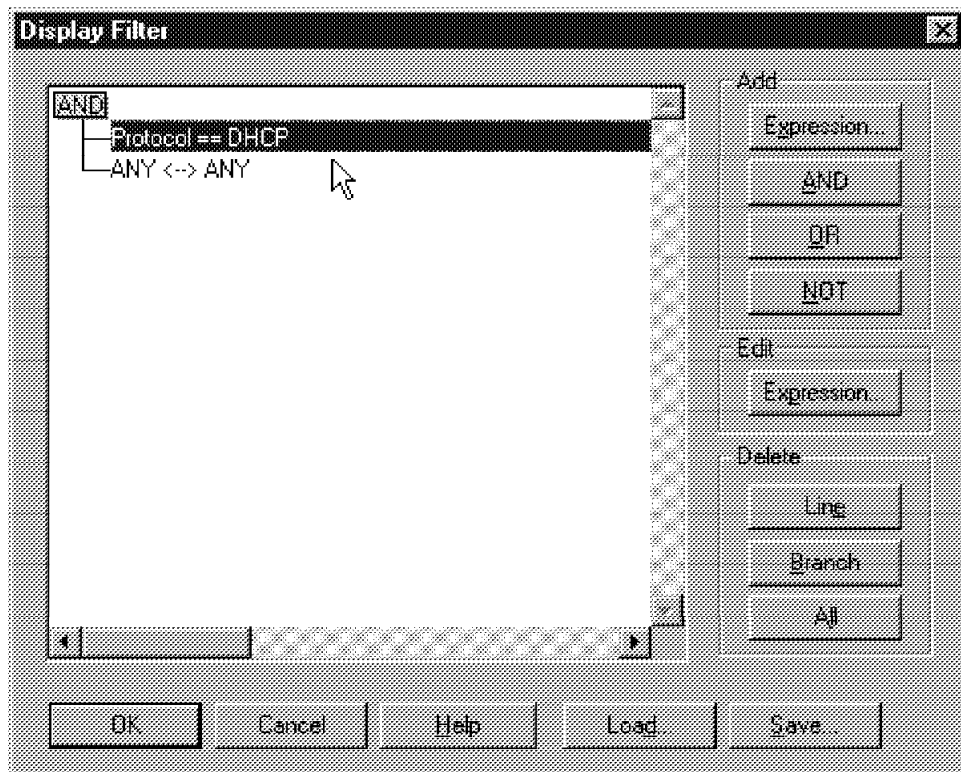


Figure 105. Network Monitor Tool - Display Filters

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.

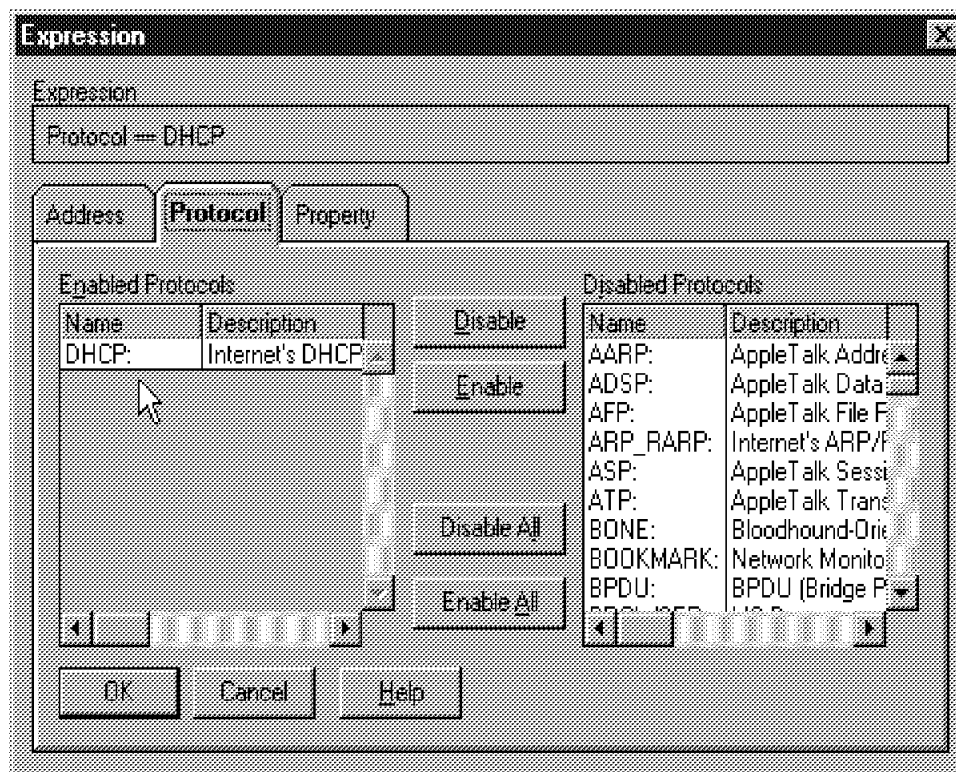


Figure 106. Network Monitor Tool - Selecting the DHCP Frames Only

- Display only frames originating from, or destined to, specific addresses, and these addresses can be expressed as MAC addresses, or IP addresses, or 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 107. 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.

