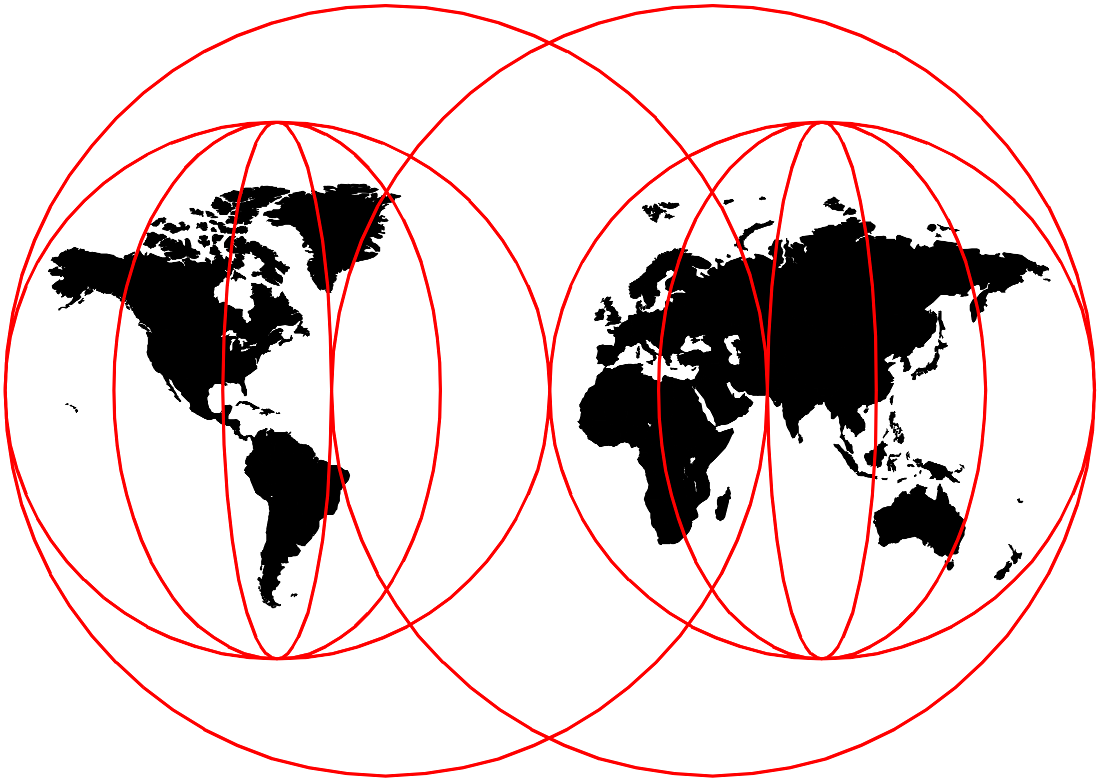
IBM Network Station Manager V2R1

Carla Sadtler, Brian R. Smith, Pawel Andrzejewski, Joan Barrett, Claude Bechard, Bernard Bostaille, David Glenn, Jarmo Lempinen, Mario A. Martinez, Gerri Passe, Henrik Sjostrand



International Technical Support Organization

www.redbooks.ibm.com

SG24-5844-00

International Technical Support Organization

SG24-5844-00

IBM Network Station Manager V2R1

April 2000

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix L, “Special notices” on page 671.

First Edition (April 2000)

This edition applies to Version 2 Release 1 Modification 0 of IBM Network Station Manager, product number 5648-C07, for use with Windows NT, AIX, and OS/400.

Note

This book is partially based on a pre-GA version of a product and may not apply when the product becomes generally available. We recommend that you consult the product documentation or follow-up versions of this redbook for more current information.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, MN 55901-7829

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.

Contents

Preface

This redbook is intended to serve as a complete guide for implementing the IBM Network Station functions. It offers a detailed description of the functions (both old and new) that are available with IBM Network Station Manager V2R1. It even highlights the differences from the previous version. Designed for the advanced user, this redbook is intended to supplement the product documentation for those that want a clearer view of how the IBM Network Station Manager is structured. It contains many helpful hints and techniques for advanced setup.

In addition, this redbook:

- Shows how to design the Network Station environment, including the separation and location of server functions
- Details how to configure the servers and how to use the IBM Network Station Manager to configure the Network Station clients
- Provides detailed information on the DHCP server functions
- Includes information on Windows Terminal Server Edition and MetaFrame setup, with examples

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization's Raleigh and Rochester Centers.

Carla Sadtler is a Senior Software Engineer at the International Technical Support Organization, Raleigh Center. She writes extensively in many areas including Secureway Communications Servers, network integration, Web-to-host integration products, and the IBM Network Station. Before joining the ITSO 14 years ago, Carla worked in the Raleigh branch office as a Program Support Representative. She holds a degree in mathematics from the University of North Carolina at Greensboro.

Brian R. Smith is a Senior AS/400 Specialist in the International Technical Support Organization in IBM Rochester. The first half of his career was spent in design, coding and testing on the System/38 and AS/400 in the area of communications. He then "jumped the wall" into technical marketing support in 1990 to pursue teaching and writing. You can reach Brian on the Internet at `brsmith@us.ibm.com`

Pawel Andrzejewski is Vice Director of the Information Systems Security Department for TRAX, one of the leading IBM Business Partners in Poland. He has been with TRAX for eight years. Prior to his current position, Pawel was employed as a PC and network hardware/software specialist responsible for maintaining TRAX's LAN and WAN (AS/400) infrastructure, and supporting and troubleshooting for customers across Poland. He holds a Master of Science in Computer Science and Automatics, awarded by the Technical University of Zielona Gora, Poland.

Joan Barrett is an Advisory I/T Availability Professional in the AS/400 Software Support Center in Canada. She has worked for IBM for 11 years. Over the past six years, she has worked in the communications group, within the AS/400 platform, supporting customers across Canada and customers in the Caribbean. During the previous five years, she worked as a Customer Service Representative in the Mid-range systems field. Her area of expertise is AS/400 communications and specifically TCP/IP and SNA protocols, workstation controllers, and IBM Network Stations.

Claude Bechard is the program manager responsible for worldwide Technical Education for the IBM Network Station in the Network Computer Division since June 1999. Since 1991, he has been a member of the International Technical Support Organization in Raleigh and produced several redbooks on SNA, on IBM Communications Server products and more recently on the IBM Network Station and Windows NT. He has 30 years of service with IBM and holds a degree in Mechanical and Industrial Engineering from the University of Montreal.

Bernard Bostaille is an IT Specialist at the IBM Global Services, Belgium. He has worked at IBM for almost three years. He has two years of experience in the Network Station field. He has also experience in Windows NT multi-user technologies and Internet-related technologies, where he has developed skills in Lotus Domino (mail architecture, administration, application development). He holds a degree in Physics Engineering from the University of Brussels.

David Glenn is a Support Specialist with the Worldwide IBM Network Station Support Center. He has supported the Network Station product over a year now. Prior to joining the Support Center team, he worked as a PC Technician where he supported such environments as 8088 and MCA-based systems, Twinax Networks, and the more modern workstations and networks that everyone uses today.

Jarmo Lempinen is an IT Specialist in the Global Services of IBM Finland. He has worked at IBM for 10 years. His background is in MVS and OS/390, including roles as a customer software support representative and systems programmer. He has also experience in Internet-related technologies and workflow management, where he has developed skills in OpenEdition, Computer Aided Telephony Systems (CATS), and Net.Commerce. He recently became involved with Network Stations.

Mario A. Martinez graduated as a Computer Engineering Technologist in 1995. Since then, he has been providing Worldwide Technical Support in the areas of Network Communications, controllers (5394 and 5494), and PC software. He has worked both in Canada and the US assisting customers in English and Spanish. Currently he occupies the position of Worldwide Support Specialist within the IBM Network Station Support Center.

Gerri Passe is a Senior Information Technology Specialist with the IBM Americas Advanced Technical Support organization. During the last several years, she has worked with AS/400 customers and Business Partners in the area of IBM Network Station implementation and has also presented at a number of internal and external technical conferences. In addition, she has seven years of prior experience as an AS/400 Systems Engineer and Services Specialist working with Client Access and AS/400 Internet connectivity. Prior to working in the AS/400 environment, she was an IBM S/390 Systems Engineer.

Henrik Sjostrand is an IT Specialist at IBM Sweden. He has two and-a-half years of experience with the Network Station and is currently the regional technical support person for the Network Computer Division, IBM Nordic. His areas of expertise include the Network Station, Windows NT multi-user environment, Java, and Internet technology. Prior to working with the Network Station, he worked with Systems Management products such as Netfinity Manager and the Tivoli framework. He holds a Master of Science in Electrical Engineering from Chalmers University of Technology in Gothenburg, Sweden.

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

Louis Behrens
Eric Bjorklund
Michael Blocksome
Nicole Buss
Tom Christopherson
Dave Gimpl
Harvey Kiel
John Peterson
Mark Plunkett
Ray Romon
Peter Van Wazer
Tony Vinski
IBM Rochester

John Bissell
George Kraft
IBM Austin

John Tesch
IBM Dallas

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 “IBM Redbooks review” on page 685 to the fax number shown on the form.
- Use the online evaluation form found at http://www.redbooks.ibm.com/
- Send your comments in an Internet note to redbook@us.ibm.com

Chapter 1. Overview of Network Station Manager V2R1

The IBM Network Station and its complementing software, the Network Station Manager (NSM), was first released to the market in April 1997. It supported the Network Station Series 100 model (Ethernet and Token-Ring). Network Station Manager included terminal emulation software for accessing AS/400 systems and mainframes (5250 and 3270 respectively), a Web browser, a Java Virtual Machine and X-windows support to access UNIX systems and Windows NT multi-user environments based on Citrix WinFrame and NCDi WinCenter. The very first release of Network Station Manager was only supported on the AS/400 system.

Since then, new models of Network Station have been introduced, and the Network Station Manager code has progressed to provide new function and support for the new hardware. The platform support for the NSM server code has also increased.

NSM at V2R1 is available for the Windows NT, AS/400, and AIX platforms. NSM V2R1 provides support for the new Network Station Series 2200 and Series 2800 models, the Series 1000 Network Stations, and the Series 300 Network Stations. NSM V2R1 does not support the Series 300 Twinax model.

Note

Because of the variety of platforms, file names and path names have been noted using a $ notation. When you see a path name or file name and you want to know the actual value for your platform, refer to Appendix A, “File names and paths” on page 609.

1.1 NSM V1Rx evolution

Version 1 Release 1 (not included in the table) introduced the Series 100 unit, Network Station Manager program, 5250 and 3270 emulators, Java 1.0.2 JVM and IBM (Spyglass) Browser. V1R1 was released in April 1997.

Version 1 Release 2 added the support for the Series 300 unit, the Navio NC Navigator 3.0 browser, and expanded the support of the Network Station Manager across all of the IBM servers. V1R2 was released during the summer 1997.

Version 1 Release 2.5 introduced the Series 1000 unit and support for Java 1.1.2. V1R2.5 was released in January 1998.

Version 1 Release 3 provided internationalization with the required NLS support for SBCS and DBCS languages, Java 1.1.4, ICA client, VT emulation and support for the S300 Twinax model. V1R3 was release June 1998. During the fall of 1998 and spring of 1999, several PTFs, with new features and functions to V1R3, were released.

Table 1 compares the various releases and shows the features that were added with each release.

Table 1. NSM V1Rx evolution

	Release 2	Release 2.5	Release 3	Release 3 added functions
Network Station Hardware				
Hardware (minimum memory)	Series 100 (8 MB) Series 300 (16 MB)	Series 100 (8 MB) Series 300 (16 MB) Series 1000 (32 MB)	Series 100 (16 MB) Series 300 (16 MB) Series 300 Twinax Series 1000 (32 MB)	
NSM Software				
Kernel	Kernel 100/300	Kernel 100/300/1000	Kernel 100/300/1000	
OS	NCDi	NCDi	NCDi	
Browser	Spyglass Browser Navio Browser 3.0	Spyglass Browser Navio Browser 3.0	NC Navigator 3.0	
Java	JVM 1.0.2	JVM 1.1.2 (eng)	JVM 1.1.4 (NLS) JITC	
Host access	3270 5250 X-windows	3270 5250 X-windows	3270 5250 VT X-windows ICA client	TN3270E ICA client enhancements (load balancing, cut/paste, virtual print, virtual com)
eSuite		eSuite WorkPlace 1.0 (Eng only)	eSuite WorkPlace 1.0 (Eng only)	eSuite WorkPlace 1.5
Printing			LPR/LPD	LU1/LU3 3270 printing
National Language Support			32 languages	Romanian Thai Hebrew Arabic
Euro				Euro Symbol support (Emulator only)
Peripheral devices				PCMCIA flash card for local boot Touch screen Multiport Serial Card PCMCIA for S/1000
Boot				
AS/400	V3R2, V3R7, V4R1	V3R7, V4R1	V3R7, V4R1, V4R2	V3R7, V4R1, V4R2, V4R3
Windows NT	Windows NT 4.0, WinCenter 3	Windows NT 4.0, WinCenter 3	Windows NT 4.0, NT/TSE, WinCenter 4	Windows NT 4.0, TSE, Wincenter 4
RS/6000	4.1.5, 4.2.1, 4.3	4.1.5, 4.2.1, 4.3	4.2.1, 4.3	4.2.1, 4.3
S/390	MVS 5.2.2 OS/390 R1, R2, R3 VM 2.1.0, 2.2.0	MVS 5.2.2 OS/390 R1, R2, R3 VM 2.1.0, 2.2.0	OS/390 R4,R5 VM 2.3.0	OS/390 R4,R5,R6 VM 2.3.0

	Release 2	Release 2.5	Release 3	Release 3 added functions
OS/2				OS/2 WSOD R2, Warp 4.0
Flash boot				Y
Split boot			Y	Y

Notes:

- Windows NT/TSE is the Microsoft Windows NT 4.0 Server, Terminal Server Edition product. This is the Windows NT multi-user environment released by Microsoft. It is based on the WinFrame product developed by Citrix.
- At the time of this writing, Microsoft Windows 2000 was not yet a supported platform for NSM V1R3 or V2R1.
- Flash boot means locally booting from a flash card inserted into a Network Station.
- Split boot denotes the capability to separate the boot code from the configuration files, so the Network Stations can boot locally, while still retrieving their configuration settings from a central location.

1.2 What's new in NSM V2R1

Network Station Manager Version 2 Release 1 (NSM V2R1) has added new features or enhanced features previously provided in NSM V1R3. Support for S/390 and for some older Network Station models has been dropped. Some of the changes from NSM R3 include:

- A new Network Station operating system that provides a more standard UNIX operating system.
- A more modernized GUI desktop, based on the Motif 2.1 industry standard.
- Netscape Communicator 4.5 replaces the NC Navigator.
- Java has been enhanced and includes a standalone JVM (the IBM enhanced 1.1.8 JVM) in addition to the Netscape JVM.
- Host access enhancements, including SSL, VTxxx support, and scalable fonts.
- eSuite WorkPlace will not be shipped with NSM. eSuite WorkPlace for Domino R2.0 is supported to provide Web-based access to the popular eSuite applications.
- A print manager is available to monitor Network Station printing.
- Flash boot support, including NSM management of compact flash cards.
- Some NLS languages have not been included in the first release of NSM V2.
- Euro support.
- Hi-color support (16-bit color palette).
- True kiosk mode, in addition to suppressed login mode.
- Additional applications such as an HTML editor, calendar function, file manager, calculator, and a graphics tool.
- NC Audio Player and NC Video Player.
- Hardware support for the new Network Station Series 2200 and Series 2800 models. Support for the Series 100 and the Series 300 Twinax has been dropped.

1.2.1 New Network Station operating system

Network Station Manager V2R1 integrates a new Network Station operating system, the *NC OS*, which will *replace* the previous *NCDi OS* from NCD. NC OS is a more standard UNIX-based operating system provided by NCi (now called Liberate Technologies). It supports functions equivalent to those already available in the Network Station product utilizing the NCDi OS.

In addition, it provides:

- Greater color depth support (65536 colors)
- Scalable font support
- Improvements in load time
- Better memory utilization
- POSIX standards compliance
- Thread support
- Preemptive multi-tasking

With these additional functions, the V2R1 Network Station operating system becomes a more robust development and operating environment. It provides greater stability and ease of adding additional software elements and hardware support.

The major components of the NC OS are shown in Figure 1.

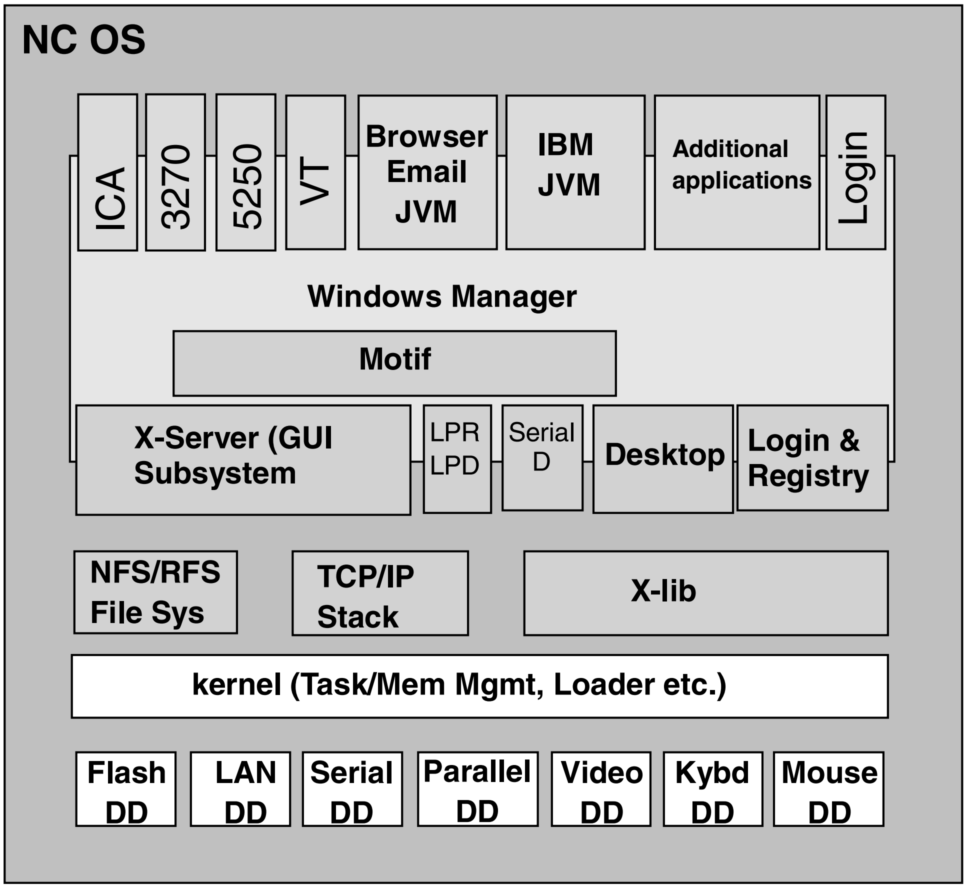


Figure 1. NC OS components

1.2.2 Modernized GUI desktop

Network Station Manager V2R1 provides a new GUI desktop with a more modern look and feel. The graphical user interface is based on the Motif 2.1 industry standard (defined by the IEEE 1295 specification). Motif is used on more than 200 hardware and software platforms. It provides application developers, end users, and systems vendors with the industry's most widely used environment for standardizing application presentation.