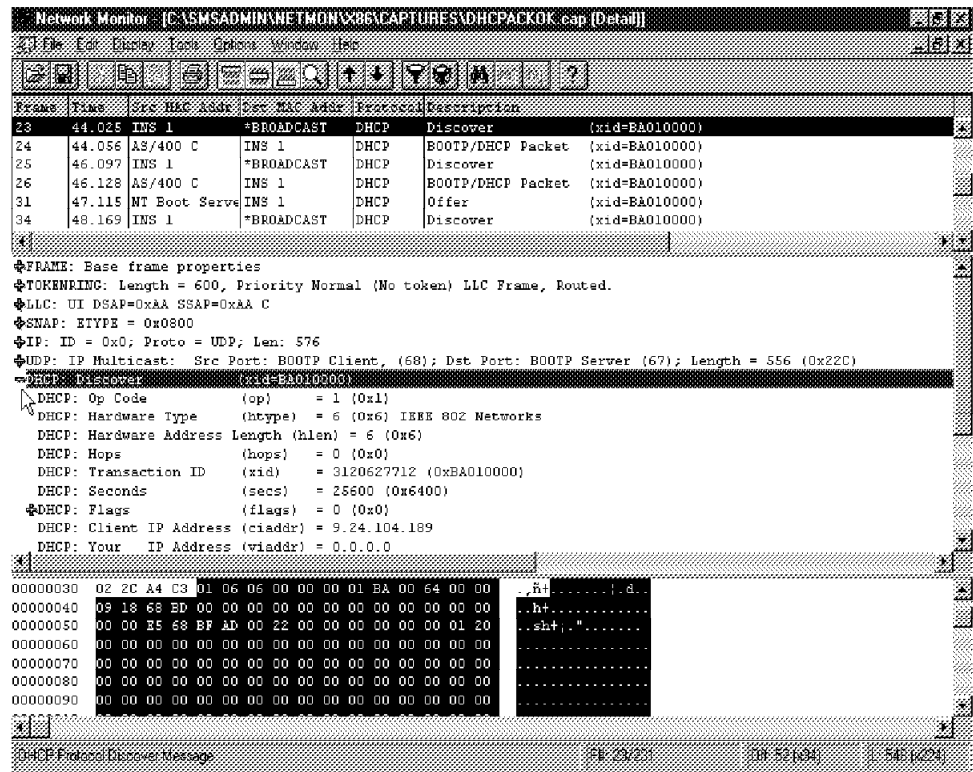


Figure 108. Network Monitor Tool - Displaying Details of Each Frame

#### 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:

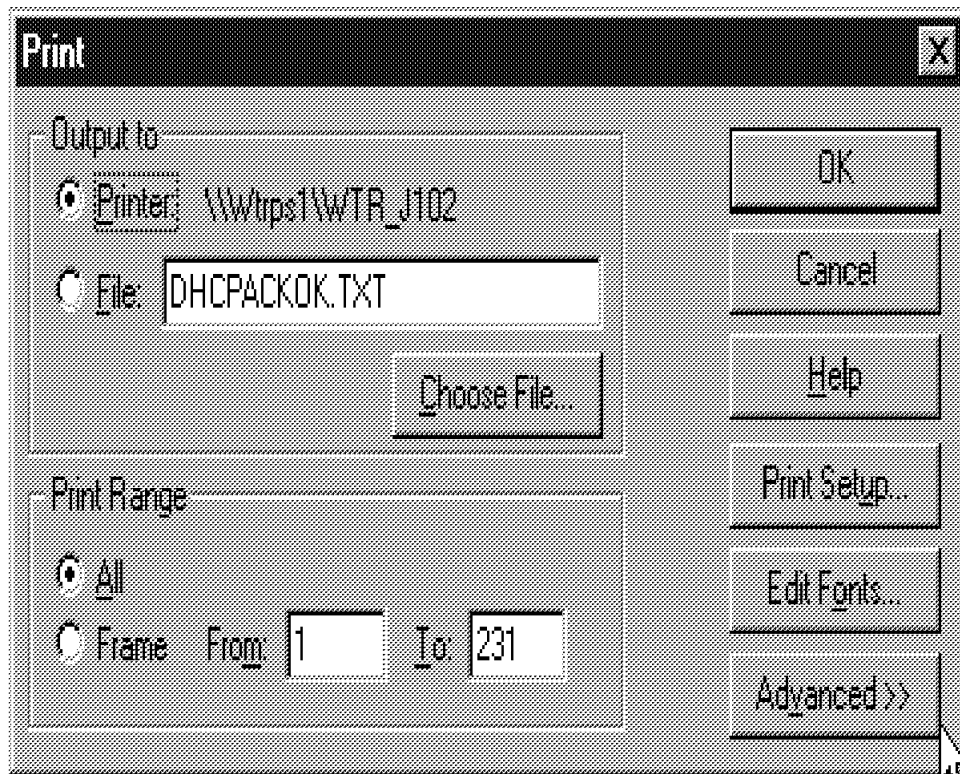


Figure 109. Network Monitor Tool - Printing Selected Frames

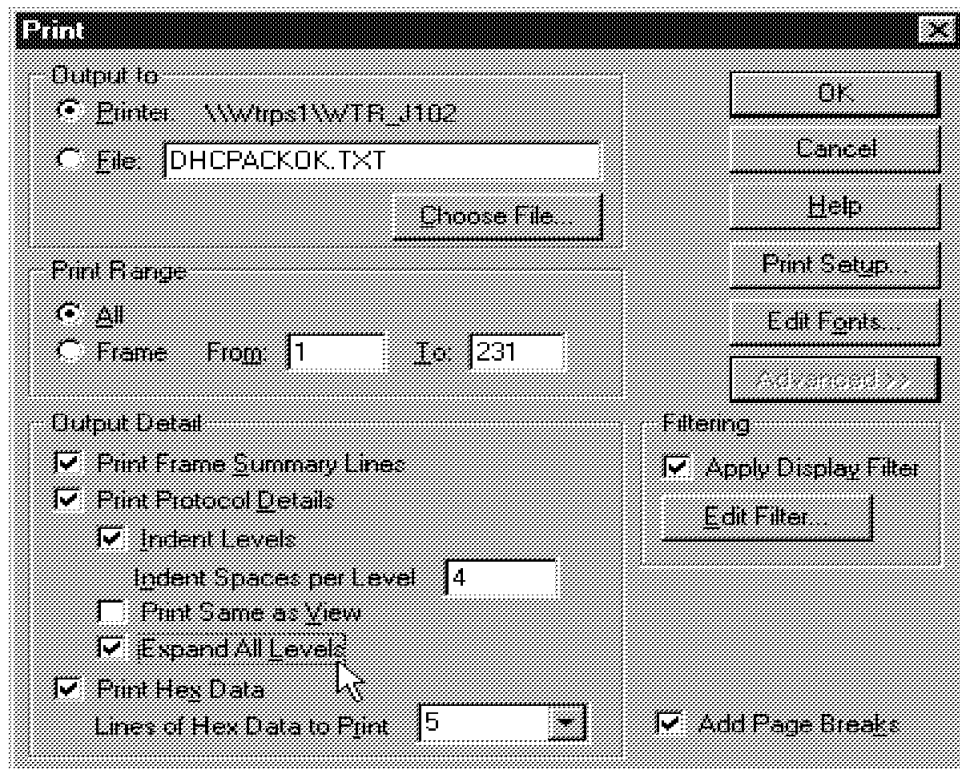


Figure 110. Network Monitor Tool - Printing Selected Frames-Advanced Options

## 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 : FFFFFFFF
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 111. Network Monitor Tool - Sample Printed Output. 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 (0x022C)
    UDP: Source Port = BOOTP Client
    UDP: Destination Port = BOOTP Server
    UDP: Total length = 556 (0x022C) 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 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 112. Network Monitor Tool - Sample Printed Output. 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 113. Network Monitor Tool - Sample Printed Output. Frame 31 - A DHCPOFFER 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 (0x248)
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 (0x240)
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 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 114. Network Monitor Tool - Sample Printed Output. Frame 31 - A DHCP OFFER Frame - Page 2

## 12.7 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 preprogrammed 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 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 9.12.14.1 -graphics`; this command starts a 3270 session with the 9.12.14.1. 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 options called `-debug`, he 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, or he can simply issue an RSH command to start the command execution remotely.

In this case, from a remote machine, he would issue:

```
RSH IP-address-of-netstation ns3270 9.12.14.1 -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.

## 12.7.1 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 of these functions, he 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 stats 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 - Start 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

Note that the above commands can be executed remotely as long as they have not been disabled. 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 (thru 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 which 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 thru RSH but cannot start the `quicksetup` command.

```
set xserver-initial-x-resources = "ncdconsole.disableReboot: false\n\
ncdconsole.disableLoginMenu: false\n\
ncdconsole.disableTerminalMenu: false\n\
ncdconsole.disableSetupMenu: true"

set exec-disabled-commands = {
#   { login }
#   { logout }
    { serial }
    { dialer }
    { quicksetup }
#   { setup }
#   { pref }
```

## 12.7.2 Help on Commands

Some help information is available on some of these commands. We have used the following, from a remote host, to get information on the nsb command, which loads the IBM Network Station Browser:

```
rsh netstationaddress loadb nsb -help
```

This produced the information below:

```
Usage: nsb [-options ...]
```

where options include:

- display host:display X Server to open a connection to
- fg color Foreground color to use in gui
- bg color Background color to use in gui
- verbose Echo verbose messages to stderr
- default Attempt to use the default colormap
- Depends on -colors setting
- private Force use of a private colormap
- colors ### Specify minimum colors needed before creating a new colormap
- 8 Force use of 8 bit visual on display
- 24 Force use of 24 bit visual on display
- gray Force use of GrayScale visual on display
- url "http://..." Specifies url to load on startup
- If port is omitted a random port is used
- noresources Use minimal fallback resource settings

We then used a few more commands to see how much we could get, and below is the output of some of these commands:

```
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 <a href="http://home.netscape.com/newsref/std/x-remote.html">http://home.netscape.com/newsref/std/x-remote.html</a>
-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.

Usage: ns3270 [3270\_options] [X-Windows\_options] hostname

3270\_options:

-----

[-cols columns] [-debug] [-graphics] [-ims] [-LANGID language\_id]  
[-MRIPATH MRInnnn] [-nographics] [-pfkeys] [-port port]  
[-rows rows] [-title title] [-trace] [-version]

X-Windows\_options:

-----

[-help]

5250 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

usage: show version | memory | connections

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	<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>	resource to be used in this instance of ncterm (may be specified more than once)

usage: login [-indirect] [hostname[:]]

usage: test net

usage: net [-display dpy] [-tcpip] [-ncdnet] [host]

---

## 12.8 Using the Config Daemon from a Remote Location

As stated previously, the preferred method of making configuration changes is to use the Network Station Manager, because its structured interface prevents the user from making errors.

When parameters cannot be changed through the Network Station Manager, or when the changes are simple alterations of existing configuration statements, then using an editor to manually alter the configuration files might be a time saver for the administrator. However, be aware that some files only have an LF at the end of a line instead of CRLF, and use of a standard PC editor might cause some problems if it is not designed to recognize this. If you must edit, use an editor which does recognize the difference, such as the PFE32 editor.

On some occasions during problem determination however, it might be useful for the administrator to remotely change the settings in a Network Station's NVRAM in order to test a situation and see the impact of configuration changes.

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, 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 115. Config Daemon Commands for Read-Only

#### Is there a better way?

This is one way of accessing the remote config daemon, if it is done from any machine with TELNET capabilities. However, if you have a Network Station, a much better way is to use the console facility on one Network Station to access another station. This is described in 12.9, "Accessing the Setup Panels from Another Network Station" on page 196.

If the password entered is the password for Read-Write, the command is much more extensive as it allows not only to 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 116. Config Daemon Commands for Read-Write

The user must know the name of the configuration parameters in order to use these commands. The complete list of configuration parameters can be found in the configd2.doc file in the /nstation/configs directory on the boot server.

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 he has 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 is trying to do problem determination on, and maybe set other parameters, and so on.

---

## 12.9 Accessing the Setup Panels from Another Network Station

Another way to have remote access to the configuration data on a Network Station is to use the console functions on one Network Station to access another 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:

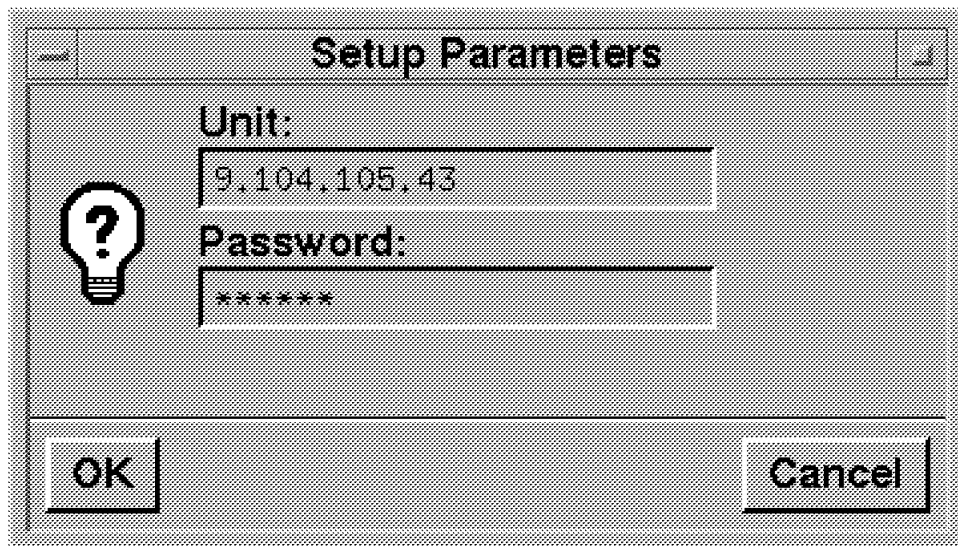


Figure 117. Connecting to a Remote Station

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 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 the **Restore Defaults** on the file pull-down.

---

## 12.10 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.

```

BL [file] boot locally
BN [file] [local-IP host-IP] [gateway-IP] [subnet mask] boot via nfs
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
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
SE nvram setup
SM show memory configuration
ST stack trace
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 118. Boot Monitor Commands

## 12.11 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
+ 0:00:00:33
%NETFILE-I-PERMCHKATTEMPT, attempting permission check for /usr/lib/X11/bitmaps/
Login
%NETFILE-W-MATCHFAIL, TFTP permission check attempt for /usr/lib/X11/bi

```

Figure 119. Message Log when File Extended Diagnostics is 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 which 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.

## 12.12 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

### 12.12.1 Using TFTP to Upload a DUMP File

Here is a suggested procedure to upload via TFTP.

- On the boot server
  - Create a directory called \nstation\service
  - Create a dummy file called yyyyyyyy.dmp where yyyyyyyy is last 8 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.
  - Stop the TFTP service on the server
  - Update the TFTP configuration to allow write operations
  - Restart the TFTP service on the server
- On the Network Station, after the Panic screen
  - Issue the UP boot monitor command. If you do not specify any other parameter (which is the easiest method), the path defaults to \nstation\service\ and the file name defaults to yyyyyyyy.dmp, where yyyyyyyy is the last 8 digits of the MAC address of the Network Station.  
  