The new NC desktop is covered in more detail in Chapter 7, "NC desktop" on page 153.

1.2.3 Netscape Communicator 4.5

Netscape Communicator 4.5 replaces NC Navigator, a Netscape 3.04 derivative, provided in the previous NSM version. Netscape Communicator 4.5 includes the Navigator browser and the Messenger (POP3 e-mail, IMAP e-mail, and news). The browser is compatible with other UNIX versions of Netscape Navigator.

Key features that are new in this version include:

- Dynamic HTML support
- Built-in Netscape JVM 1.1
- Live Connect support
- Java Script 1.3 support
- Java Plug-in
- PDF viewer
- RealPlayer plug-in
- Audio player plug-in
- Video player plug-in

The Netscape Communicator functions are covered in Chapter 12, "Netscape Communicator 4.5" on page 333.

1.2.4 Java

The Java environment in NSM V2R1 is significantly enhanced and now includes the IBM enhanced 1.1.8 JVM. This is a complete JDK, as opposed to the JRE used in previous versions of NSM. For a complete overview of the Network Station Java capabilities, see Chapter 11, "Java environment" on page 305.

1.2.5 Host access enhancements

Several enhancements have been made to the host access applications. The applications are ICA and the 3270, 5250, and VT emulators.

1.2.5.1 ICA

There are two major areas that have been changed in NSM V2R1 to enhance Network Station access to Windows applications running on a Windows NT server: ICA client enhancement and NSM configuration enhancements. The Network Station ICA client is covered in Chapter 14, "Windows application access (ICA)" on page 403.

ICA client enhancement

The ICA client is now based on the Citrix UNIX ICA client code. Citrix UNIX ICA client supports most of the popular UNIX operating systems. IBM has enhanced the Citrix code with some missing features.

The following functions are available:

- Color support: 16 and 256 colors
- Application publishing
- Cut and paste of text
- Print redirection
- Load balancing
- Remote Application Manager
- Client COM Port mapping
- Protocol compression
- Audio support
- License pooling
- Full screen support
- Kiosk mode
- Internationalization
- Secure ICA
- Restart capability
- Metaframe Terminal Edition support
- Support for Citrix Device Services from IBM

NSM configuration enhancements for ICA

In NSM V1Rx, the support for configuring access to Windows NT servers is not nearly as integrated into NSM as most other Network Station applications such as terminal emulators, Web browsers, and Java applications.

In NSM V2R1, the configuration of both ICA and X clients connecting to a Windows NT server is merged under a new section titled Windows-based Applications. A common and highly used set of parameters is available for configuration under this section. Parameters that are not common between the two clients, or low use parameters, are configured under an Additional Parameters input field.

Another new section, ICA Remote Application Manager, allows the administrator to create a list of servers and applications that the users can connect to via ICA.

1.2.5.2 5250 and 3270 emulation enhancements

The 3270 and 5250 emulators are now able to use scalable fonts for improved full screen coverage. SSL support is now included, as is the LU1/3 print support added by PTF to NSM R3. Other minor enhancements have also been made. More information on the 5250 and 3270 emulators can be found in Chapter 13, “Emulators” on page 369.

1.2.5.3 VT

The VT emulator in NSM V2R1 is based on the AIX DTTERM emulator. It supports most functions of the VT emulator in V1R3 and also adds easy keyboard remapping features and improved printing and fonts support. More information on the VTxxx emulator can be found in Chapter 13, “Emulators” on page 369.

1.2.6 eSuite environment

The Lotus eSuite WorkPlace 2.0 for Domino is an easy-to-navigate desktop environment, providing users quick access to productivity applications through a standard Internet browser. WorkPlace R2 is comprised of a set of Java applets, including a word processor, spreadsheet, chart, scheduler, presentation graphics, access to Notes WebMail, and calendaring templates. For the Network Station environment, this means easy access to the eSuite applications through the Netscape Communicator. WorkPlace 2.0 will not be distributed with NSM but may be purchased directly from Lotus.

eSuite has been withdrawn from marketing

After a long evaluation and careful assessment of business priorities, Lotus has decided to realign the marketing and development resources that currently support our eSuite offering. A core eSuite development team will be maintained to provide support for current eSuite customers and to evaluate options for integrating eSuite technologies into the Lotus Domino and Notes platforms, and into IBM WebSphere.

Lotus eSuite is not supported for V2R1 of the Network Station. If you are currently using eSuite with your V1R3 Network Station, visit the Lotus Web site at: `http://www.lotus.com/home.nsf/welcome/esuite1`

1.2.7 Printing enhancements

NSM 2.1 now provides a printer manager for Network Stations to allow a user to monitor and cancel print jobs. NSM V2R1 provides support for PostScript, PCL (emulators only), and ASCII (emulators only). Other printing enhancements include:

- Printing has been enabled for additional ports.
- Multiple copy printing is now available for some applications.
- LPD printing, PostScript, and PCL printing are now available for the VTxxx emulator.
- Serial printer options settings (baud rate, parity, and so on) can now be made in NSM.

More information on the Network Station printing capabilities can be found in Chapter 17, “Printing” on page 555.

1.2.8 Flash boot

The PowerPC-based Network Stations will continue to use the same local boot capabilities as with NSM V1R3, for example, linear flash cards of C or D series. The management of them will not be handled by NSM, but they will still need to be managed by an administrator manually as before.

The new x86-based Network Stations will use a new type of flash cards, the Compact Flash cards. These are the same type of flash cards that are found in other electronic devices on the market, such as digital cameras. Compact Flash cards can be found in sizes ranging from 8 MB and up to 96 MB (as of today). The management of the x86-based Network Stations flash cards will be handled by NSM through a Java applet. It will be able to automatically build the flash cards from predefined sets of files, the so called Bill Of Materials.

Both PowerPC-based and x86-based Network Stations continue to support the concept of separation-of-servers (split boot), which enables them to load the operating system-files (that are stable and rarely changes) from a local flash card while retrieving the configuration files from a central location. This allows for good booting performance, while maintaining a central point of management.

Both types of Network Stations will still support peer-booting from flash cards, for example, one Network Station equipped with a flash card can act as a boot server for a number of other Network Stations.

1.2.9 NLS and euro support

The following languages won’t be supported with the first release of NSM V2R1:

Japanese
Korean
Simplified Chinese
Traditional Chinese
Thai
Arabic
Czech
Greek
Hebrew
Hungarian
Polish
Russian
Cyrillic
Turkish
Vietnamese
Laotian

Albanian
Bulgarian
Belorussian
Catalan
Croatian
Estonian
Latvian
Lithuanian
Macedonien
Romanian
Serbian-Cyrillic
Serbian-Latin
Slovakian
Slovenian
Ukranian
Icelandic

1.2.10 Hi-color support

Hi-color support refers to the support of a 16-bit color palette (for 65536 colors) for the applications and NC OS. This section explains what the solution was for Version 1 and now with Version 2 of the NSM.

1.2.10.1 NSM Version 1

The operating system used in Network Station Manager V1Rx only supports a common 8-bit color palette (256 colors) for the applications and NCDi OS. It turns out that many times, when several Network Station applications are simultaneously active, and the total number of registered colors exceeds 256, “false colors” appears.

An 8-bit pseudo color palette, the “Web palette”, is used on the Network Station to limit the color “flash” problem. The Web color palette is a de facto standard which defines a set of 216 invariant colors creating a usable spectrum covering the full range of red, green, and blue values. Applications that restrict their allocation of colors to these values will be assured of their availability. The colors are shared among the applications and are not private.

1.2.10.2 NSM Version 2

The new Network Station Manager version supports a common 16-bit color palette (65536 colors) for the applications and NC OS. This is usually referred to as Hi-color support.

The hardware of the S1000 and S2800 models are capable of supporting 8, 16, and 24 bit color depths. However, the hardware of the S300 cannot support more than 256 colors and, therefore, cannot benefit from the new 16-bit color palette.

All local applications (JVM, Netscape Communicator, and so on) launched from a Network Station S1000 or S2800, will operate with hi-color. The color “flash” problem encountered with the previous NSM version will not display anymore.

However, the current 8-bit pseudo color palette API and user interface is preserved within all platforms. This allows the continued support of the S300 and preserves compatibility with external 8-bit X-windows applications.

Once a color-depth operational mode is active, mixed modes of operation won’t be supported. All clients must be capable of 8- or 16-bit color depths.

1.3 NSM V2R1 hardware support

Three IBM Network Station models were available until now: the Series 100, the Series 300, and the Series 1000. All of these models are based on a PowerPC CPU architecture. These models will remain unchanged.

Two new Network Station models are now also available: the Series 2200 and the Series 2800. These models are based on an Intel x86 CPU architecture.

Network Station Manager V2R1 will support the Series 300 (except the Twinax model), the Series 1000, the new Series 2200 and Series 2800. V2R1 support for the Series 1000 was added in mid-November of 1999. The planned date for V2R1 NSM Series 300 support is the during the first quarter of 2000. Details of the hardware features of these machines and their capabilities are covered thoroughly in 3.2, “Network Station hardware components” on page 36.

1.3.1 Peripheral devices and connection support

Hardware features and peripherals currently supported by NSM V1R3 on the Series 300 and Series 1000 models will continue to be supported by NSM V2R1. In addition, new peripheral devices will be supported. They will attach to the Network Station via the PCMCIA slot (for PowerPC), the PCI slot (for x86) or the serial port of either platform models.

Both PowerPC and x86 platforms will support the attachment of a multi-port serial device, a touch-screen device and a lightpen device. The exception is the Model 2200, which did not support a touch-screen or a lightpen device at the time of this writing. For setup and configuration information regarding the touch-screen support, see 3.2.6.7, “Touch-screen support” on page 44.

The PowerPC platforms will continue to support C and D series linear flash cards (PCMCIA slot) and the x86 platforms will support ATA compact flash cards (internal socket) for booting via flash card.

NSM V2R1 provides Java communication APIs (packaged as javax.comm) for device driver development.

1.3.1.1 Series 2800 device attachment

The Series 2800 is only supported by NSM V2R1. Figure 2 shows a detailed view of the device connectivity for the Series 2800.

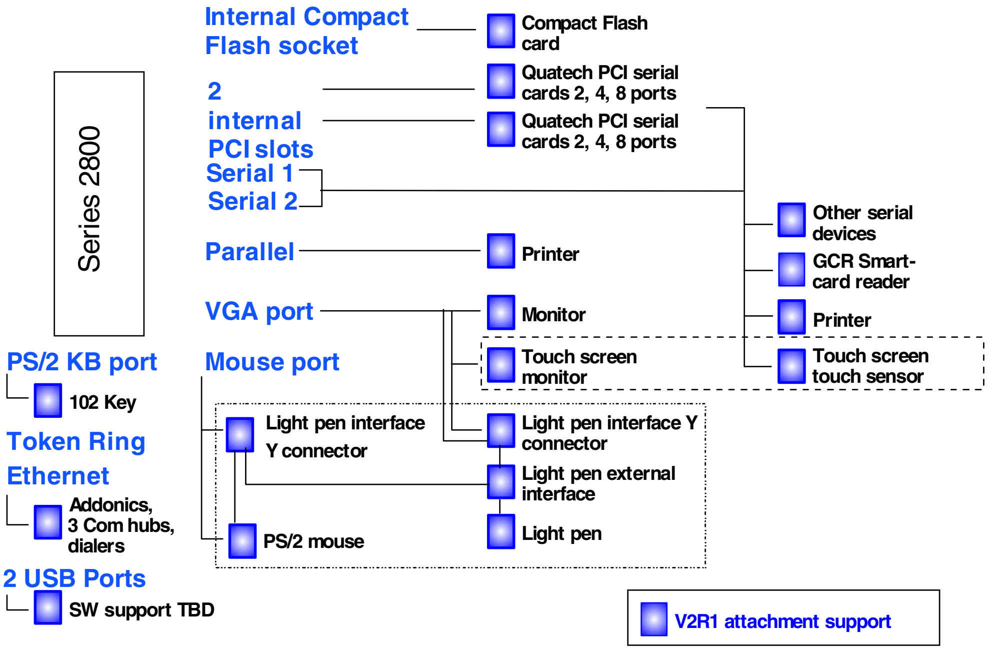


Figure 2. Series 2800 device attachment

Although the Series 2800 has two USB ports, software support has not been included with NSM V2R1. We anticipate that the software support will be provided at a future date.

Smart card support is provided through the Java communication API. The GCR410 reader connects to the serial port.

1.3.1.2 Series 2200 device attachment

The Series 2200 is only supported by NSM V2R1. Figure 3 shows a detailed view of the device connectivity for the Series 2200.

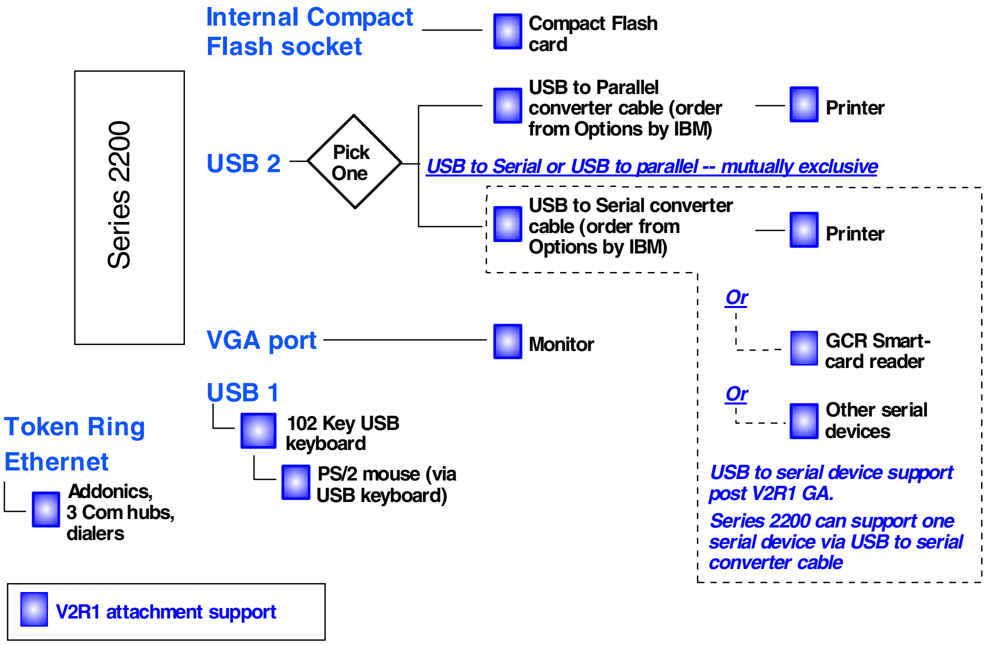

Series 2200
Internal Compact Flash socket
Compact Flash card
USB 2
Pick One
USB to Parallel converter cable (order from Options by IBM)
Printer
USB to Serial or USB to parallel -- mutually exclusive
USB to Serial converter cable (order from Options by IBM)
Printer
Or
GCR Smart-card reader
Or
Other serial devices
USB to serial device support post V2R1 GA.
Series 2200 can support one serial device via USB to serial converter cable
VGA port
Monitor
USB 1
102 Key USB keyboard
PS/2 mouse (via USB keyboard)
Token Ring
Ethernet
Addonics, 3 Com hubs, dialers
V2R1 attachment support

Figure 3. Series 2200 device attachment

The universal serial bus (USB) is an emerging serial interface standard for telephony and multimedia devices. Each USB port is a single connector for devices that previously used serial, parallel, keyboard, mouse and game ports. USB uses Plug and Play to determine which type of device has been attached to the connector. The 2200 does provide USB support for the 102 USB keyboard and PS/2 mouse via the USB keyboard. It also provides USB to parallel converter cable support. It is anticipated that USB to serial support will be announced at a later date.

Smart card support is provided through the Java communication API. The GCR410 reader connects to the serial port.

1.3.1.3 Series 1000 device attachment

NSM V2R1 provides support for the Series 1000, including the previously supported device attachments. In addition, NSM V2R1 will provide support for GCR Smart Card reader (serial port), internal Smartcard reader, and touch-screen touch sensor (Figure 4 on page 12).

Smart card support is provided through the javax.comm interface.