**Note:** If you specify a filename, then do not specify an extension (dmp). If you do, you will get filename.dmp.dmp as the filename, which will be invalid.
  - The adapter is opened, the ring entered, and a progress indicator bar appears (similar to the progress bar you get during a kernel load).
- On the server, after the upload, remember to stop the TFTP service, reset the configuration to read only and restart the TFTP service.

### 12.12.2 Using NFS to Upload a DUMP File

If you prefer to upload using NFS, the procedure is as follows:

- On the boot server:
  - Create a directory called x:\nstation\service, where x is whatever drive you want
  - Create a dummy file called yyyyyyyy.dmp, where yyyyyyyy is the last 8 digits of the MAC address of the Network Station (or a simpler name if you wish).
  - Define an NFS alias of /tftpboot/ for the x:\nstation\service\ and specify write access
  - Update the NFS config to remove the use of NT security  
  
**Note:** There is no need to restart the NFS service for this to take effect.
- On the Network Station, after the Panic screen:
  - Issue the UN boot monitor command followed by a filename (The filename should be the name you used to create the dummy file).  
  
**Note:** A filename MUST be specified; there is no default filename as with the UP command.
  - Let the path default to /tftpboot/ (which is why we had you create an alias of tftpboot before).
  - Specify an extension for the filename. There is no default so you can use your own. We use .dmp for consistency with the TFTP method.
  - The adapter is opened, the ring is entered and a progress indicator bar appears.

- Remember to turn Windows NT security back on after the upload if this is your normal mode of operation.

### 12.12.3 Which Method Should You Use for the Upload?

Which method to use is probably more a user preference issue than anything else. However, since this command will likely be used by an end user, at the request of an administrator which might be at a remote location, our recommendation is to make it as easy as possible for the user to execute.

Also, the execution should not be disruptive to other users, if possible.

We find that the NFS method is the least disruptive, because it does not require an NT service to be stopped and restarted on the server.

On the other hand, a filename must be specified on the UN command (whereas the user can just use the UP command with no parameters); but, the administrator can set it up so that the filename is easy, such as the user name. The administrator has to create a dummy file anyway, so he can use the name he likes.

Note that the user might be asked to accompany the DUMP file with the output from the DS and ST commands as well. This is really determined by the service personnel.

---

## 12.13 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:

- 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.
- Issue the NV command to run the NVRAM utility
- Type L to load the Network Station's defaults
- Type S to save these default parameters; confirm Yes
- Type Q to quit and return to the boot monitor
- Use F1 to get back to the SETUP utility

---

## 12.14 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 which are necessary to boot the Network Station.

There might be cases where you, as the administrator, forgot what password was set for a particular station.



You might also get the case where the station was booted from a boot server which is not yours, and that server's configuration files included a password which 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:

- Power off the Network Station.
- Open the cover.
- Locate the TP1 and TP2 test points.

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.

- CAREFULLY shunt the TP1 and TP2 test points with a flat head screwdriver, and while holding tightly, power on the station.
- A red message NS0210 NVRAM initialize jumper detected after 2-3 seconds indicates success.
- Power off, re-install the cover and you are ready to proceed.

---

## 12.15 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 is 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 (see the configd2.doc file), 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 which 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 using the **Reboot** item on the Console pull-down, or you can use the control key sequences we discussed earlier.

---

## 12.16 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.

---

## Appendix A. Sample Configuration Files

We include here a listing of the configuration we have been using in the production of some of the examples in this document.

Please be aware that these files reflect a test environment as opposed to a real production environment; for example, we have opened up all of the Network Station console pull-down menus by modifying the standard parameters, but an administrator would likely not do this with real users.

You should read Chapter 5, "IBM Network Station Customization Files" on page 41 first in order to get familiar with what each of the files is supposed to contain and whether they should be modified or not.

The files listed below are as they are after we made some entries using the Network Station Manager and also after we made some changes manually to suit our needs. Whenever possible, we have not altered the original files, as supplied with the installation, but we have put most of our changes in the defaults.dft file.

Our imbedded comments are preceded by the # sign, which is also the way to specify comments in these configuration files.

```
*****
*****
* File: \nstation\configs\itsonctl                                     *
*****
* This file was created, as is, when we used the NSM to configure    *
* data specific to the itsonctl workstation. We had specified this  *
* itsonctl name first in the DHCP configuration, as option 12.      *
*                                                                     *
* Initially, you will not have such a file, and it is not needed,   *
* until such time that you want to configure workstation specific   *
* parameters.                                                        *
*                                                                     *
* The file only contains pointers to get the kernel to read other   *
* configuration files.                                               *
*****
```

```
read standard.nsm
read itsonctl.nst
read itsonctl.trm
```

```
*****
*****
* File: \nstation\configs\standard.nsm                               *
*****
* This is normally the first file read when there are no workstation *
* specific files.                                                    *
* This file causes all the other files to be read.                 *
* You would normally not alter this file unless you have a need to  *
* add other files or alter the read order.                           *
*****
```

```
read required.nsm
read control.nsm
```

```

read hosts.nsm
read defaults.nsm
read defaults.dft

```

```

*****
*****
* File: \nstation\configs\required.nsm                      *
*****
* This file is the main configuration file. The content here is *
* as is supplied with the installation. We want to change some of *
* these parameters, but we do it in the defaults.dft file below *
* rather than modify this original file. This is the recommended *
* method                                                         *
*****

```

```

set boot-automatically = true
set boot-desired-source = tftp
set boot-persistent-loading = false
set boot-second-source = none
set boot-tcpip-broadcast-boot-request = false
set boot-test-ram = true
set boot-third-source = none
set config-add-domain-to-unit-name-as-filename = false
set config-auto-save-file = false
set config-auto-save-nvram = true
set config-generic-file = true
set config-load-initial-file = true
set config-persistent-loading = false
set config-unit-ethernet-address-file = false
set config-unit-ip-address-file = false
set config-unit-name-file = true
set config-use-decimal-ip-address-notation-as-filename = false
set exec-access-control-enabled = true
set exec-access-control-list = {"127.0.0.1" tcpip}
set exec-command-menu = {
    { "Console" "console" }
}
set exec-disabled-commands = {
# { login }
# { logout }
    { serial }
    { dialer }
    { quicksetup }
    { setup }
    { pref }
}
set exec-startup-commands = {
    { actlogin }
}
set file-manager-access-control-enabled = true
# set file-manager-access-control-list = { }
set file-name-type-for-initial-tftp-servers = unix
set modules-load-policy = {
    { "libx2" at-boot }
    { "libxt" at-boot }
    { "libxm" at-boot }
    { "libconf" at-boot }
    { "actlogin" at-boot }
}

```

```

    }
set pref-console-key-sequence = "Alt-Shift-Home"
set pref-screensaver-interval = 3
set serial-access-control-list = { { "127.0.0.1" tcpip } }
set tcpip-dns-default-domain = nil
set tcpip-name-cache-ignore-case = true
set tcpip-name-server-protocol = dns
# set tcpip-name-servers = { }
set unit-query-for-name-at-boot = none
set xserver-access-control-enabled = true
set xserver-access-control-enabled-default = true
# set xserver-access-control-list = { }
set xserver-initial-x-resources = "ncdconsole.disableReboot: true\n\
ncdconsole.disableLoginMenu: true\n\
ncdconsole.disableTerminalMenu: true\n\
ncdconsole.disableSetupMenu: true"

*****
*****
* File: \nstation\configs\control.nsm *
*****
* We have not modified this file. It is the original file as *
* created by the installation process *
*****

set boot-prom-update-file = nil
set java-appletviewer-command = default
set pref-keyboard-auto-repeat = true
set pref-keyboard-auto-repeat-rate = 20
set pref-keyboard-auto-repeat-start = 500
set pref-mouse-acceleration = 300
set pref-mouse-arrangement = right-handed
set pref-power-manage-powerdown-time = 60
set pref-power-manage-standby-time = 20
set pref-power-manage-suspend-time = 40
set pref-screen-background-bitmap-background = "#4A0BC1"
set pref-screen-background-bitmap-file = "/NStation/ProdData/SysDef/ibmwall.xbm"
set pref-screen-background-bitmap-foreground = "#7F3FF5"
set pref-screen-background-color = "#0183C6"
set pref-screen-background-type = bitmap
set pref-screensaver-bitmap-file = "/NStation/ProdData/SysDef/ibmwall.xbm"
set pref-screensaver-enable = true
set pref-screensaver-style = bitmap
set pref-screensaver-time = 600
set pref-xserver-backing-store = disabled
set serial-access-control-enabled = false
set unit-contact = nil
set unit-global-password = nil
set unit-location = nil

*****
*****
* File: \nstation\configs\hosts.nsm *
*****
* This file is not created by the installation process, although it *
* is put in the standard.nsm file as a file to be read. *
* So far, we have not seen if the NSM is supposed to update this *

```

```

* file or not.
* We have therefore use it to make any change to any TCP/IP related
* parameters, so that we group all these in this single file.
* We have also used it in the same manner as the traditional
* TCP/IP hosts file, that is to equate host names to IP addresses
* to avoid a DNS name lookup or to supercede the DNS entries
*****

# We specify below the two Domain Name Servers that we use
# on this itso network
#
set tcpip-name-servers = {
    {9.24.104.108}
    {9.24.104.209}
}

#
# The entry below must be set in order for the browsers to work
# properly; otherwise, the browsers will not be able to resolve
# any of the URLs you specify
#
set tcpip-dns-default-domain = itso.ral.ibm.com
set tcpip-name-cache-ignore-case = true
set tcpip-name-server-protocol = dns
#
# The entries below are just like a traditional HOSTS file in
# TCP/IP. In this case, we indicate that the name WTSCPOK should
# be resolved as 9.12.14.1. This avoids a DNS lookup and allows you
# to use your own names without a need to update the DNS.
#
set tcpip-name-local-cache = {
    { wtscpok 9.12.14.1 }
}

*****
*****
* File: \nstation\configs\defaults.nsm
*****
* We have not modified this file.
*****

set java-appletviewer-command="java -verbose ncd.applet.NCDAppletViewer"
set pref-keyboard-auto-repeat-rate=30
set pref-mouse-acceleration=1000
set pref-screen-background-bitmap-background="#90A0F0"
set pref-screen-background-bitmap-file="/NStation/ProdData/SysDef/tiles.xbm"
set pref-screen-background-bitmap-foreground="#6279EA"
set pref-screen-background-type=bitmap
set pref-screensaver-style=blank

*****
*****
* File: \nstation\configs\defaults.dft
*****
* This file is where we put all the changes that we want to make to
* all the preceeding parameters. But putting these changes here, we
* override the above parameters without altering the original files.
*****

```

```

# The parameter below is normally set to none. We set it to tcpip
# when we want, at the NEXT boot, the station to use the itsonct1
# (the workstation specific file) as the first file instead of the
# standard.nsm file. this is what triggers this file to be read.
#
set unit-query-for-name-at-boot = tcpip
#
# Below, we specify the host names or IP address of those hosts
# which are authorized to use the RSH command in order to cause
# local execution of a command
#
set exec-access-control-list = {
    {"127.0.0.1" tcpip}
    {"9.24.104.175" tcpip}
    {"wtr05210.itso.ral.ibm.com" tcpip}
}
#
# The parameter below indicates that x-clients trying to access
# this X-server (i.e. trying to export their display to this
# station) need to be identified in the local access control list
#
set xserver-access-control-enabled = true
set xserver-access-control-enabled-default = false
#
# So, we would normally specify the authorized x-clients in the
# list below. However, we commented it out because we use another
# facility instead, which is the xhost command. We use this command
# in the startup files to dynamically populate the Access control
# list instead of using the xserver-access-control-list parameter
# here. The effect is the same.
# set xserver-access-control-list = { } (Disabled thru the #)
#
# The statements below determine which of the pull-down menus on
# the Network Station console get enabled. These entries were
# initially set (in the required.nsm above) to true, which
# means they were disabled, and that would probably be fine
# for a normal user. But we needed to have all of these enabled
# to work as an administrator, so we set them all to false
#
set xserver-initial-x-resources = "ncdconsole.disableReboot: false\n\
ncdconsole.disableLoginMenu: false\n\
ncdconsole.disableTerminalMenu: false\n\
ncdconsole.disableSetupMenu: false"
#
# Additionally, even though we enabled the SETUPMENU pull-down in
# the preceding statement, that particular pull-down has three
# entries, which are the commands to access the configuration
# data on the Network Station. These individual commands can
# also be individually enabled/disabled. In the statement
# below, in addition to the login and logout commands, we are
# enabling the quicksetup, setup and pref commands, by specifying
# the comment symbol (#) besides it so that it is NOT included
# in the list of commands to be disabled. See the settings in the
# original required.nsm above
#
set exec-disabled-commands = {
# { login }
# { logout }
    { serial }
}

```

```

    { dialer }
#   { quicksetup }
#   { setup }
#   { pref }
}

```

```

*****
*****
* File: \nstation\configs\itsonctl.nst
*****
* This file was created by the NSM when we specified a few
* workstation specific settings for the itsonctl station.
* It will be read after all the files above and therefore override
* any of the previous settings for the same parameters
* Note that it will be read ONLY if we have also enabled it by
* settings the unit-query-for-name-at-boot parameter
*****

```

```

set pref-power-manage-standby-time=10
set pref-xserver-backing-store=when-mapped
set serial-access-control-enabled=false
set unit-contact="Claude Bechard"
set unit-location="ITS0-Raleigh - Claude's Office"
set xserver-keyboard-type=ibm-ps/2

```

```

*****
*****
* File: \nstation\configs\itsonctl.trm
*****
* This file is created by the NSM but it has no initial content.
* It is meant for the administrator to use if he wants to
* add workstation specific parameters not supported by the NSM or
* to manually override the parameters in the itsonctl.nst above
*****

```

```

set boot-test-ram = false
# In this case, we have manually added a statement here which
# causes this particular station to bypass its RAM test during
# the boot phase. This is used just as an example.