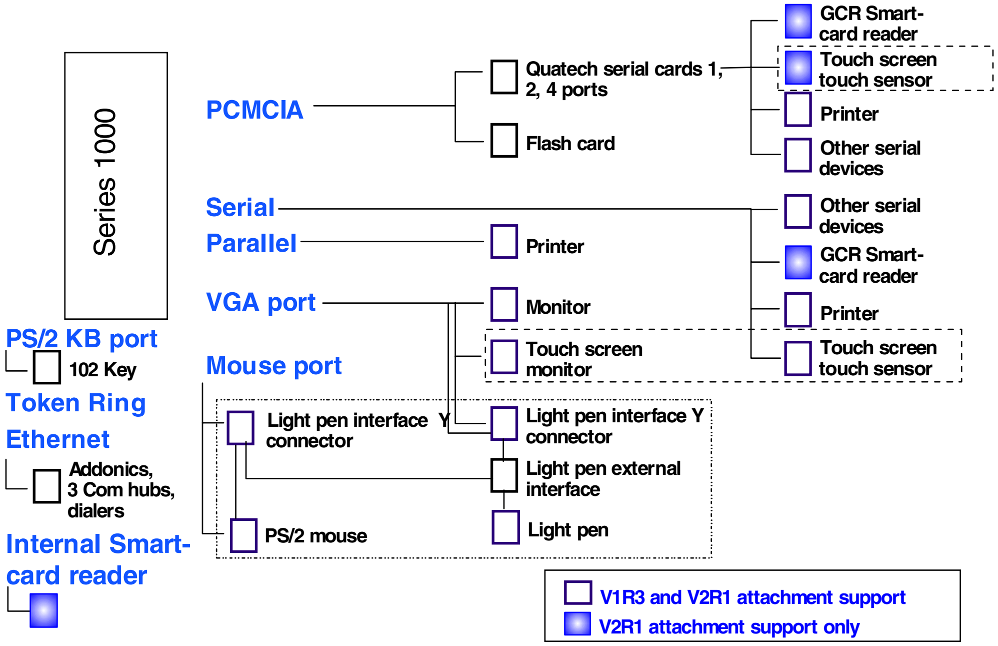

Series 1000
PCMCIA
Quatech serial cards 1, 2, 4 ports
Flash card
GCR Smart-card reader
Touch screen touch sensor
Printer
Other serial devices
Serial
Parallel
Printer
Other serial devices
GCR Smart-card reader
Printer
VGA port
Monitor
Touch screen monitor
Touch screen touch sensor
PS/2 KB port
102 Key
Mouse port
Token Ring
Ethernet
Addonics, 3 Com hubs, dialers
Light pen interface Y connector
Light pen interface Y connector
Light pen external interface
PS/2 mouse
Light pen
Internal Smart-card reader
V1R3 and V2R1 attachment support
V2R1 attachment support only

Figure 4. Series 1000 device attachment

1.3.1.4 Series 300 device attachment

NSM V2R1 will provide support for the Series 300 (with the exception of the Twinax model), including the previously supported device attachments. The planned date for V2R1 NSM Series 300 support is the during the first quarter of 2000. In addition, NSM V2R1 will provide support for the GCR Smart Card reader and the touch-screen touch sensor (Figure 5).

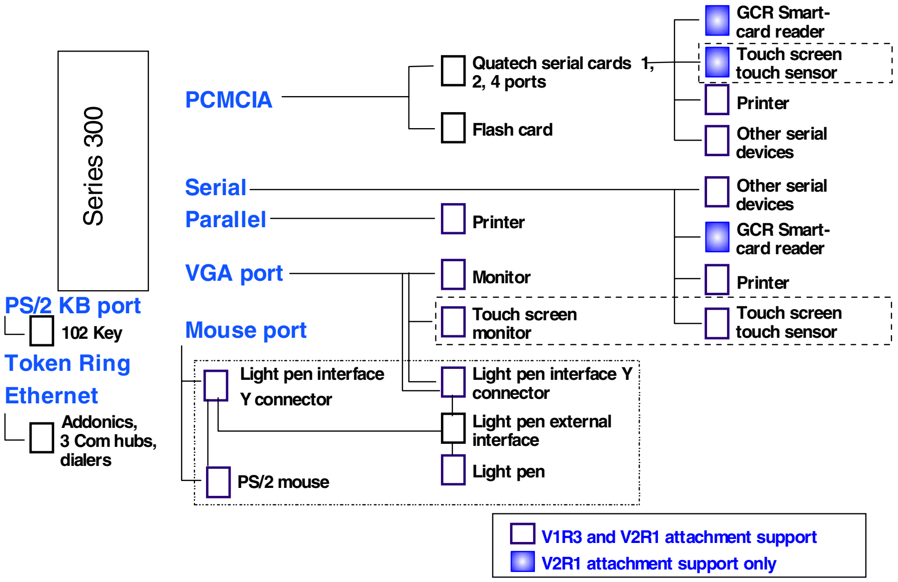

Series 300
PCMCIA
Quatech serial cards 1, 2, 4 ports
Flash card
GCR Smart-card reader
Touch screen touch sensor
Printer
Other serial devices
Serial
Parallel
Printer
Other serial devices
GCR Smart-card reader
Printer
VGA port
Monitor
Touch screen monitor
Touch screen touch sensor
PS/2 KB port
102 Key
Mouse port
Token Ring
Ethernet
Addonics, 3 Com hubs, dialers
Light pen interface Y connector
Light pen interface Y connector
Light pen external interface
PS/2 mouse
Light pen
V1R3 and V2R1 attachment support
V2R1 attachment support only

Figure 5. Series 300 device attachment

Smart card support is provided through the javax.comm interface for GCR410 readers attached to the serial port.

Chapter 2. Network Station architecture

This chapter introduces you to the IBM Network Station by providing you first with a high-level perspective of the overall Network Station environment. You will gain an understanding of the different hardware and software components involved and how they are architected to interact with each other to provide a network computing environment.

This chapter also brings to your attention many of the design issues and decisions that need to be made when planning and implementing a network of IBM Network Stations. We only provide a glimpse of those issues in this section because we want to focus mainly on your understanding of the overall picture before getting into more technical details. Chapter 3, “Planning and design issues and choices” on page 35, provides additional details on the design issues and choices that we only briefly highlight in this chapter.

In the following text, we gradually build a particular diagram by adding pieces to it until we get a complete picture. This allows us to focus only on certain pieces at a time and to simplify the explanations that lead to a complete diagram.

2.1 Network Station hardware components

The first piece of the puzzle is the IBM Network Station. First, we need to understand what an IBM Network Station is, especially for those for whom this might be their first exposure to network computers, or thin clients to which they are sometimes referred. The best way to do this is to examine the components that make up an IBM Network Station or any network computer for that matter.

2.1.1 Network Station core components

Figure 6 shows the core components of Network Station.

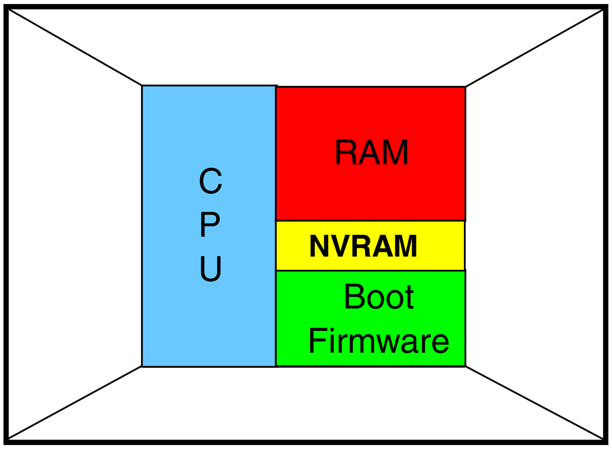


Figure 6. Network Station hardware components: Core components

The core components are:

- **A Central Processing Unit**

  With the currently available models of the Network Station, the processors range from a Power PC 403 66 MHz engine (Series 300) to an x86 based

MMX 266 MHz (Series 2800). This range allows a selection based on the type and number of applications that need to be executed on a particular station. For details on the types of processors, see the specific hardware section.

- **Random Access Memory**

  Part of this memory is non-volatile (NVRAM) to allow certain pieces of data to remain permanently between power off and power on of the station. The rest of the memory is traditional RAM holding the operating system, applications and data, which must be reloaded after a power off. Note that this is a real memory system and there is no paging into virtual memory on disk.

- **Boot Firmware**

  This firmware is code that is given control after a power on, it is responsible for performing power on self tests as well as initiating the sequence of events that are required for the station to contact a server on the network and download its operating system.

2.1.2 Network interfaces

The next required component is a network interface card that allows the station to communicate with other hosts on the network, in particular with a server to download its operational code (Figure 7). This adapter can be either an Ethernet adapter or a Token-Ring adapter.

During the power-on sequence, as soon as the self diagnostics tests are completed, the adapter is opened for the station to communicate on the network and contact one or more servers. We discuss the nature and role of these servers in a moment.

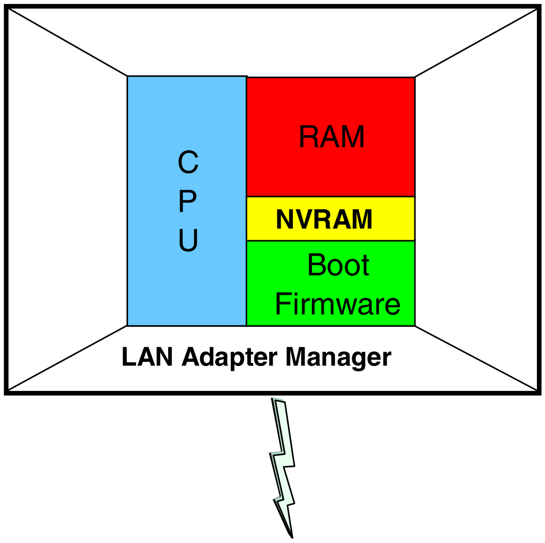


Figure 7. Network Station hardware components: Network adapter

2.1.3 Monitor and video support

The next component is the display monitor (Figure 8). A variety of monitors are supported in different video modes and resolutions. A window manager software component manages windows displayed by the different applications operating on the Network Station.

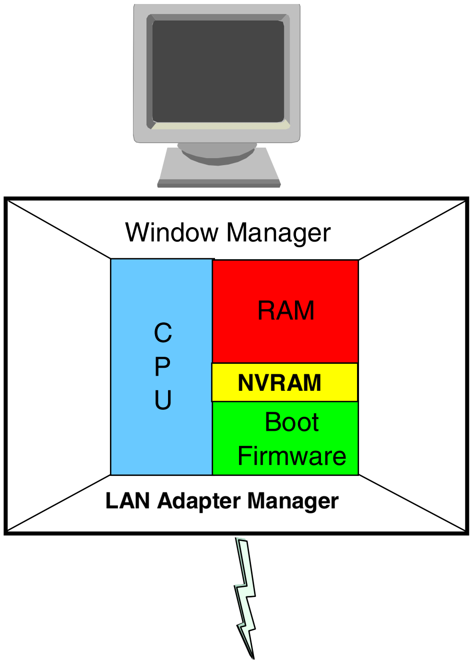


Figure 8. Network Station hardware components: Monitor

2.1.4 Keyboard and mouse

Next is the support for keyboard and mouse input (Figure 9 on page 16). The keyboard is a standard 102-key PC keyboard, which is available in different language configurations, and a two-button mouse.

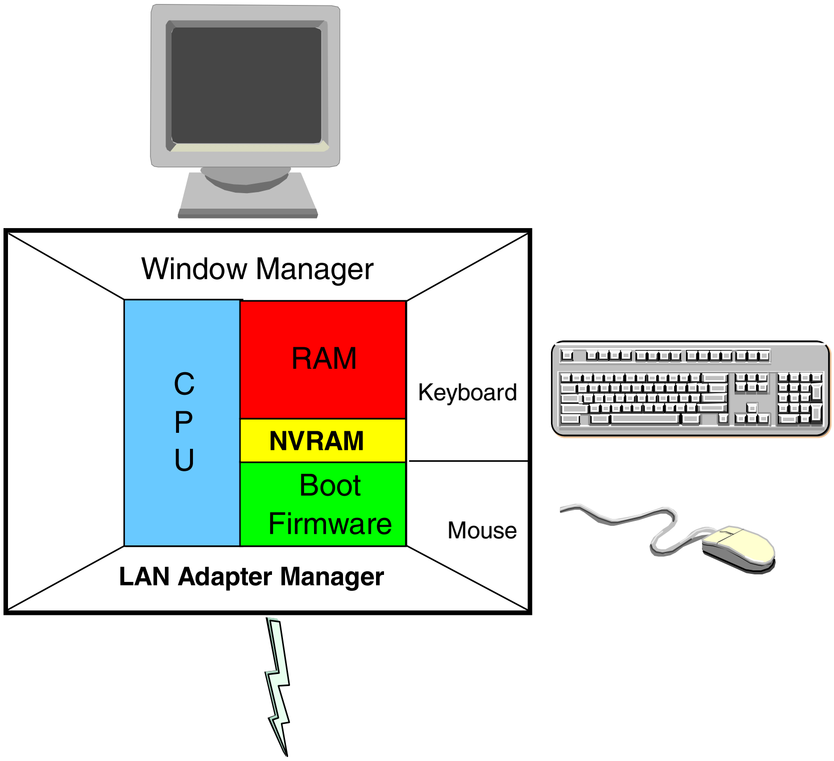


Figure 9. Network Station hardware components: Keyboard and mouse

2.1.5 Input/output ports and devices

Finally, there are a variety of I/O ports and devices available that depend on the different models. For example, consider these scenarios:

- All models have some form of audio support, ranging from an 8-bit mono integrated speaker to a 16-bit stereo jack on the latest models.
- All models have at a minimum one serial port and one parallel port. The serial port can be used to attach a serial printer or communication device. The parallel port typically is used to attach a parallel printer. The exception is the Series 2200, which has two of the new USB ports.
- Some models allow the use of a Smart Card, while others support a PCMCIA Type II adapter or PCI adapters.
- Some of the latest models also provide a Universal Serial Bus(USB) port capability that allows for easy expansion of I/O devices connectivity. Both the Series 2200 and 2800 have USB ports. However, at the time of this writing, the Series 2800 has not enabled the ports in software.
- All models also allow the use of flash memory cards to provide a limited local storage capability, mostly for implementing local boot capabilities.

We take a more detailed look at the availability of these devices, for each model, in Chapter 3, “Planning and design issues and choices” on page 35.

This completes a quick tour, on the hardware side, of a typical Network Station. Figure 10 shows the I/O parts and devices, along with all the hardware requirements.

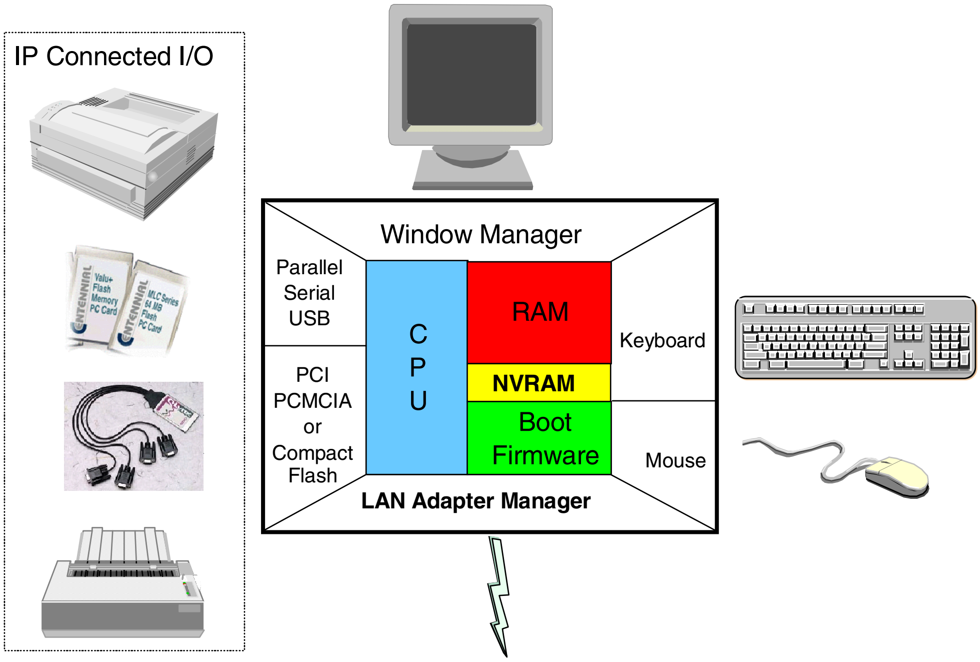
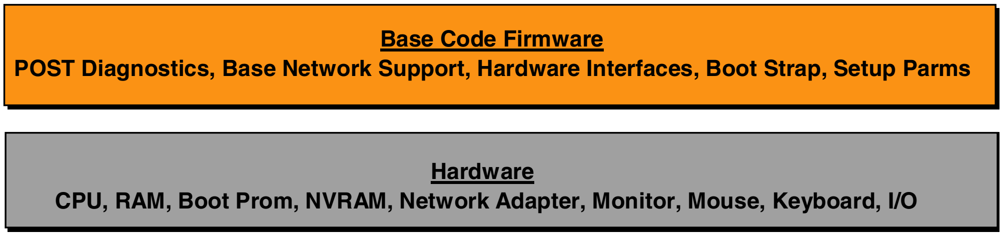


Figure 10. Network Station hardware components: I/O devices

2.2 Network Station software components

We now examine the software components that reside on a Network Station and that are necessary to the operation of the Network Station. The base components, as illustrated in Figure 11, form the first layer above the hardware components. These base components include the diagnostics routines, such as those performed during the Power On Self Tests (POST) when the user powers on the station.



Base Code Firmware
POST Diagnostics, Base Network Support, Hardware Interfaces, Boot Strap, Setup Parms

Hardware
CPU, RAM, Boot Prom, NVRAM, Network Adapter, Monitor, Mouse, Keyboard, I/O

Figure 11. Network Station base components

Most importantly, the base components include the firmware, which is code permanently resides on the station on a Programmable Read Only Memory (PROM) chip. It is given control after the POST completes and then performs the steps necessary to boot the Network Station. This code is called the *boot monitor*.

The boot monitor is the component responsible for booting the Network Station. It determines how it is going to behave and how it is going to initiate the boot process by reading some of the configuration data that is permanently recorded in the Network Station's NVRAM.

With this information, the boot monitor can contact a boot server on the network and download the operating system required by the particular model of the Network Station on which the boot monitor resides.

The boot monitor can be easily replaced, when new features or functions become available, by downloading a new version from a remote server and replacing the current one recorded in the PROM. This process is called *reflashing the PROM*.

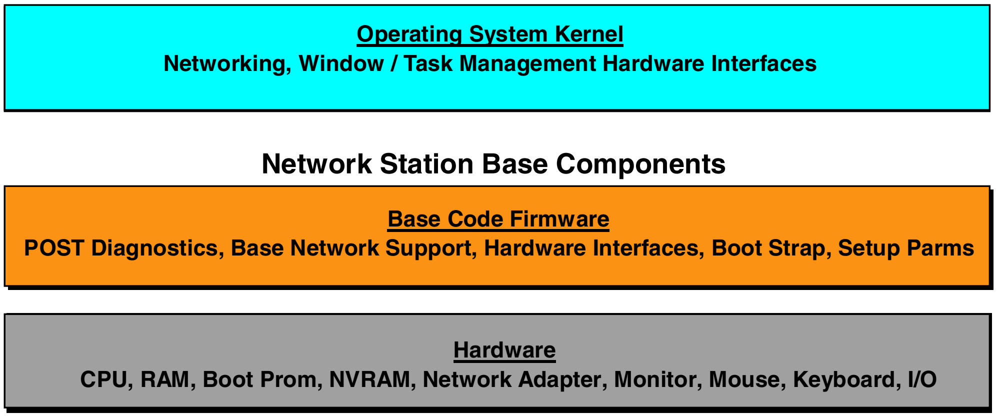

Operating System Kernel
Networking, Window / Task Management Hardware Interfaces
Network Station Base Components
Base Code Firmware
POST Diagnostics, Base Network Support, Hardware Interfaces, Boot Strap, Setup Parms
Hardware
CPU, RAM, Boot Prom, NVRAM, Network Adapter, Monitor, Mouse, Keyboard, I/O

Figure 12. Network Station's operating system

The operating system is a Berkely Software Distribution (BSD) UNIX-like software and can be seen at a high level in Figure 12. It is available in two ways:

- Prior to V2R1, the kernel was supplied by NCD inc. and was designed to run on Power PC engines.
- With V2R1, the kernel is supplied by Liberate (you will notice their copyright during the boot process) and is designed to operate on both a Power PC engine (except the Series 100) or on an x86 engine as available in the new Series 2800 and Series 2200.