```

```

*****
*****
* File: \nstation\userdata\claudes\claudes.nsu
*****
* This file is created by the NSM. Since this one is read after
* the user has logged in, it is meant to specify parameters which
* are specific to one user.
* In this case, CLAUDE is the name of the specific user
*****

```

```

set java-appletviewer-command = "java -verbosegc ncd.applet.NCDAppletViewer"
set pref-keyboard-auto-repeat-rate = 20
set pref-keyboard-auto-repeat-start = 100
set pref-mouse-acceleration = 1000
set pref-mouse-arrangement = right-handed
set pref-screen-background-color = "#99FFCC"
set pref-screen-background-type = solid-color

```



```

set pref-screen-background-type = bitmap
set pref-screensaver-bitmap-file = "/NStation/ProdData/SysDef/ibmwall.xbm"
set pref-screensaver-bitmap-file = "/NStation/ProdData/SysDef/ibmwall.xbm"
set pref-screensaver-enable = true
set pref-screensaver-style = bitmap
set pref-screensaver-time = 900
read /nstation/UserData/claudea/claudea.usr
# notice this last statement which directs a read of the next file

*****
*****
* File: \nstation\userdata\claudea\claudea.usr *
*****
* This file created by the NSM but it has no initial content. *
* It is meant for the administrator to use if he wants to *
* add user specific parameters not supported by the NSM or *
* to manually override the parameters in the claudea.nsu above *
* or any of the preceding configuration files. *
*****

set pref-console-key-sequence = "Pause"

## With this command, we are setting the key sequence which toggles
## the console on and off on the desktop to the Pause key.
## This is only effective for user claudea because this file only gets
## processed when the user named claudea logs in.

set exec-disabled-commands = {
#   { login }
#   { logout }
#   { serial }
#   { dialer }
#   { quicksetup }
#   { setup }
#   { pref }
}

## Above, we inserted # (comment mark) to prevent the disabling
## of the login, logout, quicksetup, setup and pref commands on
## the console pull-downs. Again, this is effective only for user
## claudea because this file is processed only when user claudea
## logs in.

*****
*****
* File: \nstation\ProdData\sysdef\startup.nsm *
*****
* This is the first of three STARTUP.NSM files. this is the system *
* level file, applicable to all workstations; the next one will be *
* the user level file, applicable to all users, and the last one *
* is the specific user file, applicable to one specific user *
* *
* In this file, we specify some initial settings for the http port *
* for example, and the fact that we do want a task bar to appear on *
* the user's desktop. *
* We also specify that the MENU bar contains buttons to start a *
* 3270 session, a 5250 session, the IBM browser, the Navio browser *
* and an X-session *

```

```
* We also start the window manager (wm) *
```

```
*****
SET TRACE ON
SET NSM_HTTP_PORT 80
SET NSM_LOGOUT YES
SET NSM_HIDE YES
SET NSM_TOPBOTTOM YES
SET NSM_LOCK YES
SET NSM_TASKBAR YES
MENUITEM "5250" ns5250
MENUITEM "3270" ns3270
MENUITEM "IBM Browser" loadb nsb
MENUITEM "Navio Browser" loadb navio
MENUITEM "new X session" rsh 127.0.0.1 login
RUN wm
```

```
*****
*****
* File: \nstation\userdata\sysdef\startup.nsm *
```

\* Some of the same parameters we had in the previous file are  
 \* repeated here (no harm done). We added (thru the NSM) the  
 \* name and port for the socks host (this is required for the  
 \* browsers to work properly. We also include on the menu bar an  
 \* entry to start an X-session with a WinCenter server. Notice  
 \* the xhost command which adds the wincenter host to the access  
 \* control list so that the WinCenter x-client can use the  
 \* Network Station's x-server

```
*****
```

```
SOURCE /nstation/ProdData/SysDef/startup.nsm
SET TRACE ON
SET NSM_HIDE YES
SET NSM_LOCK YES
SET NSM_LOGOUT YES
SET NSM_TASKBAR YES
SET NSM_TOPBOTTOM YES
SET NSM_HTTP_PORT 80
SET SOCKS_HOST socks1.server.ibm.com
SET SOCKS_PORT 1080
RUN xhost wincenter.itso.ral.ibm.com
MENUITEM "WinCenter" rsh wincenter.itso.ral.ibm.com wincenter -display ${IP}:0
```

```
*****
*****
* File: \nstation\userdata\claudea\startup.nsm *
```

\* The entries here are only applicable to the user names claudea.  
 \* We added three entries on the menu bar. The first two are starting  
 \* an X-session on the rs600026 AIX host to execute the xclock  
 \* application and to get and AIXTERM session on the Network Station  
 \* The last one starts a java applet.

```
*****
```

```
SOURCE /nstation/UserData/SysDef/startup.nsm
SET FULL_NAME "Claude Bechard"
RUN xhost rs600026.itso.ral.ibm.com
MENUITEM "AIXterm-RS600026" rsh rs600026.itso.ral.ibm.com aixterm -display ${IP}:0
MENUITEM "Xclock" rsh rs600026.itso.ral.ibm.com xclock -display ${IP}:0
MENUITEM "java-clock-a" appletviewer /nstation/java/classes/demo/clock/example1.html
```



---

## Appendix B. Boot Monitor Commands

Here is a list of commands available from a boot monitor command prompt.

You can also get this list 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  
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  
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  
SE nvram setup  
SM show memory configuration  
ST stack trace  
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. Useful Control Key Sequences

We have reproduced here, for your convenience, the table which lists the control key sequences.

These 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.

<i>Table 7. Key Combinations For Setup Utility and Boot Monitor Program</i>			
<b>Key Combination</b>	<b>Context</b>	<b>Action</b>	<b>Special Note</b>
Esc	Boot time	Stops downloading kernel and invokes Network Station Utility Main Menu	
Left Alt + Left Ctrl + Left Shift + F1	Network Station Setup Utility	Enter the boot monitor program	Only 101/102 keyboards
Left Alt + Left Shift + F1	Network Station Setup Utility	Enters the boot monitor program	Only 5250/3270 keyboards
F1	Boot monitor program	Switch to Network Station Setup Utility Panels	
Left Alt + Caps Lock + Pause	Window manager	Use keys in this sequence. Enters boot monitor program	All applications terminated and there is no chance to switch back to the window manager.

Note that the key sequence to toggle the console on and off the Network Station desktop is, by default, on the NT platform, the "Alt+Shift+Home" key sequence. However, this is a configurable parameter, using the following statement:

```
set pref-console-key-sequence = "Alt-Shift-Home"
```

This parameter is, by default, in the required.nsm file.





---

## Appendix D. Configuration Parameters

Where does one find the information on the parameters that can be specified in the configuration files?