Apart from being able to operate on both types of CPUs, the V2R1 kernel also has thread support and pre-emptive multitasking, which should prevent an application from causing a Please Alert Nearest Incident Center (PANIC).

It is important to remember as well that the kernel uses a linear memory model, which means that all applications use real memory and that there is no virtual memory or memory swapping. This is mainly because there is no local storage facility in the Network Station can be used for swapping memory. However, network paging is enabled in V2R1 so that code can be paged over the network. The memory manager can reuse read-only pages and re-read the executable as necessary from the boot server. A practical example of this is the help information related to the 5250 emulator that would only be paged to the Network Station from the boot server when needed.

Adding more memory to a Network Station increases the total number of local applications that can be run simultaneously, but not the performance. In low memory conditions, applications may not be loaded by the kernel. In critical low memory conditions, the kernel may close applications to free memory as a last resort.

Once the operating system is loaded, it passes control to a login routine responsible for getting the user’s name and password, authenticating that user with a remote server, and then loading the user’s preferences and applications. Some of these applications can be started automatically or they can be loaded started on request by the user.

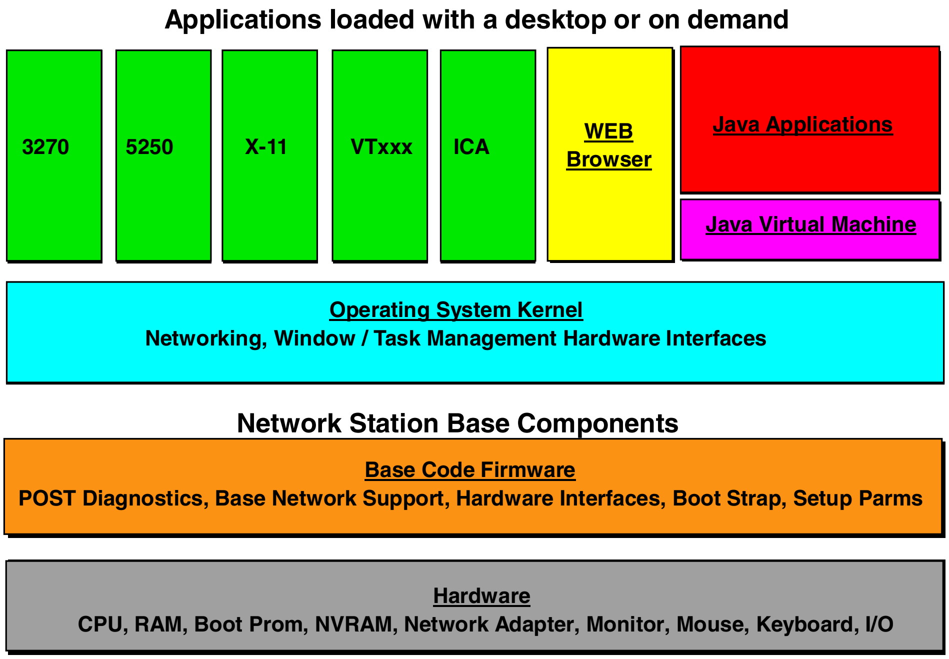

Applications loaded with a desktop or on demand
3270
5250
X-11
VTxxx
ICA
WEB Browser
Java Applications
Java Virtual Machine
Operating System Kernel
Networking, Window / Task Management Hardware Interfaces
Network Station Base Components
Base Code Firmware
POST Diagnostics, Base Network Support, Hardware Interfaces, Boot Strap, Setup Parms
Hardware
CPU, RAM, Boot Prom, NVRAM, Network Adapter, Monitor, Mouse, Keyboard, I/O

Figure 13. Network Station applications

The native applications available to the user are either host access applications, browser for Web access, or Java applications. The applications available for host access are shown in relationship to the operating system in Figure 13. They include:

- A 3270 emulator
- A 5250 emulator
- An X windows terminal capability to access a AIX or UNIX system as well as a multi-user Windows NT system using the X11 protocol
- A VTxxx emulator
- An ICA client to access a WinFrame or MetaFrame server (multi-user WIndows NT) using the ICA protocol.

For access to the Web, the Web browser is based on Netscape Navigator 4.5.

Most Java applications or applets, either home grown or available on the market, can be executed on the Network Station’s JVM running version 1.1.8.

In summary, note that once the Network Station is powered off, all software loaded in memory disappears, and must be reloaded after the next power on. Only the firmware necessary to reboot the Network Station remains.

You must remember that one of the main advantages of a thin client is that since the software only resides on the server, individual copies of the software do not need to be maintained and updated on every station. Every time a station loads either the kernel or an application, it is an opportunity to get a fresh updated copy of the software since it only needs to be updated on the server in order to be propagated to all stations.

2.3 The boot process architecture

We now continue onto the next major topic: the *boot process*.

We define the boot process as all the activities that must take place between the time that the user powers on Network Station and the time where the user is able to load an application to do useful work. When broken down into the individual events, there is a significant number of activities that must take place as part of the boot process. We use a step-by-step approach to identify each of the important steps, gradually building a diagram that summarizes all the major steps.

In this particular section, we remain on a fairly high level and avoid unnecessary details to concentrate mainly on understanding the overall architecture of the boot process.

Once you master the overall concepts involved, the step-by-step description of the boot process is repeated in the next section. This section also provides additional detailed information on each of the steps involved.

2.3.1 Inserting into the network

Let's start with Figure 14, where we see a Network Station that we attach to an IP LAN network.

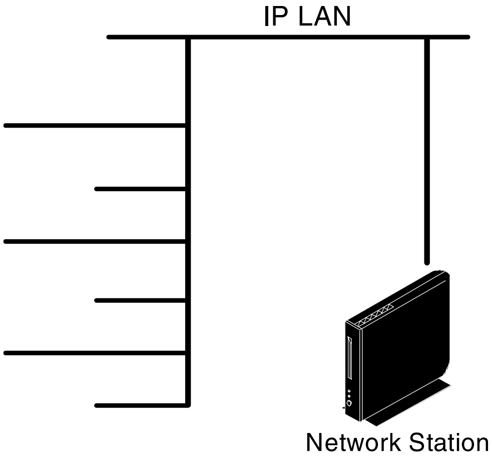


Figure 14. Boot process: IP LAN network

It does not matter at this point whether this is on a local area network (LAN) or Wide Area Network (WAN), or how the network is actually configured. The concept is the same so we leave the details of the network design for the next chapter.

The important point to remember is that the Network Station only supports TCP/IP. It does not support NetBIOS, IPX, or any other network protocol so it must be attached to an IP network.

After the station is powered on and has executed the POST tests, the boot monitor, stored in the station's PROM chip, effectively controls the initiation of the boot process, and opens the network interface adapter to insert itself into the network. It uses the Media Access Control (MAC) LAN address that was stored in the non-volatile memory (NVRAM), along with data such as keyboard layout and screen resolution. From this point on, this station can identify itself uniquely on the network by using its MAC address.

2.3.2 Obtaining an IP address

The Network Station functions as an IP host. Therefore, to communicate with other IP hosts, it needs to have an IP address of its own.

The IP address that the station must use to communicate on the network can be obtained in one of three ways:

- The IP address is manually entered into the Network Station's NVRAM by an administrator, using the Setup utility (which is the interactive interface of the boot monitor on the station).
- It can request and obtain an IP address from a BOOTP server.
- It can request and obtain an IP address from a DHCP server.

For this example, we use the DHCP server method (Figure 15), which is the recommended method. Section 3.4.2, "Obtaining an IP address" on page 49, discusses the advantages and disadvantages of each of these methods.

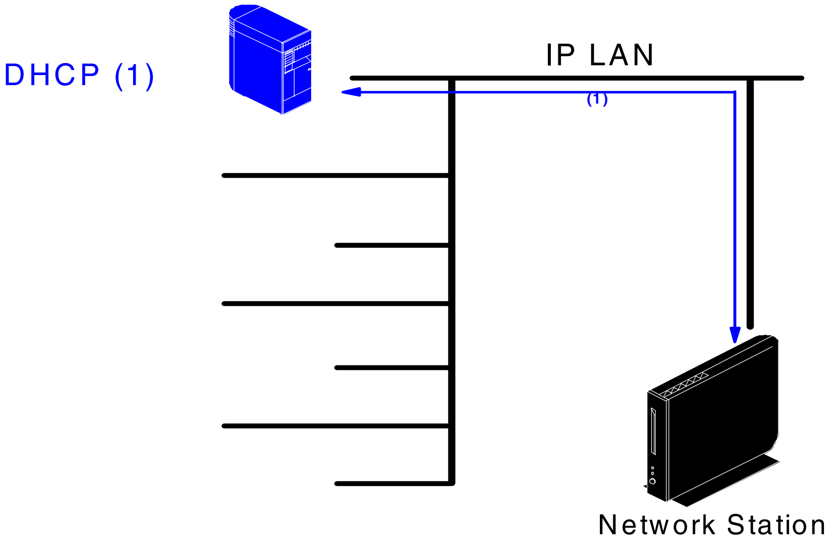


Figure 15. BOOT process: Contacting a DHCP server

To obtain an IP address from a DHCP server, the boot monitor on the Network Station issues a broadcast (that's the only thing it can really do at this point since it does not yet have or own an IP address) on the network. It asks any DHCP server that is listening to respond by sending an IP address that it can use.

Contained in this broadcast frame is the station’s MAC address, which allows the station to uniquely identify itself to DHCP servers.

Note

This process of requesting an IP address from a DHCP server is not something specific to the Network Station. It applies to any IP host in the network that has the ability to dynamically obtain an IP address.

On receipt of this broadcast, one (or possibly more than one) DHCP server on the network responds by allocating an IP address that the station is allowed to use for a specified period of time. Note that the server can specifically recognize the station by its MAC address (if this MAC address has been specifically defined in the server) or it can choose to respond to requests originating from any MAC address.

Along with an IP address, the DHCP server can also send other vital pieces of information such as the address of a boot server that the station should contact to obtain its operating system, and the path to the directory where the operating system file can be found, and a few other pieces of configuration data. We examine this in more detail in 5.5.2, “DHCP configuration” on page 134.

2.3.3 Obtaining an operating system

Now that the station has its own IP address, it becomes a recognized citizen on the network and has the ability to communicate directly with any other IP host on the network. The next important task is to obtain a copy of the operating system that it requires to operate.

There are two ways to obtain its operating system:

- The station contacts a designated boot server on the network from which it downloads a copy of the operating system. This is the example we use here since it is the most common case.

  A boot server may be located on the same physical local area network segment as the station, or it can be located across a wide area network. These are network design considerations that we discuss in 3.4, “The boot process” on page 45, along with the use of multiple boot servers for redundancy and load balancing.

- If the station is equipped with a flash memory card, it can be configured to load its operating system directly from this local storage device. This is a special case that we examine in Chapter 6, “Flash card management” on page 143.

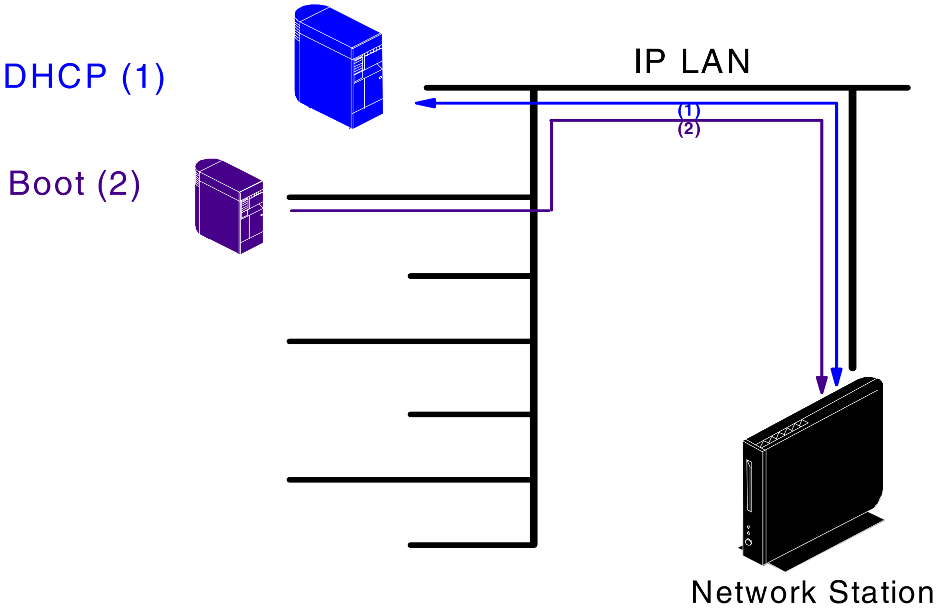


Figure 16. Boot process: Contacting a boot server

Using the address of a boot server that was obtained from the DHCP server, the station contacts the designated boot server (Figure 16) and downloads a copy of its operating system. Unlike Version 1 Release 3, the operating system (which we will call the kernel from now on) in Version 2 Release 1 is downloaded in a non-compressed format and, therefore, does not require decompression after the station receives it.

Typically, a V1R3 kernel file is about 4.2 MB (2.4 MB when compressed) and the V2R1 kernel for the Series 2800 and 2200 is approximately 1.2 MB. Also, note that the kernel in V2R1 is not compressed.

After the kernel file has been downloaded (and uncompressed if using V1R3) by the boot monitor code, control passes to the operating system for the remainder of the operations.

2.3.4 Obtaining system configuration files

The next task in the boot process is for the operating system to set up the proper operational environment for this particular station. To accomplish that, the operating system must obtain system configuration data.

System configuration data consists of:

- **Terminal specific configuration data**: These are the configuration parameters that apply to a specific hardware terminal. Examples of such items are:
  - Does this specific station have a printer attached?
  - What language is to be used during the boot sequence?
- **System defaults**: These are the configuration parameters that apply to all users. Examples of such items can be:

- – Is the mouse defined as right-handed or left-handed for all users?
- – What is the background color of the screen?
- – What is the screen saver background bitmap?

This system configuration data is obtained from a configuration server as shown in Figure 17. In this particular description, we show this configuration server to be a separate physical server, but it does not necessarily have to be that way. It could be on the same server as the boot server, for example. However, because we are focusing more on the concepts here than on the actual implementation, we use separate servers.

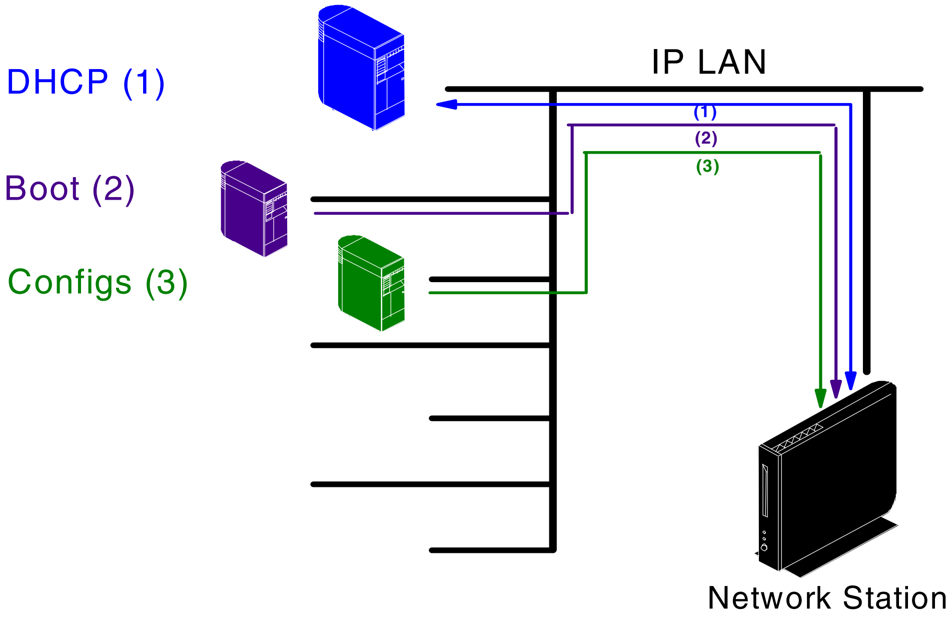


Figure 17. Boot process: Contacting a configuration server

How does the kernel know the address of the configuration server where the configuration files are stored? This address is supplied to the Network Station either as one of the pieces of information returned by the DHCP server, or as a manually configured parameter using the setup utility of the Network Station to enter the data in NVRAM.

The kernel contacts the assigned configuration server and downloads the system configuration files. Some of the parameters considered as system defaults may be overridden later on by additional configuration files that apply to a group or a specific user.

2.3.5 Authenticating a user

The next major step in the boot process is to identify the user that will use the Network Station. The kernel gives control to a login client routine, which displays a panel to the user asking for a user name and password.

After the user enters the data, the login client contacts an authentication server to validate the identity of the user and that the correct password is used.

How does the login client know the address of the authentication server? There are three possibilities:

- Unless it is specifically identified, the default authentication server is the same server as the boot server.
- The address of the authentication server has been specified in the DHCP data (or manually configured in NVRAM).
- The user has used the ROAM button on the login panel to manually enter the address of a specific authentication server. This is used in cases where a user has travelled to a different location and needs to be authenticated by a server back home.

The login client contacts the login server on the authentication server (Figure 18), and verifies that this user is defined and has used the correct password.

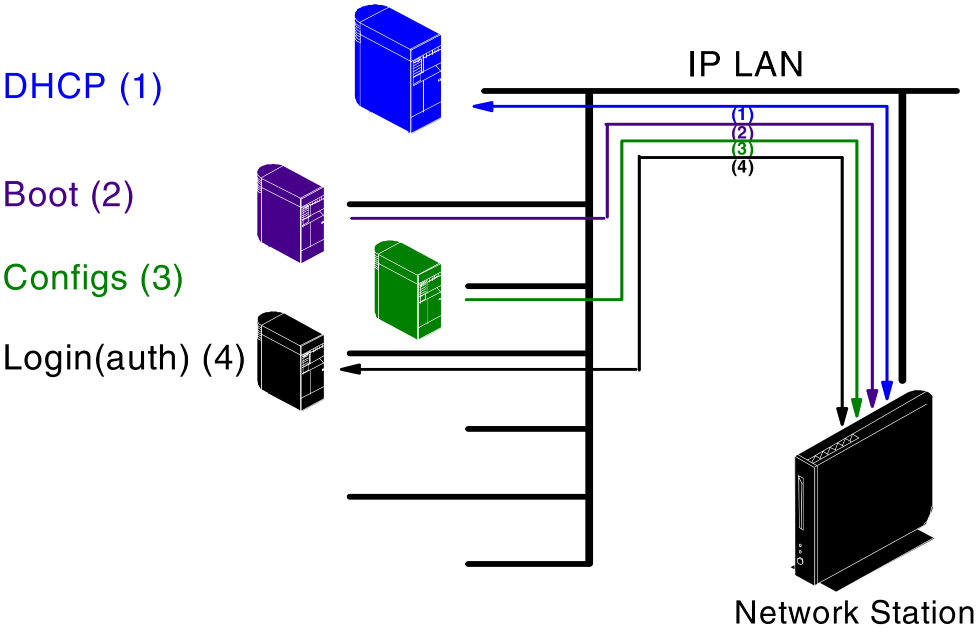


Figure 18. Boot process: Contacting an authentication server

Once the user has been authenticated, the kernel now knows the user and the group it belongs to and is, therefore, in a position to download additional configuration files that are specific to this group and this user.

These configuration files are called the preferences (configuration data) because they represent the specific user preferences, such as a left-handed mouse when the system default is right-handed, or a particular set of colors for the desktop, and so on.

2.3.6 Obtaining user preferences

Therefore, the next step is to download these preferences from a preferences server as shown in Figure 19 on page 26.

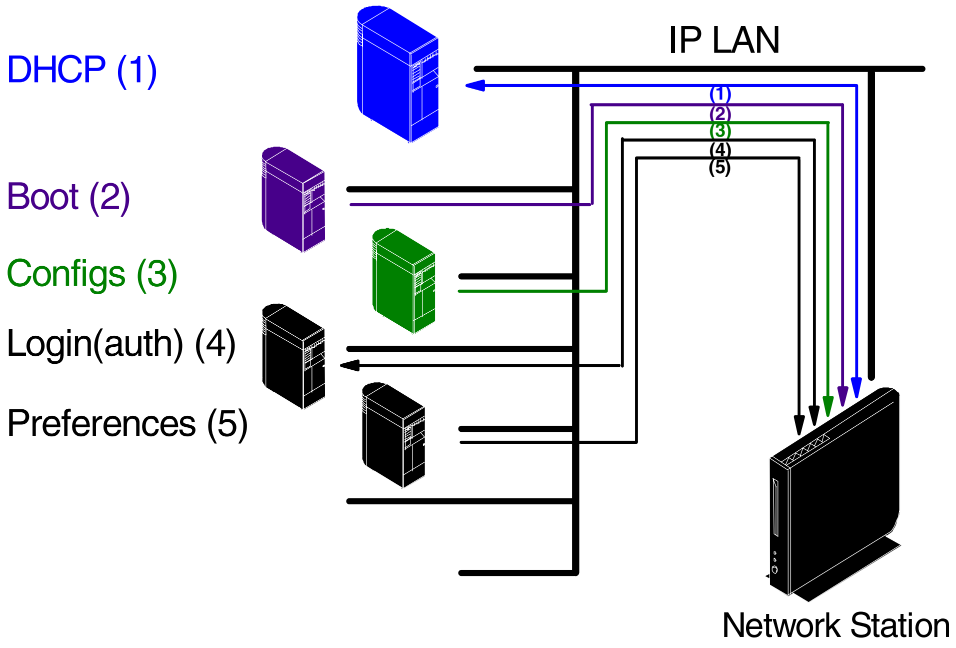


Figure 19. Boot process: Contacting a preferences server

In the current versions of the product (V1R3 and V2R1), the preferences server is always the same as the authentication server. However, this can be changed through a manual alteration of one of the configuration files.

The kernel fetches the preferences configuration files based on the user name and group name, and overrides the system default parameters for those parameters contained in the preferences files. The preferences files also contain the information necessary to identify the applications that are to be autostarted based on the user profile and the setup of the desktop and the applications to be made available to the user.

2.3.7 Downloading native applications

The next step is to load the applications that are specified as autostarted, or to load applications on request when the user clicks on a specific icon on the desktop to start an application.

The native applications, such as the emulators, or any Java application or applets are modules that need to be downloaded from a server as shown in Figure 20. In this version of the product, the native applications server is, by default, the same as the boot server and cannot be specified otherwise.

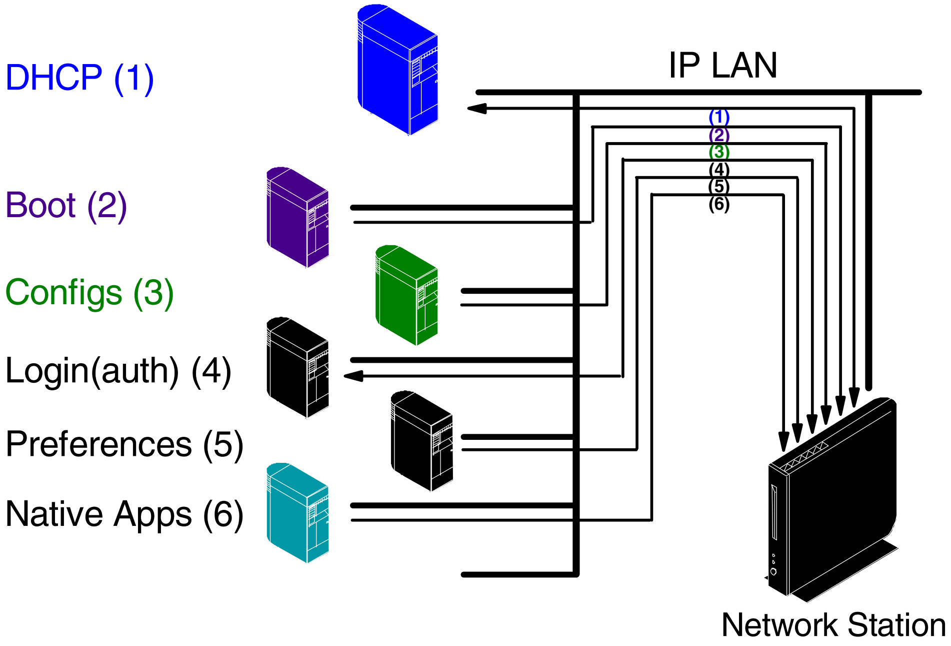


Figure 20. Boot process: Contacting a native application server

However, logically the native application server can be located on a different server altogether.

The applications modules requested are downloaded, loaded into the Network Station memory, and given control.

2.3.8 Using a home server

Some of the native applications allow the user to set applications preferences, such as emulator colors for example, or, in the case of a browser, to save bookmarks. Because there is no local storage on the Network Station where these application preferences can be stored, each user is given a home directory on a server where these can be stored.

This server is called the *home server* (Figure 21 on page 28) and, at this point, is the same server as the authentication server.

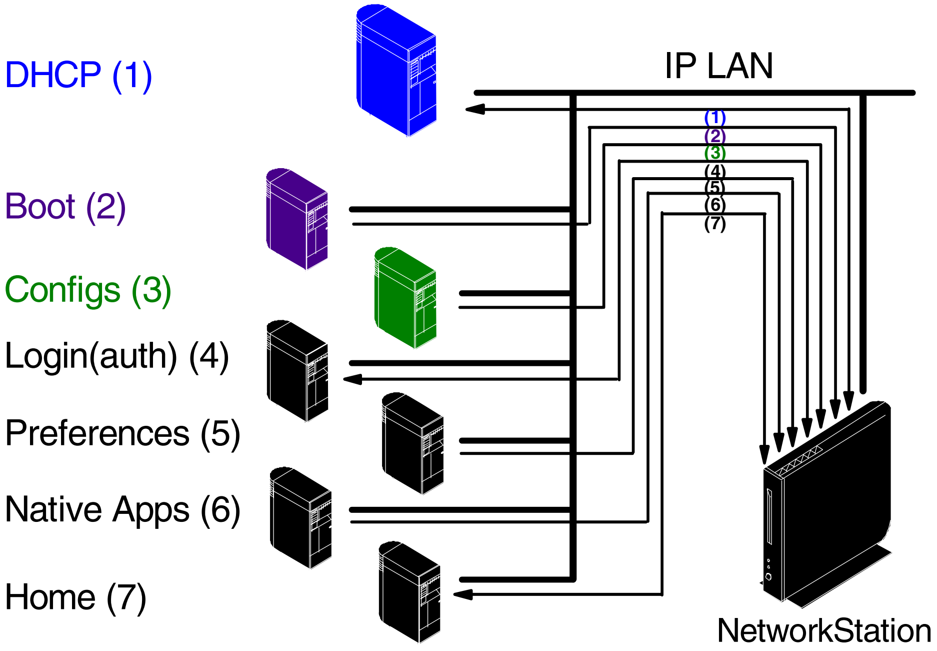


Figure 21. Boot process: Contacting a home server

The home directory on the home server is automatically allocated to each user that logs on without the user having to take any specific steps for that to happen.

If the user has some home grown local Java applications that they need to use, and these applications require some local storage, the home server can serve as the target server for these files. However, this is not mandatory because any remote server can be designated as a file server and accessed by local applications.

2.3.9 Contacting application servers

At this point, the boot process is essentially completed and the user has full control of their desktop.

As the user starts different applications, it is likely that they will access one or more application servers. For example, using a 3270 emulator will cause the user to contact a S/390 server, using a 5250 emulator means accessing an AS/400 server, using an ICA client means accessing a MetaFrame server, and using a Web Browser will give them access to the Web. An example of this is shown in Figure 22.

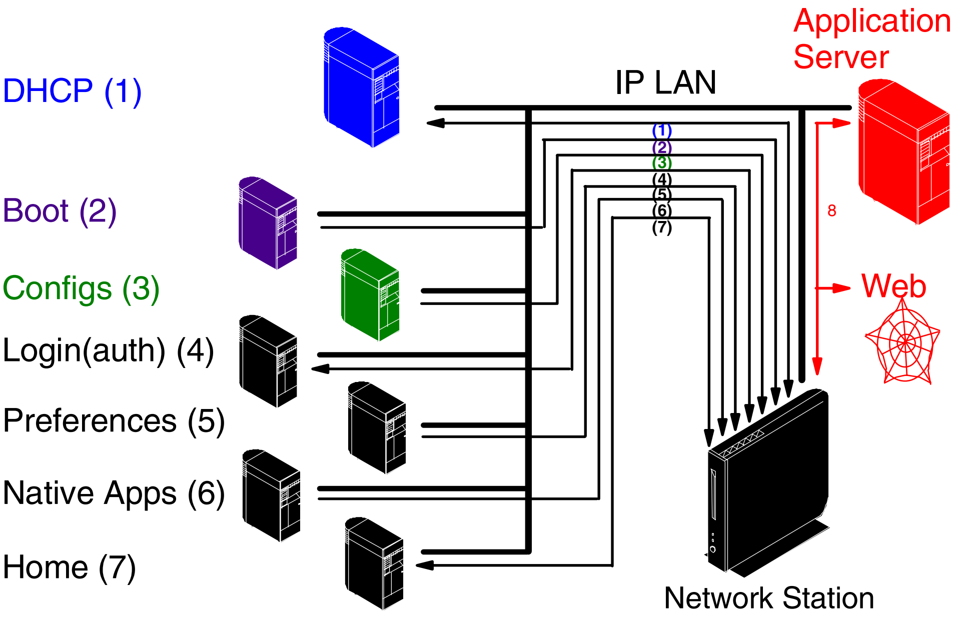


Figure 22. Boot process: Contacting application servers

The Network Station is just like any other IP host. It has access to any hosts or servers on the network and applications can be started and stopped as required by the user.

2.3.10 Summary

From this point on, only the native applications server can still be accessed whenever a native application requires to be loaded or reloaded. The home server is accessed whenever the user needs to change or enter some application preferences. The boot server is accessed even if the user does not log out. In V2R1, the application is not loaded en masse as it was in Version 1 of NSM. Rather, it is demand paged in as its pages are accessed. If the boot server is down, it is unlikely that the application can function for long.

Access to the DHCP server may be required in cases where the lease on the IP address has expired and the station needs to contact the DHCP server to renew the lease. This would take place automatically without the user being aware of the process taking place.

As previously stated, to describe the overall boot process, we proceeded step-by-step, identifying along the way each individual type of server that needs to be accessed, and for what purpose, since our intent was mainly to understand the role of each server.

In reality, some of these logical servers are actually combined and reside on one physical machine. Although, in theory, one could set it up in such a way as to use all of these servers. In practice, some of these will always be combined. In the next section, we look at some of these decisions and the advantages and disadvantages of either separating or combining some of these servers.

2.4 Boot process examples

Now that you have an overall understanding of all the logical steps and servers that make up the boot process, let us look at a few typical practical examples.

2.4.1 A LAN boot example: Workgroup with less than 50 users

Figure 23 shows an environment that would be typical for a small workgroup, for example between 10 and 50 users. All the components are on a local LAN segment and the total number of users that could be handled really depends on the overall network traffic that they generate.

The servers used could be AS/400, RS/600, or PC servers. It is possible to have a mix of servers, although that would probably be unusual in such a small environment because of the skills required to maintain multiple platforms.

Figure 23 shows a small AS/400 installation or small Windows NT Terminal Server Edition installation, for example.

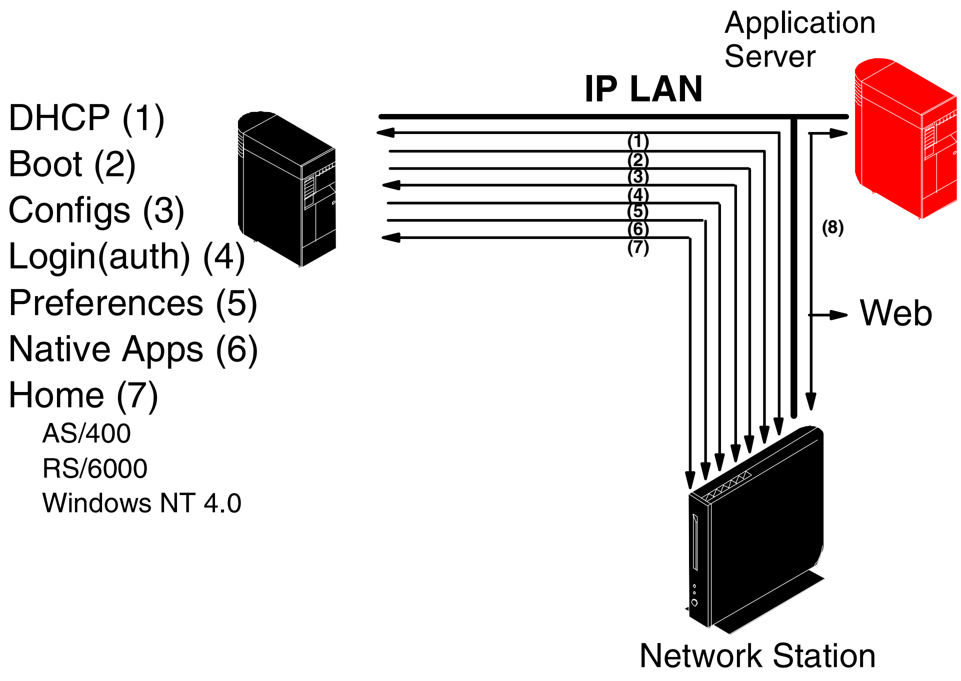


Figure 23. A LAN boot example: Workgroup less than 50 users

As discussed previously, if there is a small enough number of stations, a DHCP server may not be required and NVRAM could be used in that case. For the same reasons, the application server does not have to be a separate machine. The same server could be used for all functions provided that it is powerful enough for the tasks at hand.

2.4.2 A LAN boot example: Workgroup larger than 50 users

As we stay within a local LAN environment but move to a larger workgroup where the number of users is above 50, there are a few more considerations that come into play. For example, we may want to consider the need to use multiple boot servers to maintain a reasonable performance, the need to monitor the capacity of the LAN, and a greater need to plan for a worst case scenario and for backup mechanisms. In this case, it starts to make sense to separate the server functions as shown in Figure 24.

Because of the larger number of users, a DHCP server should now be used to facilitate the management of IP addresses. You should also have the flexibility to easily re-assign where the stations boot from, for example, in cases where we want to start use load balancing and in emergency situations.

Whether to use multiple DHCP servers and where to locate these servers becomes a question of overall network planning and design, as well as network policies within the organization. See Chapter 3, “Planning and design issues and choices” on page 35, for additional details on this issue.

In this case, we need more than one boot server to satisfy the needs of all the stations and we may want to install a boot server on each LAN segment, if there are multiple segments, or allocate a boot server to IP subnets and manage this through the DHCP server. All of this highly depends on the actual topology of the network and traffic volumes and patterns.