These parameters can be found in a file named configd2.doc located in \nstation\configs. It is a sizable file (274 KB) as it contains detailed information on over 600 parameters.

As this file is too big to be listed here, we have extracted a few records in order to explain the type of information contained in this file.

The configuration parameters are divided into GROUPS; each configuration parameter belongs to a particular group, and the configd2.doc file lists these parameters according to the group they belong to. For example, there is a group called CONFIG, which is the one we took our example from.

We have listed below two parameters from that group; the config-access-control-enabled and the config-access-control-list. Since this second parameter is a table, we have listed below the table entry parameters that accompany this second parameter:

GROUP config

NAME	config-access-control-enabled
HIDEBOX	Console=>Setup=>Change Setup Parameters=> Access Control=>Enable Config Access Control
SNMP NAME	ncdAccessConfigdAccessControlEnabled
SNMP PATH	ncdAccess 8
TYPE	BOOL
DEFAULT	false
PERMISSION	READ-WRITE
EFFECT	IMMEDIATE
NVRAM	NO
DESCRIPTION	Specifies whether requests for connections to the configuration daemon from outside the terminal will be checked against the host access control list

NAME	config-access-control-list
HIDEBOX	Console=>Setup=>Change Setup Parameters=> Access Control=>Config Access Control List
SNMP NAME	ncdAccessConfigdHostTable
SNMP PATH	ncdAccess 9
TYPE	TABLE
PERMISSION	READ-WRITE
EFFECT	IMMEDIATE
NVRAM	NO
DESCRIPTION	Specifies the host access control list for the configuration daemon.

BEGIN TABLE ROW ENTRIES

NAME	index
SNMP NAME	ncdAccessCHTIndex

SNMP PATH ncdAccessConfigdHostTable 1  
 TYPE INTEGER  
 VIEW SNMP ONLY  
 MIN 0  
 MAX 4294967295  
 PERMISSION READ-ONLY  
 NVRAM NO  
 DESCRIPTION  
     Index into the Config Access Control List

NAME host  
 SNMP NAME ncdAccessCHTAddress  
 SNMP PATH ncdAccessConfigdHostTable 2  
 TYPE STRING  
 DEFAULT nil  
 PERMISSION READ-WRITE  
 EFFECT IMMEDIATE  
 NVRAM NO  
 DESCRIPTION  
     Specifies the network name/address  
     of a node granted permission to  
     remotely access the configuration  
     daemon.

NAME family  
 SNMP NAME ncdAccessCHTFamily  
 SNMP PATH ncdAccessConfigdHostTable 3  
 TYPE CHOICE  
 CHOICES { tcpip ncdnet }  
 DEFAULT tcpip  
 PERMISSION READ-WRITE  
 EFFECT IMMEDIATE  
 NVRAM NO  
 DESCRIPTION  
     Specifies the type of network connection for  
     which this entry applies.

END TABLE ROW ENTRIES

Here are a few explanations on each of the above entries:

- GROUP config

This simply indicates that this is the beginning of the parameters that are part of the group config.

- The next 14 lines describe the characteristic of the first parameter, called config-access-control-enabled.

- NAME config-access-control-enabled

This is the name of the parameter as is used in the configuration file. For example, in this case, the line set config-access-control-enabled = true could appear in one of the configuration files.

- HIDEBOX Console→Setup→Change Setup Parameters→ Access Control-Enable Config Access Control

This entry describes how to access the parameter setting through the Console pull-down menus by listing the path required to get to this parameter.

Remember that when you use the Console Setup pull-down, you can see the setting of the parameter, and even temporarily change the value of a parameter, but you cannot change it permanently. For a permanent change, you must update the configuration file on the server.

- SNMP NAME `ncdAccessConfigdAccessControlEnabled`

This is the name of the SNMP variable

- SNMP PATH `ncdAccess 8`

this is the path to the SNMP variable.

- TYPE `BOOL`

indicates the type of parameter. In this case, since this particular parameter can only have the value true or false, it is a boolean type (0 or 1). The next parameter, for example, is a table and therefore its type is `TABLE`.

- DEFAULT `false`

This is the default value of this parameter, assuming that it is not specified. Some parameter do NOT have a default value, in which case this is identified as `NIL`.

- PERMISSION `READ-WRITE`

Most parameters are read-write; however, there are a few that are read-only.

- EFFECT `IMMEDIATE`

This indicates whether changing this parameter will immediately affect the way the station operates, or not. Another potential value of this field, for certain parameters, could be "at boot" for example, indicating that the effect would only become active after a reboot.

- NVRAM `NO`

This indicates whether this parameter is permanently stored in NVRAM or not. If YES, then the value remains even after a reboot of the station. About 80 of the 600 parameters are stored in NVRAM.

- DESCRIPTION

A description the purpose of the parameter.

- The next parameter is the `config-access-control-list`.

Its characteristics are similar to the parameter we just described above, except for the type, which is `TABLE`. This means that this parameter does not have a single value but a table of values.

All the entries that follow, from the `BEGIN TABLE ROW ENTRIES` to the `END TABLE ROW ENTRIES`, describe the entries that can be specified in this table. There is always an index entry first, then, in this case:

- A host entry, which is the IP address or host name address of the host which is given authority to use this feature
- A family of host, which can, in this case, only be `tcpip` or `ncdnet`, as indicated by the `CHOICES` entry.

For example, this parameter could be coded as follows:

```
set  config-access-control-list = {  
    { 9.24.104.180 tcpip }  
    { host1.itso.ral.ibm.com tcpip }  
}
```

---

## Appendix E. Special Notices

This publication is intended to help anyone with a need to install and configure the IBM Network Station Manager for Windows NT Server 4.0 program and related products in order to support and manage a network of IBM Network Stations. The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM Network Station Manager for Windows Server 4.0. See the PUBLICATIONS section of the IBM Programming Announcement for the IBM Network Station Manager or Windows NT Server 4.0 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 use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	AS/400
IBM	MVS/ESA
OS/390	OS/400
RS/6000	S/390
System/390	VM/ESA
VSE/ESA	400

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 F. Related Publications

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

---

### F.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How to Get ITSO Redbooks" on page 225.

- *S/390 - IBM Network Station - Getting Started*, SG24-4954-01
- *RS/6000 - IBM Network Station - A Companion Guide*, SG24-2016-00
- *AS/400 - IBM Network Station - Getting Started*, SG24-2153-00

---

### F.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042





---

## 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 BookManager BOOKs of redbooks, type the following command:

```
TOOLCAT REDBOOKS
```

To get lists of redbooks, type one of the following commands:

```
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
```

To register for information on workshops, residencies, and redbooks, type the following command:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
```

For a list of product area specialists in the ITSO: type the following command:

```
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.htm>). 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** — 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	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States) or (+1)001-408-256-5422 (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.htm>). 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

### Numerics

3270 auto action 107  
3270 graphics 107  
3270 screen size 107  
3270 sessions- number 112