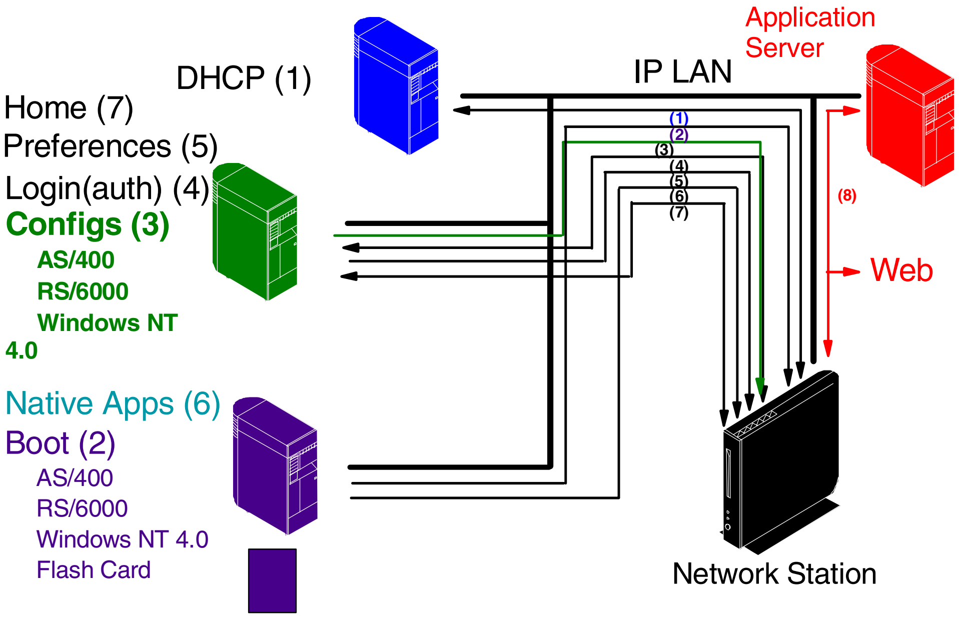


Figure 24. A LAN boot example: Workgroup greater than 50 users

Another possibility for booting Network Stations is to use a *flash card boot*. A flash card is like a local storage device on which the files that are needed for booting a station, such as the kernel, the fonts, and the application modules, can be recorded.

The card is inserted into the Network Station and the boot monitor is directed to read these files from the local card instead of from a server on the network.

This can be advantageous where there are a small number of users in a remote office connected through a low bandwidth link and where a boot server in such a small location becomes hard to justify. Other Network Stations (see the discussion in the beginning of Chapter 6, “Flash card management” on page 143, for advice regarding the number of Network Stations that can peer boot from another with a flash card) can also boot from another Network Station that has a boot flash card in a process called *peer booting*.

The files on the flash card can be managed, to a certain extent, using Network Station Manager.

Yet another option may also be a thin server running on an IBM 2212 Nways router or the newer Whistle InterJet, for example. For more information about the Whistle InterJet, see the Web site at: `http://www.whistle.com/`

All the other servers, such as the configuration, authentication, preferences, and home servers, are combined on the same physical machine, where we also have the Network Station Manager application that can be used to manage the configuration files for system and user definitions.

Typically, these configuration files are small, compared to the kernel and application modules. Therefore, the load on such a server is much less than on a boot server. From an administrative point of view, it is much easier to combine all of the configuration data and user accounts on one server rather than to manage multiple sets of configuration files on multiple servers.

In a Windows NT environment, even though this server could potentially reside on the same machine as a backup domain controller, an analysis would be required first to determine whether this can negatively impact the performance of the Backup Domain Controller (BDC). Typically, the Primary Domain Controller (PDC) and BDC are machines dedicated to these functions.

2.4.3 A LAN/WAN boot example: Enterprise greater than 500 users

Here is another large enterprise environment example, based on a real customer with upwards of 5,000 users in 65 remote branches. This customer uses a centralized management approach at the headquarters location and uses network management tools such as Tivoli’s IT Director and others to manage the remote servers and Network Stations. The Network Stations have Single Network Management Protocol (SNMP) Management Information Base (MIB) capabilities (read only) and can be rebooted remotely from a central location.

The branch offices have no local Information Technology staff because the actual Network Stations are easy to install and maintain. They can be installed and plugged in right out of the box without any other intervention.

The local branch offices are connected to the corporate central LAN through a variety of WAN links, using different technologies such as Frame Relay.

The management of IP addresses is centralized and controlled through the corporate DHCP server. This allows the corporate network administrators to easily change the configuration data for each an every Network Station in the network and direct them to boot from selected boot servers, all without any intervention at the local branch office.

The authentication and preferences servers are also centralized, located on the corporate LAN, and allow management and control of all user configuration data in a single location. A user from any branch can easily roam from branch to branch and still have their user preferences stay the same.

The native applications are obtained form the local boot server, but the home directories are located on the home server at the central site. This facilitates the management and backup of these files.

Finally, all application servers are accessed on the corporate LAN. Figure 25 shows an example network of systems for this scenario.

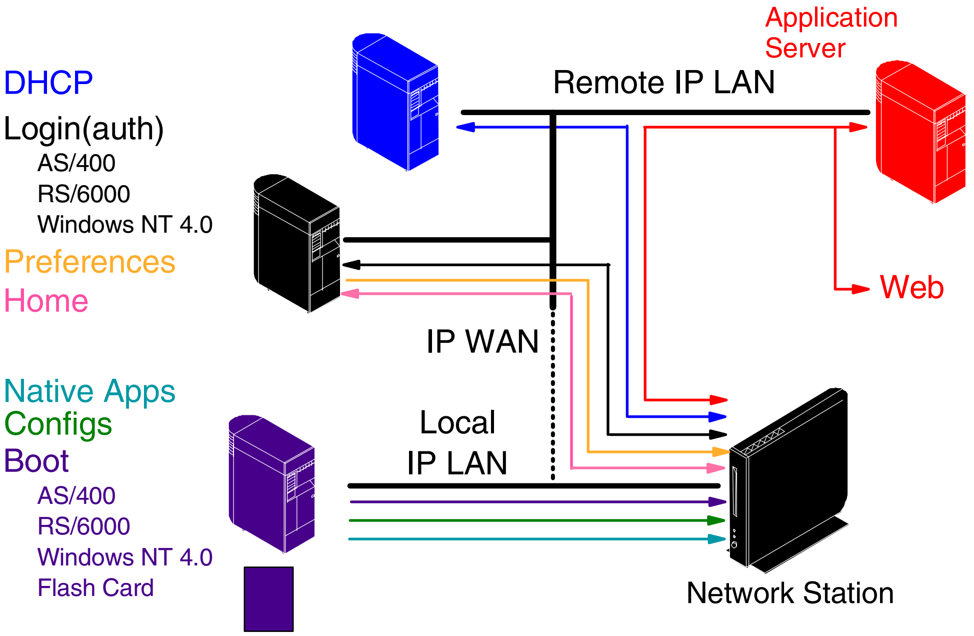


Figure 25. A LAN/WAN boot example: Enterprise greater than 500 users

2.4.4 Review of the boot process

Here are the key phases of the boot process:

1. The Power On Self Test (POST) displays the logo, counts the memory, and checks the presence of the keyboard and mouse.
2. The LAN adapter is opened, and the station inserts itself into the network.
3. The station retrieves the network information it needs to contact a boot server:
   - If using a Network boot (recommended method):
     a. A DHCPDISCOVER frame is broadcasted on the network. The frame contains the MAC address of the station.
     b. A DHCP server returns the IP address that the station should use, the boot server address, and the path to the kernel file.
   - If using an NVRAM boot (for small networks or test cases), the station loads the station IP address, the boot server address, and the path to the kernel file from the local NVRAM.
4. Trivial File Transfer Protocol (TFTP) or Network File System (NFS) is used to download the operating system.

5. NFS (or Remote File Sharing (RFS) for AS/400) is used to download the configuration files.
6. The user logs on and gets authenticated.
7. NFS (or RFS for AS/400) loads the user preferences files.
8. NFS loads the application modules.
9. NFS mounts the server’s file system.

2.4.5 Summary

In summary, installing Network Stations is easy since there is little to do but unpack the machines, connect devices, and power up, assuming that everything has been planned in advance to support these stations. Equally, installing the actual server or servers can also be an easy task once all the planning decisions regarding the type of server or servers to use, their location, and their role have been done.

The installation planning itself is the hard part, especially the network planning and design part which is the biggest and most critical part. The main tasks are to understand the LAN environment and network topology of the installation. The capacity of the LAN must be well understood, as well as the existing administration procedures and policies, the security policies, and the availability and distribution of Information Technology skills. The service level requirements must also be well understood to ensure that they are met.

Essentially, because the Network Stations highly depend on the network for their operation, the network design and planning are the most essential and the most critical factor in the implementation of Network Stations.

Chapter 3, “Planning and design issues and choices” on page 35, looks at the planning and design issues by attempting to identify the important elements that must be considered and by providing as many details as possible on each of these elements. The objective is not necessarily to provide the answers, but to provide all the questions that should be asked and provide some insight into the impact of some of the key decisions that are made.

Chapter 3. Planning and design issues and choices

In Chapter 2, “Network Station architecture” on page 13, we focused on understanding the architecture of the Network Station environment and the boot mechanisms while avoiding, on purpose, getting into too many technical details.

In this section, we review these same steps. This time, we focus mainly on identifying and understanding the choices that exists at each step along the way, from the different models of Network Stations that one can choose from, to the many network design choices that need to be analyzed when implementing a network of IBM Network Stations.

The goal is to provide a good understanding of some of the planning and design issues and choices when planning the implementation of IBM Network Stations, the advantages and disadvantages of some of these choices, when appropriate, and other issues that might need to be investigated further.

We will do this by building diagrams and adding pieces in a gradual fashion, so that we can focus only on a subset of components at a time, until we get a complete picture.

3.1 Summary

When you consider the implementation of Network Stations, planning is the key to success. There are three primary areas of planning you need to consider:

- The installation and configuration of the Network Station units themselves

  This is the easy part. It consists mainly of deciding which models are required in which locations, and the amount of memory they should have, the type of network adapter if using different types, and possibly keeping track of which units (MAC address) go to which location.

  The installation itself is simply a matter of unpacking the Network Station, attaching the I/O devices, and plugging the unit into the network.

  If using DHCP, there is no need for any configuration at the remote site. You simply plug it in and are ready to begin.

- The installation and configuration of the servers required to support these Network Stations

  This part of planning is a bit more involved since it requires you to take more factors into consideration and definitely requires Information Technology skills. Yet, if you consider only the actual server installation and configuration planning activities, these represent only a medium level of difficult. This is especially true once you know where the servers are to be located, how many are required, and which logical server functions each machine is to perform, which are all decisions that come from planning the next step (network).

- The network design and analysis activities required to ensure that the existing (or new) network can support the network traffic volumes and patterns generated by the Network Stations

  This is by far the most difficult and critical planning activity. It will have the biggest impact on the success of the installation.

Network administrators must perform these tasks:

- Assess the impact of the additional traffic generated by the boot and application activities of the new devices. Or, if using a new network, they must estimate the traffic volumes and patterns to design an initial network topology
- Determine whether the current capacity of the network can handle the additional traffic. If not, they must determine the changes that are required in the current topology.
- Analyze where the different logical server functions should be located to meet the service level criteria of the enterprise.
- Analyze the location of the servers in light of the administrative and network management policies of the organization.
- Assess whether the planned implementation meets the security guidelines of the network.
- Determine the level of fail-safe operation and backup that needs to be implemented.
- Take into account the level of IT skills required at each level in the network.

There are so many aspects to network planning that we cannot provide you with the answers here. However, we try and identify the major decisions, trade offs, and options that need to be examined further during the planning activities. Each of these must be considered in the context of the specific environment that is being implemented.

3.2 Network Station hardware components

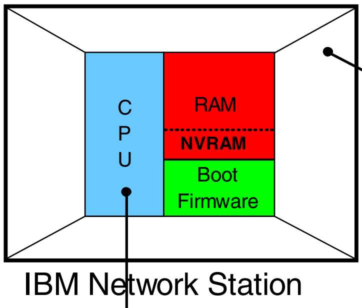
Let’s start again with the Network Station Hardware and examine the different choices that are available on the hardware side. Table 2 summarizes the key decisions to be made.

Table 2. Key hardware decisions

Choices	Factors to consider
Model	Application types and mix
Memory Size	Number of simultaneous applications (real memory) and print buffer requirements
Adapter Type	Choice of technology (Token-Ring or Ethernet)
Monitor Type	Applications used and user requirements
Video Support	Resolution and video refresh rates needed by user or application
Mouse	Normally 2-button (shipped); can use 3-button for AIX
I/O Ports and Devices	Audio, serial, and parallel are standard; PCI, PCMCIA, flash card, touch screens, multiple serial adapter card, and others are based on special needs

3.2.1 Network Station models

The IBM Network Station models available are shown in Figure 26, in the table on the right.



Model	Description
8361-100	Series 100 Ethernet
8361-200	Series 100 Token-Ring
8361-110	Series 300 Ethernet
8361-210	Series 300 Token-Ring
8361-341	Series 300 Twinax
8362-A22	Series 1000 Token-Ring (32M)
8362-A23	Series 1000 Token-Ring (64M)
8362-A52	Series 1000 Ethernet (32M)
8362-A53	Series 1000 Ethernet (64M)
8363-Txx	Series 2200 Token-Ring
8363-Exx	Series 2200 Ethernet
8364-Txx	Series 2800 Token-Ring
8364-Exx	Series 2800 Ethernet

Model	Technology	Speed
Series 100	Power PC 403	33 MHz
Series 300	Power PC 403	66 MHz
Series 1000	Power PC 603	200 MHz
Series 2200	Intel-based MMX	233 MHz
Series 2800	Intel-based MMX	266 MHz

*** Series 100 is V1R3 only**

Figure 26. IBM Network Station models and processors

The table at the bottom in Figure 26 identifies the different processor types for each family of IBM Network Stations. This gives you a feel for the processing power available with each model, when making a decision about which model to select.

Note that the Series 100, 300, and 1000 use a Power PC processor. and Therefore, they require the NCDi kernel that is available with V1R3 of Network Station Manager.

The Series 2800 and Series 2200 models on the other hand are x86-based and require the new NCi kernel available with Network Station Manager V2R1.

Note that Series 100 is not supported by NSM V2R1, and that the new Series 2800 and Series 2200 are not supported by NSM V1R3, but the Series 300 and Series 1000 are supported by NSM V2R1.

Which Network Station model to choose

Given these choices of Network Station models, which model is appropriate and in what circumstances or environment?

The raw processing power itself is not necessarily the important factor. For example, you do not question the processor that is in your cell phone or calculator, as long as it does the job it was intended to do. The same applies here in terms of choosing a model of the Network Station.

The primary decision factor to be considered when choosing a particular model is the intended workload of the Network Station. Simple emulator applications, for example, are less demanding than Java applications.

Many customers may already have the following older Network Station models in their environment. They may choose to keep them if they still fit the application requirements. Support is still offered in the new NSM.

- Series 100: Basic Host Access (not supported by NSM V2R1!)

  Use the Series100 when the applications requirements are only entry level, such as host terminal emulation. In other words, the Series 100 is appropriate when replacing dumb terminals, sometimes called “green screens”, where a minimum of processing is done on the Network Station.

- Series 300: Host Access, no browser and no Java

  Use the Series 300 when the applications are host emulators or when using the station as an X Windows terminal to access remote servers such as UNIX and AIX systems or WinFrame and WinCenter multi-user Windows NT systems.

  Generally, the 300 is less suited to browser use and not suited for Java applications. NSM V2R1 dropped support for the Twinax version of this Network Station.

- Series 1000: Web Access, light to medium Java

  Use the Series 1000 when you are using Java applications or Lotus eSuite WorkPlace 1.5. In fact, Lotus eSuite Workplace should not be used on anything less than the Series 1000.

  Use the Series 1000 also for Internet access through a browser, as well as possibly some light or simple Java applets or applications.

The following newer models should be considered for the applications as indicated:

- Series 2200, host access, Web access, and light Java

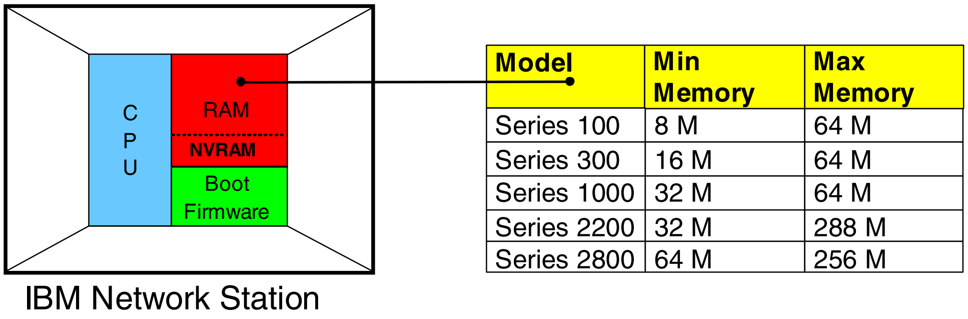
  Use the Series 2200 when the workload is fairly similar to the Series 1000 but you want to use an x86-based engine and the newer hardware.

- Series 2800, host access, Web access, and heavy Java

  Use the Series 2800 when in addition to host access and Web browsing when there is a need for heavier Java work.

3.2.2 Network Station: Memory sizes

The next important element is the amount of memory that each Network Station should have. The maximum amount of memory available on the different models is listed in Figure 27.



Model	Min Memory	Max Memory
Series 100	8 M	64 M
Series 300	16 M	64 M
Series 1000	32 M	64 M
Series 2200	32 M	288 M
Series 2800	64 M	256 M

Figure 27. Memory sizes

As a reminder, the Network Station is a real memory system. The amount of memory must, therefore, be chosen more carefully since virtual memory swapping cannot be used as a substitute or corrective.

In general, increasing the amount of memory increases the number of applications that can be run, but it does not improve the performance. If a low memory condition exists when an application is required, the application simply cannot be loaded. In critical low memory conditions, the kernel may close applications to free memory as a last resort.

How much memory is needed

The amount of memory required is a matter of calculating the total number of applications that are expected to be run simultaneously and adding up the memory requirements of these applications.

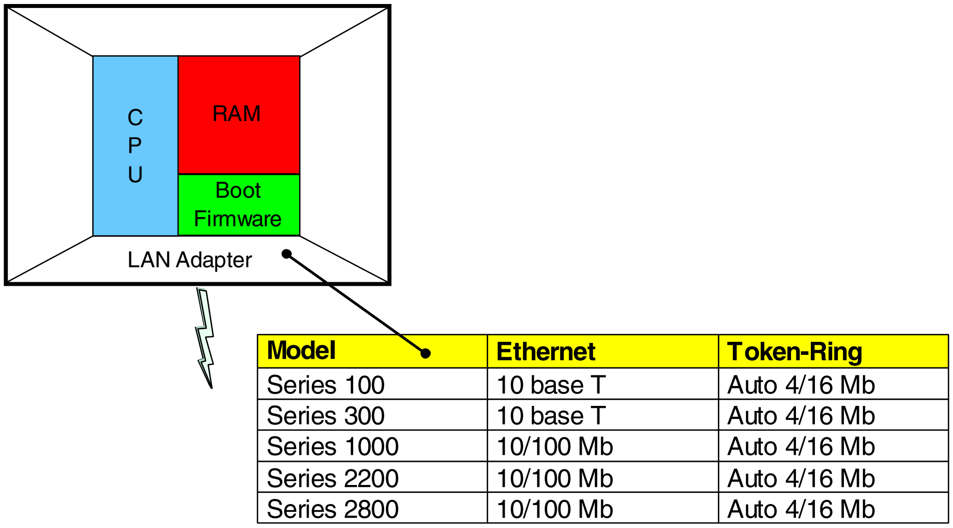
Memory requirement tables are available on the Web at: `http://www.pc.ibm.com/` See Appendix I, “V2R1 memory requirements and network load” on page 643, for details on how to retrieve such documents.

These tables provide an estimate of the amount of memory required by each application. Note that the amount of memory required varies in some cases when you are using extended or non-extended fonts or Double Byte Character Set (DBCS) languages.

One item that is not mentioned in these tables is the amount of memory required for printing. If the Network Station is receiving or sending large print requests, you might give special consideration to the amount of memory required for print buffers, especially if the remote systems do not support LPR/LPD streaming.

3.2.3 Network interface adapters

The Network Station can use either a Token-Ring or an Ethernet network interface card. All Token-Ring adapters are auto 4/16 Mb adapters, while Ethernet adapters are the 10 Mb version in the Series 100 and 300, and 10/100 Mb in all other models. Figure 28 shows the network adapters for each model.



Model	Ethernet	Token-Ring
Series 100	10 base T	Auto 4/16 Mb
Series 300	10 base T	Auto 4/16 Mb
Series 1000	10/100 Mb	Auto 4/16 Mb
Series 2200	10/100 Mb	Auto 4/16 Mb
Series 2800	10/100 Mb	Auto 4/16 Mb

Figure 28. Network Station hardware components: Network adapters

Which adapter to choose

The choice of the adapter is most likely and simply pre-determined by the type of network that you are implementing. In other words, it is more likely that the choice of the transport technology will be a network design decision that will simply dictate the type of adapter required. There are no specific advantages or disadvantages that need to be considered in choosing between a Token-Ring and an Ethernet adapter other than the inherent characteristics and capabilities of these two technologies, which we do not intend to debate in details in this section.

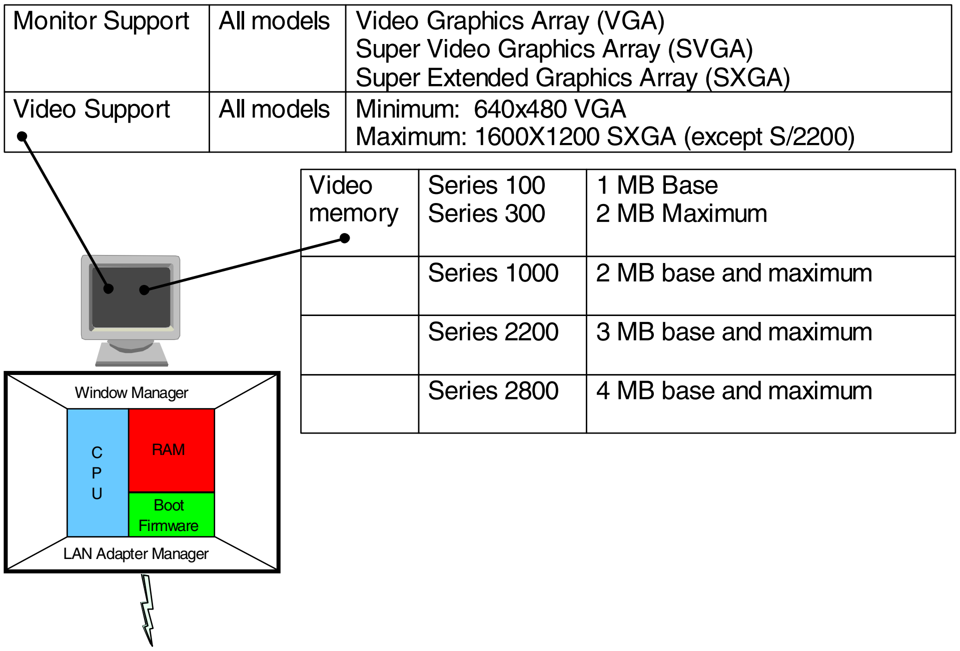
One characteristic that may come into play with Network Station is the fact that during boot storms, after a power outage for example, a Token-Ring adapter may be best. It does not suffer from the collisions experienced with Ethernet adapters.

3.2.4 Monitor and video support

The monitor and video mode support choices are:

- All models support Video Graphics Array (VGA), Super Video Graphics Array (SVGA), and Super Extended Graphics Array (SXGA).
- All models support a minimum resolution of 640x480 (VGA) to a maximum of 1600x1280 (SXGA) with the exception of the Series 2200 that does not support 1600x1280.
- The video memory is 1 MB base to 2 MB maximum in the Series 100 and 300, 2 MB base and maximum in the Series 1000, 3 MB base and maximum in the Series 2200, and 4 MB base and maximum in the Series 2800 with support for 2D and 3D acceleration.

Figure 29 shows the monitor and video supported on each model of the network station.



Monitor Support	All models	Video Graphics Array (VGA) Super Video Graphics Array (SVGA) Super Extended Graphics Array (SXGA)
Video Support	All models	Minimum: 640x480 VGA Maximum: 1600X1200 SXGA (except S/2200)

Video memory	Series 100 Series 300	1 MB Base 2 MB Maximum
	Series 1000	2 MB base and maximum
	Series 2200	3 MB base and maximum
	Series 2800	4 MB base and maximum

Figure 29. Network Station hardware components: Video support

The numbers in Table 3 indicate the maximum color depth available at different resolutions with the different Network Station models both at V1R3 and V2R1 paired with the maximum screen refresh rate.

Note: The pairs of numbers xxx/yyHz represent the maximum color depth as xxx and the maximum refresh rate as yyHz. For example, 64k/85Hz would be a 16-bit color depth and an 85Hz refresh rate. 256/48Hz (interlaced) would be an 8-bit color depth and a refresh rate of 48Hz interlaced.

Table 3. Maximum color depth (colors available) and refresh rates at different screen resolutions

Resolution	S/300, S/1000 at V1R3	S/300 at V2R1	S/1000 at V2R1	S/2200 at V2R1	S/2800 at V2R1
640 by 480	256/85Hz	256/85Hz	64k/85Hz	64k/75Hz	64k/85Hz
800 by 600	256/85Hz	256/85Hz	64k/85Hz	64k/75Hz	64k/85Hz
1024 by 768	256/85Hz	256/85Hz	64k/85Hz	64k/75Hz	64k/85Hz
1280 by 1024	256/75Hz	256/75Hz	64k/75Hz	256/60Hz	64k/85Hz
1600 by 1280	256/48Hz (interlaced)	256/48Hz (interlaced)	64k/48Hz (interlaced)	not supported	64k75Hz
Note: The actual resolution and refresh rate depends on the display capabilities.					

Here are few design decisions you need to make:

- The only hardware decision is whether to use an extra 1 MB of video memory if you are using a Series 100 or 300.

  You need to pay attention to this in cases where using a 17-inch flat screen that must run in 1280 by 1024 resolution.

- The mode used will likely be driven by the choice of a particular resolution that you want to use. This may very well be more of a user decision than a system design decision.

  Given that there is a wide range of modes and resolution available, a combination of the set of applications used, the physical size of the monitors used, and the resolution considered comfortable by users will dictate the choices to be made.

3.2.5 Keyboard and mouse support

There are also connections for the keyboard and mouse (Figure 30 on page 42). The keyboards are 102-key PC keyboards, which are available in different languages. The mouse is a two-button mouse.

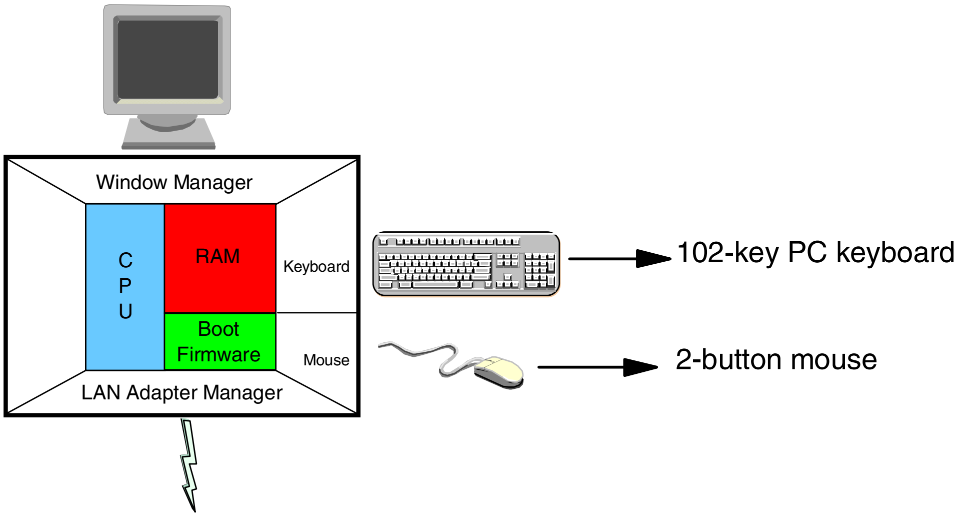


Figure 30. Network Station hardware components: Keyboard and mouse

3.2.5.1 Which keyboard to select

Keyboard selection becomes necessary when dealing with one or more languages different than English.

Series 2200 keyboard USB attached

The Series 2200 keyboard and mouse, unlike the Series 2800, are connected to a Universal Serial Bus (USB) port.

See the product publications for a list of selectable keyboards.

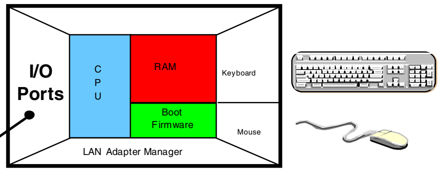
3.2.5.2 Which mouse to select

The standard mouse shipped with the Network Station is a two-button mouse, which applies to all environments.

However, if the user is a UNIX or AIX user, a three-button mouse may be more appropriate. It is supported but not shipped with the Network Station.

3.2.6 Other I/O ports and devices

There are a variety of I/O ports and devices that are available depending on the different models. These capabilities are summarized in Figure 31.



I/O Ports	Series 100	Series 300	Series 1000	Series 2200	Series 2800
Audio	8-bit Speaker	8-bit Speaker	16-bit Jack	16-bit Stereo Output Jack Mono Input Jack	16-bit Stereo Output Jack Mono Input Jack
Serial Port	1	1	1	No	2
Parallel Port	1	1	1	No	1
PCI Adapter Slots (half-length)	None	None	None	No	2
PCMCIA Type II	Yes	Yes	Optional	No	No
Smart Card	No	No	Yes	No	?
USB Ports	No	No	No	2	2
Flash Memory Cards	PCMCIA (linear C/D) (8 to 40 MB)	PCMCIA (linear C/D) (8 to 40 MB)	PCMCIA (linear C/D) (8 to 40 MB)	Compact Flash (8 MB to 96+ MB)	Compact Flash (8 MB to 96+ MB)

Figure 31. Network Station hardware components: I/O ports and devices

3.2.6.1 Serial port

One native serial port is available by default on all models except the Series 2200. The Series 2800 provides two native serial ports.

If more than one serial port is required, using a Personal Computer Memory Card International Association (PCMCIA) Multiple Serial Adapter is a possible option to increase the number of serial ports from one to four. This type of adapter is not provided by IBM but by third parties.

On the Series 2800, using PCI adapter cards can provide an additional eight serial ports per PCI adapter. Note that adding additional ports permits the attachment of devices, such as MICR readers, pole displays, cash drawers, etc. IBM does not supply any device drivers for these devices. Application programming is required to send and receive data to these ports and devices.

3.2.6.2 Parallel port

The parallel port is typically used to attach a parallel printer.

3.2.6.3 PCMCIA type II adapter

This is standard on the Series 100 and 300 but optional on the Series 1000. On the Series 2800, PCI adapters are available instead, but not on the Series 2200.

3.2.6.4 Smart Card

Note that a Smart Card reader can be attached, but that the software to support it is not provided.

3.2.6.5 USB ports

Note that the Series 2200 provides only two USB ports (meaning that there are no serial or parallel ports, only USB ports). One USB port is used by the mouse and keyboard, leaving one port available for other uses.

Usually, it is possible to find devices that attach to the keyboard port (for example, card swipe readers) and, while not supported, they usually work fine. The intelligence is built into the device instead of in the device driver.

The Series 2800 has two USB ports available in addition to the other usual ports.

3.2.6.6 Flash memory cards

The use of flash memory cards was not a standard option on the Network Station. However, it was released as a Request for Price Quote (RPQ) in Release 3 of Network Station Manager in September 1998. This feature allows the Network Station's operating system and other application code to be loaded from a flash card instead of being loading from the network. If the boot server is not accessible via the LAN, but only across a WAN, it is really not a viable solution to boot across a WAN (although possible). In such a case, a flash card becomes an acceptable alternative.

The flash memory card represents one possible solution in cases where loading the operating system and application files would otherwise need to be done across a slow-speed WAN link, or where additional local boot servers may need to be implemented and maintained locally to provide boot services. Other Network Stations can also be booted from a flash card in another network station. This is known as *peer booting*.

In all cases of flash booting, we recommend that you load large stable files from the flash memory card. Load smaller more volatile configuration files from a centrally administered server on the network.

There are two types of flash adapter cards:

- The *PCMCIA flash adapter card* that comes as linear C series, which can hold up to 10 MB, and linear D series, which can hold up to 40 MB
- The *Compact Flash Card*, which can hold from 8 MB to 96 MB and fits into a compact flash card adapter slot, which can be reached from inside the Network Station on Series 2200 and 2800

  Because the casing of these stations can easily slide out of the housing, it is an easy operation to insert a flash card into the adapter receptacle.

For more information about flash booting and peer booting, see Chapter 6, "Flash card management" on page 143.

3.2.6.7 Touch-screen support

The series 300, 1000, and 2800 (not the 2200 at the time of this writing) support the attachment of touch screens. The touch-screen monitors that are supported with V2R1 of NSM and the above hardware are only:

- IBM Microtouch Monitors: G70 t, G42, G54, G74, G94, flat panel T55A
- ELO TouchSystems' IntelliTouch Ultra; Visit Elo on the Web at:
  `http://www.elotouch.com/`

The setup of a touch-screen is fairly simple. You connect the monitor cable just like a monitor and the serial cable to the serial port on the Network Station (port 1 for the 2800, which is the bottom port when the system is standing up).

Then, use NSM to enable the touch-screen daemon. Set the preference level to **WorkStation**. Then, click **Hardware->Workstation->Monitor Settings** to specify that you are using an IBM or ELO touchscreen. Optionally, the touch daemon can be started using either of the following command lines:

- `/usr/local/nc/bin/ibmtouchdaemon`
- `/usr/local/nc/bin/elotouchdaemon`

  Specify the serial port to be used (for example, `/dev/tty00`)

You can calibrate the touch-screen in NSM V2R1 using one of three ways:

- The desktop GUI task bar **Toolkit->Calibration Tools**
- The command line interface: `/usr/local/nc/bin/calibrate`
- Automatically by the touch daemon the first time when either `/usr/local/nc/bin/ibmtouchdaemon` or `/usr/local/nc/bin/elotouchdaemon` is entered on the command line.

3.3 Network Station software components

In Chapter 2, “Network Station architecture” on page 13, we examined the Network Station software components. There are actually no real design decisions to be made here because everything is basically standard.

The only possible choice concerns the number and types of applications that need to be run on the Network Station. We discussed the issue of the memory required for these applications in 3.2, “Network Station hardware components” on page 36.

3.4 The boot process

As we did when we first introduced and described the boot process earlier, we go through each of the boot process steps again. This time we discuss each step in much more detail and focus on the choices that can be made at each step, including the advantages, disadvantages or impact, if any, of making certain choices in the design of the environment.

At then end of this section, you should:

- Be aware of all the main choices that must be considered in your planning.
- For each choice, understand the impact of that particular choice.

We do not pretend to address all possible issues and combinations of choices that can be made. Hopefully, we cover enough of the important aspects that you can extrapolate for other cases that may not be specifically covered.

3.4.1 Inserting Network Station into the network

We start at the point where we connect a Network Station to the network.

Table 4 on page 46 summarizes the key decisions to be made.

Table 4. Network decisions

Choices	Factors to consider
Type of network	There is only one choice, which is an IP network
Adapter type	Choice of technology (TRN or Ethernet)
Network topology and design	This is clearly the most difficult and the most important part of the planning and design

3.4.1.1 Networking protocol

As mentioned earlier, the first choice in choosing a type of network or a networking protocol is easy because TCP/IP is the only choice. TCP/IP is the only protocol that the Network Station supports (Figure 33).

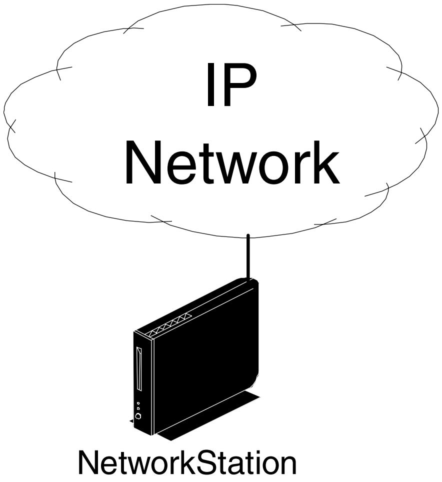


Figure 32. Boot Process: IP Network

If you are implementing Network Stations in a brand new network environment that did not exist before, there is a need for a new network planning and design effort. This will ensure that you are building a network that will accommodate the number of Network Stations that you plan to implement.

On the other hand, a more common situation may be that you are adding Network Stations to an existing network or replacing existing equipment, such as non-intelligent terminals. In that case, there is a need to assess the impact that the different traffic demands and patterns will have on the network.

Many customers today have networks that can handle multiple protocols, in either parts of the network or in the entire network. For example, there may be an existing Systems Network Architecture (SNA) backbone network, with an implementation of Multi-Protocol Transport Networking facilities that allows the IP protocol to be routed to all points in the network. In effect, in this case you have an IP network in place that supports the needs of the Network Station. However, if the network is strictly SNA, NetBIOS, or IPX/SPX, you need to implement a separate parallel network, or implement some multi-protocol capabilities to support Network Stations.

3.4.1.2 LAN network interface adapter

The Network Station communicates on the network using a LAN adapter, either Token-Ring or Ethernet. The choice of using one or the other is often determined by existing network facilities. If no network exists, then it becomes a choice of which technology is considered to be the best for a specific environment.