### A

access control 151  
access control - file level 156  
administrator password 85, 147  
applet viewer configuration 128  
application log 166  
apply 100  
autostart - browsers 130

### B

backup domain controller 12  
bibliography 223  
bookmarks 142  
boot monitor - key sequence 149, 215  
boot monitor commands 2, 196  
boot monitor update 85  
boot sequence (DHCP) 58  
BOOTP - What is it? 55  
browser configuration requirements 119

### C

client definition (dhcp) 70  
Client Hardware Type 71  
client id 71  
command line 188  
commands 189  
commands - boot monitor 196  
components installed 25  
config daemon 193  
configd2.doc file 217  
configuration - NFS 21  
configuration - TCP/IP 20  
configuration files 2, 41  
configuration parameter documentation 217  
configuration password 152  
connect to new unit 196  
console 96  
console - messages 160  
console - setup pull-down 99  
console - statistics pull-down 96  
console key sequence 96  
console messages 104  
console password 152  
console pull-down 104

control key sequences 149  
control.nsm 42

### D

dadmin command (dhcp) 76  
defaults.dft 43  
defaults.nsm 43  
desktop manager settings - nsm 87  
DHCP - What is it? 55  
DHCP classes 63  
DHCP clients 64  
DHCP configuration program 60  
DHCP default configuration file 61  
DHCP documentation 57  
DHCP global options 63  
DHCP log 169  
DHCP log - sample 171  
DHCP logging 75  
DHCP options 61  
DHCP options list 67  
DHCP Protocol driver - Installing 18  
DHCP protocol driver - re-installing 32  
DHCP protocol driver - removing 31  
DHCP relay 58  
DHCP server parameters 63  
DHCP subnets 63  
dhcpack 59  
dhcpdecline 59  
dhcpdiscover frame 58  
dhcpcoffer 58  
dhcprequest 58  
dhcpsd.cfg file 27, 60  
dhcpsd.log 170  
diagnostic access control 152  
diagnostic port 161  
directories installed 28  
disabling commands 190  
disabling the DHCP protocol driver 31  
disk cache - browsers 125  
disk space 28  
Display client information 76  
display filters (network monitor) 179  
display server (dhcp) statistics 76  
DNS 13  
documentation Web site 15  
domain name server 13  
download Web site 13  
downloading from the Web 13  
Dump file - uploading 198  
dynamic IP address 57

## E

- editing files manually 42
- editor - pfe32 42
- emulators - Network Station 105
- ENTER key function 107
- Event viewer (NT) 166
- exports file 27, 149
- extended file diagnostics 197

## F

- file diagnostics - extended 197

## H

- hardware settings - nsm 81
- hostname file 44
- hostname.nst 44
- hostname.trm 44

## I

- IBM Network Station browser - installing 19
- initial configuration file 44
- installed components 25
- installed directories 28
- Installing - DHCP Protocol Driver 18
- installing - IBM Network Station browser 19
- Installing - IBM Network Station Manager 18
- installing - Java Development Kit 17
- installing - Navio 19
- installing - TCP/IP services 20
- installing NT 4.0 12
- Internet Information Server 12

## J

- Java Development Kit - installing 17
- JDK 15

## K

- keyboard remap - 3270 106

## L

- launch dhcp configuration 61
- local file system 149
- lock file - Navio 144
- Lock Screen - menu item 91
- Locked TCP/IP Properties 18
- log file - Web server 171
- log files - DHCP 75
- Log Out - menu item 91
- login 155
- login chooser panel 104

## M

- MAC address - Network Station 57
- memory usage 97
- Menu bar 49
- menu item - browsers 131
- menuItem 51
- message log 159
- message log - saving 163
- messages - sample log 164
- mount points 150
- MS DHCP 13
- MS IIS 12
- multiple browser sessions 135
- multiple instances - dhcp configuration 61

## N

- Navio - installing 19
- navio configuration - nsm 137
- network computer profile 2
- Network monitor (NT) 173
- network protocols 13
- Network Station browsers 14
- Network Station Manager 79
- Network Station Manager - Installing 18
- Network Station manager - LOGIN 23
- Network Station manager - registry entries 28
- Network Station manager URL 23, 79
- networking file system - configuration 21
- New X session - menu item 92
- NFS - configuration 21
- NFS alias 155
- NFS protocol 149
- NFS security 154
- NFS UID 156
- NFSD 21
- NSMAdmin user group 22, 79
- NSMUser user group 22, 79, 157
- NSNAdmin user group 157
- NT security 155
- NT services 25

## O

- option 12 - dhcp 81

## P

- PANIC screen 198
- partition size - NT 4.0 12
- password - administrator 147
- password - configuration 152
- password - console 152
- performance considerations 2
- permissions - setting 156
- pfe32 editor 42
- popup keypad 106

- positioning 2
- preference files - application 52
- preferences 2
- preferences - browsers 133
- preferences - Navio 140
- prerequisites 11
- primary domain controller 12
- printing 2
- product documentation 11
- products to download 16
- promiscuous copy mode 173
- proxy server 120, 123

## Q

- quick setup 99

## R

- re-installing the DHCP protocol driver 32
- read order - configuration files 47
- redbooks 1
- registry entries - Network Station manager 28
- reinitialization - dhcp server 76
- remote command execution 189
- remote config daemon 193
- remote configuration 193, 196
- remote execution access control 152
- removing the DHCP protocol driver 31
- removing the products 29
- required.nsm 42
- rsh - using 189

## S

- sample DHCP log 171
- sample dhcp log file 76
- sample dhcpsd.cfg file 73
- sample network monitor output 185
- security log 166
- setup 99
- setup - file pull-down 101
- setup task list - nsm 80
- setup utility - key sequence 149, 215
- Show/Hide - menu item 91
- SOCKS server 120, 123
- standalone server 12
- standard.nsm 42
- startup files 48
- statistics 98
- subnet definition (dhcp) 69
- System log 166

## T

- TCP/IP services - installing 20
- TCPIP configuration 20
- telnet 5998 (messages) 161

- telnet 5999 193
- terminals pull-down 103
- test network 102
- TFTP security 153
- TFTP vs NFS 95, 153
- TFTPD 20
- TIMED 21
- Top/Bottom - menu item 91

## U

- uninstalling 29
- unlisted clients (DHCP) 57
- uploading dump file 198
- URL - Network Station manager 23, 79
- user defaults - nsm 81
- user groups 22
- user preferences 101
- userid.nsu 45
- userid.usr 45
- utilities 102

## V

- verbose option 159
- version 96

## W

- Web server 12
- Web server log file 171
- Web server updates 27
- window manager 103

## X

- x connections 97
- x server access control 151
- xserver 151





---

## ITSO Redbook Evaluation

IBM Network Station Guide for Windows NT  
SG24-2127-00

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.com>
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to [redbook@vnet.ibm.com](mailto:redbook@vnet.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! )

---

---

---

---

---



Printed in U.S.A.

S624-2127-00