In terms of performance and reliability, both are probably valid choices. However, die-hard proponents of each of these technologies would argue and make a case for each of these as being superior to the other. We certainly do not intend to enter this debate here because we consider that both have merits. In practice, many networks often use both technologies in many parts of the network.

If it is a brand new network implementation, and the possibility exists of making it homogeneous, then one advantage of using only one type of network adapter is in the area of asset management. In this case, having a reduced number of asset types always has a positive impact by simplifying equipment procurement.

In the diagrams used in this section, we assume a Token-Ring implementation for illustration purposes only.

3.4.1.3 Network topology and design

The most important network decisions concern the relative placement of the different servers and Network Stations given the existing topology and traffic patterns of the network. As with all network design cases, estimating the traffic patterns and the bandwidth requirements, while maintaining an acceptable and optimal cost, to properly satisfy the needs of the users is always the goal and the challenge.

There are so many alternatives when it comes to network design, that we definitely do not intend to provide a network design tutorial here. All we can do is show a few examples to illustrate the types of decisions that can be made and let you apply these examples to your own environment.

Most choices and decisions that we discuss here deal with the placement of the different servers that need to be accessed by Network Stations. Consideration is also given to the quantity of information that needs to be transmitted and through which type of facilities.

Figure 33 on page 48 illustrates a simplified typical network in a corporate organization.

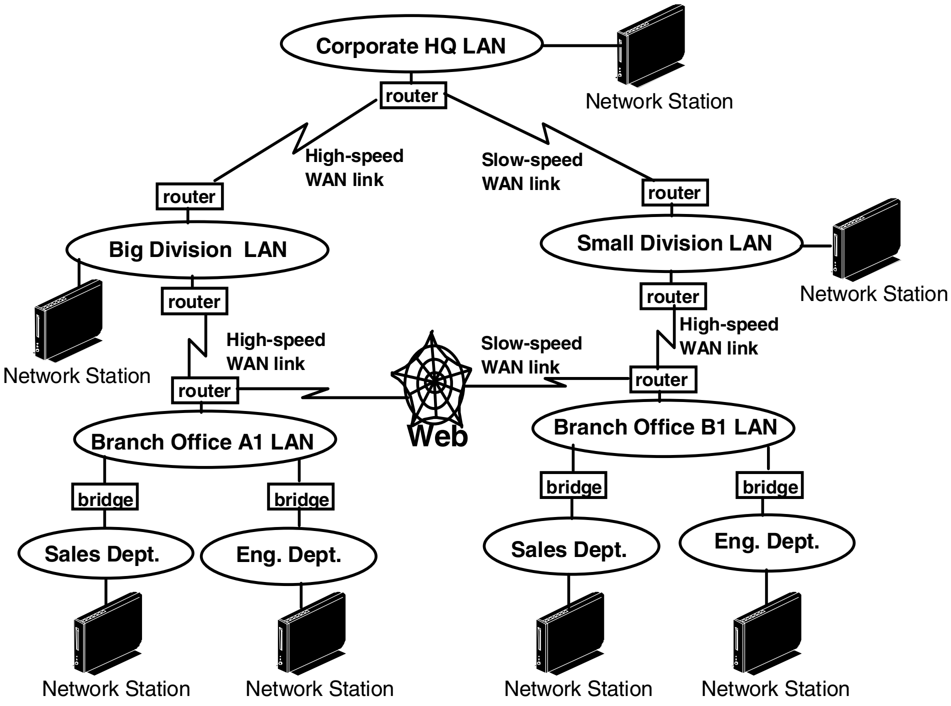


Figure 33. Network topology example

In Figure 33, many LAN segments are connected to each other using either bridges or routers connected to each other via high- or slow-speed WAN links, which could use different technologies, such as frame relay, Asynchronous Transfer Mode (ATM), and so on.

This sample corporation has multiple remote branch offices. Each branch office has a branch office LAN segment, as well as a LAN segment for each department in the branch office. Since all departments are within the same physical facility, all LAN segments in the branch are bridged together, effectively providing a single logical LAN segment.

Each branch office's LAN is connected to its divisional headquarter's LAN via routers and a WAN link. The link is high speed since there is a lot of traffic expected between the branches and their divisional headquarters. Each branch office also has a WAN link to the Web.

Each divisional LAN is tied into the corporate LAN via a WAN link as well. The link is high speed in the case of one division and slow speed in the case of the other since it is a small division with reduced traffic to headquarters only.

What becomes important in our discussions, when deciding on the location of a server, is whether the facilities in place are adequate to sustain a reasonable amount of traffic caused by the addition of these servers.

In the following examples, we use this sample network as the base for some scenarios. We simplify the network since the details are not necessarily important at this point.

3.4.2 Obtaining an IP address

Table 5 summarizes the key decisions to be made. Note that most decisions here have to do with how to set up the DHCP server to handle a Network Station environment. This topic can get quite involved. We have made an attempt here to keep it as simple as possible while trying to at least mention most of the areas that need to be examined.

Table 5. Boot-related decisions

Choices	Factors to consider
Boot using NVRAM or Network	Number of Network Stations in the network. NVRAM only for a small number or special cases; otherwise, use DHCP.
BOOTP or DHCP Server	DHCP Server recommended; more flexibility than BOOTP
DHCP Server Platform	Depends mainly on the existing network or equipment. The platform itself is not relevant.
DHCP Server Product	Depends on the features and functions desired, such as unlisted client support, class support, or others.
DHCP Server Location	Depends on the policies of decentralization and expected topology of the network in terms of the presence of bridges and routers
Number of DHCP Servers	Depends on the centralization policies of the organization, the performance required, and the amount of desired redundancy

If you remember our previous discussion of the boot process, the Network Station first needs to obtain an IP address, which it can do in one of three ways:

- The IP address is manually entered into the Network Station’s NVRAM by an administrator using the Setup utility.
- The station requests an IP address from a BOOTP server.
- The station requests an IP address from a DHCP server.

3.4.2.1 NVRAM or BOOTP/DHCP server: Which to use

Should you use NVRAM or a BOOTP/DHCP server? For those who may not yet be familiar with the Network Station, non-volatile random access memory (NVRAM) is an area of the Network Station’s memory where permanent configuration information can be recorded so that it is not erased between power off and power on.

The NVRAM method applies only when there is a small number of Network Stations to manage, or in a testing and problem determination environment.

Here are the advantages to using NVRAM:

- In cases where there is a very small network, with most machines located in the same physical site, and the network environment is stable.

  Using NVRAM avoids having to maintain a BOOTP or DHCP server. This also means having someone with the skills to implement and manage a DHCP server.
- In cases where there is a local printer attached or serial devices and the station also has the same fixed IP address.

- In cases where settings need to be done on a per-station basis such as when operating a station in suppressed login mode, restricted access, and so on.

The disadvantages of using NVRAM are:

- This method requires that an administrator be physically present at the Network Station's site to use the Setup utility on the station. They must enter the required configuration data, or each Network Station must be initially configured at a central site before being shipped to a specific remote location, which requires a good administrative tracking system.

  At a minimum, the data that needs to be entered consists of:

  - The Network Station IP address
  - The gateway IP address
  - The IP subnet mask
  - The IP address of the boot server
  - The IP address of the configuration server (only if different from the boot server)
  - The path name to the kernel
  - The boot protocol

  Actually, the last two parameters are optional because, if nothing is specified, each possible value is tried by the boot monitor. This increases the overall boot time. Therefore, we prefer that you specify the correct value.

- The IP address assigned to the station is fixed and cannot be changed from a central location. This means that even a station that is used infrequently must have a permanent IP address that cannot be used by anyone else. In most cases, this is probably not important because you should not power off Network Stations anyway. If there are changes in the topology of the network that requires changing the IP addresses of some stations, the change of address cannot be done from a central site when using the NVRAM method.
- The boot server IP address (or configuration server IP address) recorded in NVRAM also cannot be easily changed remotely from a central site to take advantage of load balancing to direct the station to boot from a different server, if required.

  The address can actually be changed by manually altering some configuration files on the boot server and then causing the station to reboot to read the new configuration files. This requires a lot of custom manual intervention. The DHCP method is much easier to implement and less costly to operate when there is a significant number of stations involved.

In other words, any change to the station's network and boot parameters requires a manual intervention at the station's site. This renders the station management more costly unless there are a very small number of stations, preferably all in the same physical location.

3.4.2.2 BOOTP or DHCP

Generally, DHCP is much superior to BOOTP in flexibility since BOOTP provides only a subset of the DHCP capabilities. Therefore, DHCP is the recommended method.

The differences between BOOTP and DHCP

Figure 34 shows the differences between a BOOTP frame and a DHCP frame.

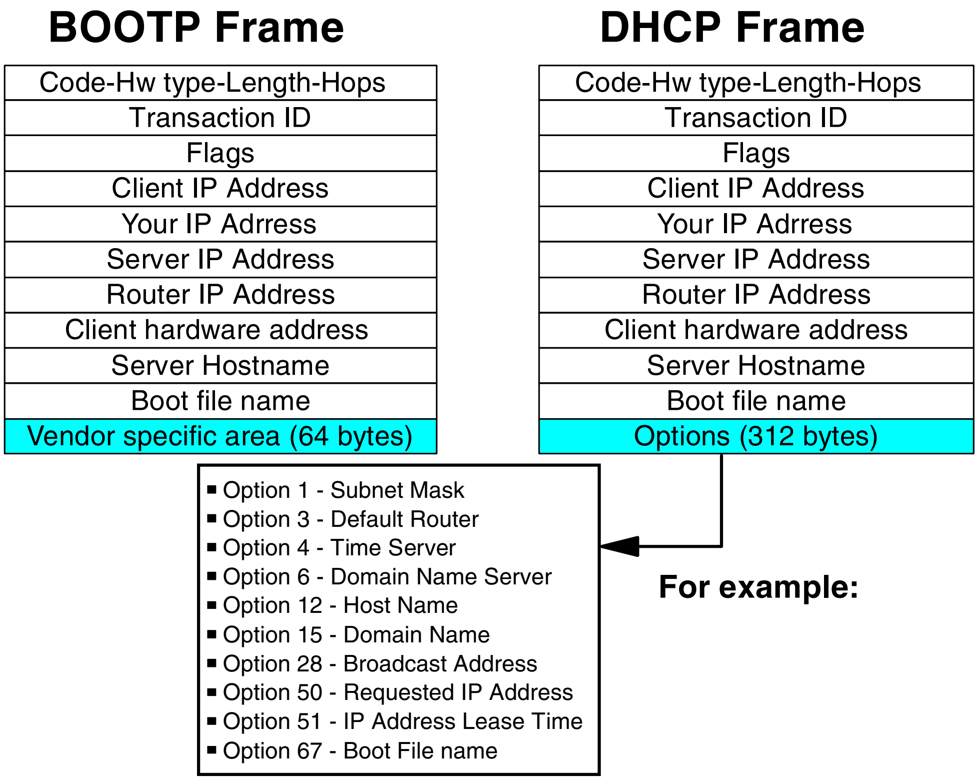


Figure 34. BOOTP and DHCP frame formats

Both BOOTP and DHCP have such basic information as client IP address, server IP address, boot file name, and so on. Notice that the BOOTP frame only has 64 bytes of vendor-specific information at the end of the frame, compared with 312 bytes of options for the DHCP frame.

In addition, these DHCP options are pre-architected options. Option numbers 0 to 127 and 255 are standardized to contain specific information as shown by the sample options in Figure 34. Non-standard option numbers 128 to 254 are user defined to include additional fields if required. For example, the following options have been added to support Network Station:

- Option 98: Authentication Server
- Option 211: Base Code Server Protocol
- Option 212: Configuration Server Address
- Option 213: Configuration Files Directory
- Option 214: Configuration Server Protocol
- Option 219: Failover Boot Server

Another important difference is that BOOTP only allows fixed IP addressing, where DHCP allows for dynamic IP addressing. In other words, a BOOTP server must already contain a configuration table with the MAC address of all potential BOOTP clients and the associated IP addresses that are to be allocated to those specific clients. With DHCP, the clients can still be defined with their MAC addresses specifically identified. Instead of recording a fixed IP address against that MAC address, DHCP allows it to dynamically allocate an IP address at the time that the client requests it.

DHCP also supports unlisted clients. This means that DHCP clients do not need to predefine their MAC address in the DHCP server configuration tables in order to be allocated a dynamic IP address. Therefore, in large networks where you need the flexibility to manage all the possible options from a central site, DHCP is a much more flexible solution and the only recommended method.

If the network is fairly small, and we make the same arguments as for the NVRAM method, then BOOTP is still an acceptable method but more restrictive.

Table 6 summarizes the main differences between BOOTP and DHCP.

Table 6. Summary: BOOTP versus DHCP

Capability	BOOTP	DHCP
IP address allocation	Fixed	Dynamic
Unlisted client support	No	Yes
Vendor Information	64 bytes	312 bytes
Architected options	No	Yes

3.4.2.3 DHCP server: Which platform and product to use

Assuming that you decide to use a DHCP server because of the added flexibility that it provides, there are two important decisions you must make concerning the DHCP server. In some cases, some of the decisions may be related to one another. The questions are:

- On which platform do you run the DHCP server?

  Use of a DHCP server is a standard TCP/IP function which has nothing to do specifically with Network Stations. In other words, most TCP/IP networks today use a DHCP server, regardless of whether the network contains Network Stations.

  It is likely that a DHCP server (or servers) already exists in the network to which you are adding Network Stations and that the corporate policy already dictates who controls the DHCP server. If there is no DHCP server yet, the choice of a platform may be dictated by the availability of existing equipment. All platforms, whether they are an S/390, AS/400, RS/6000, or PC, have a DHCP product that can be used.

  The question of how many DHCP servers you intend to use, and where you intend to locate the DHCP servers are all questions that the network administrator is responsible for determining. These questions may influence the choice of platform. For example, if there are already S/390 processors at the corporate office and this is where the DHCP server should be located, then it would make sense to run the DHCP server on an S/390 host.

  There is also nothing that precludes using different DHCP servers in the same network. However, this often becomes more a question on how much homogeneity is needed in the network. It is often a political decision related to how centralized or decentralized the organization is.

- Which specific DHCP server product should you use?

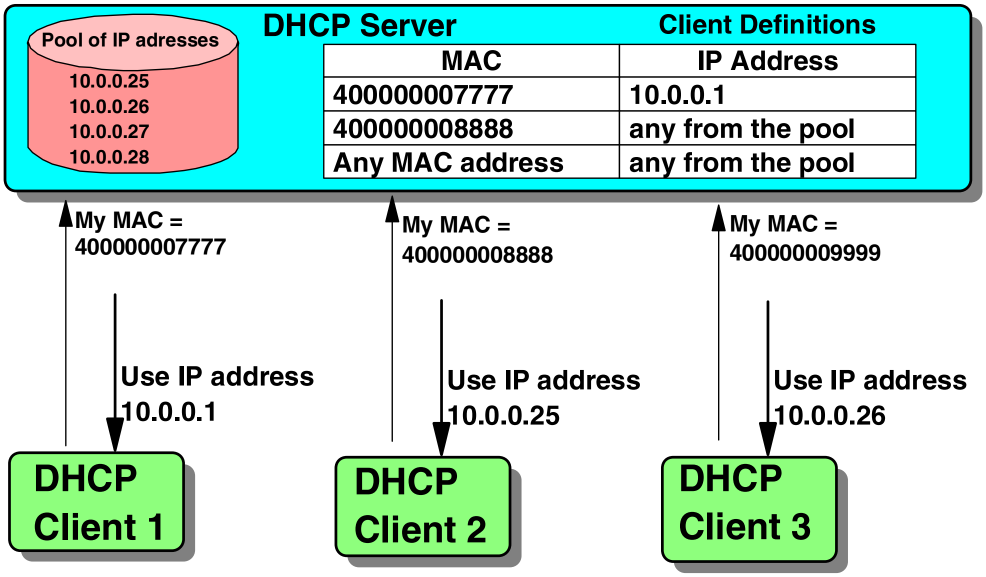
  In some cases, as in the PC platform for example, you may be able to choose more than one DHCP server product. For example, Microsoft's DHCP server is part of the base Windows NT Server product, and the IBM DHCP server is supplied with the Network Station Manager product.

  Most DHCP servers today are fairly similar in the sense that they all provide the same base DHCP functions. However, there are some slight differences in the additional features and functions that can be useful in the management of Network Stations.

  For example, you may want to investigate the following features and capabilities to see if they should be used or if they provide you with an advantage:

  - Ability to support unlisted clients

    This is the ability of having the DHCP server respond to any client, even if that client's MAC address has not been defined in the DHCP server's configuration file. This is useful in cases where you do not want to keep track of MAC addresses, yet want to be able to respond to any client. We believe that this may be the most common situation.



MAC	IP Address
400000007777	10.0.0.1
400000008888	any from the pool
Any MAC address	any from the pool

Figure 35. Listed and unlisted DHCP client support

In Figure 35, when DHCP Client 1 asks the DHCP server for an IP address, the server already has the MAC address (7777) of the client identified in its configuration table. It also has a fixed IP address already reserved for that specific client, which always gets this same address.

When DHCP Client 2 asks for an address, its MAC address is also present in the DHCP server configuration table. This time, it simply states that any address can be used, which causes the server to allocate the next available address for a pool of addresses, which is 10.0.0.25 in this case.

DHCP Client 3, on the other hand, does not have its MAC address specifically defined in the configuration table. However, the server has a configuration parameter that directs it to allocate the next available address from the pool (this is called *unlisted client support*), which is 10.0.0.26 in this case.

– Ability to support classes

The Network Station's DHCP client identifies itself to the server as belonging to a particular class. This allows the DHCP server to return a specific set of options based on the class of the device or client. The classes are listed in Table 7.

Table 7. DHCP classes

IBM Network Station Model	Description	DHCP class
8361-100	Series 100 - Ethernet - 8 MB	IBMNSM 2.0.0
8361-200	Series 100 - Token-Ring - 8 MB	IBMNSM 2.1.0
8361-110	Series 300 - Ethernet - 16 MB	IBMNSM 1.0.0
8361-210	Series 300 - Token-Ring - 16 MB	IBMNSM 1.1.0
8361-341	Series 300 - Twinax - 1 MB	IBMNSM 3.4.1
8361-A22	Series 1000/32 MB-TRN	IBMNSM A.2.0
8361-A23	Series 1000/64 MB -TRN	IBMNSM A.2.0
8361-A52	Series 1000/32 MB - ETH	IBMNSM A.5.0
8361-A53	Series 1000/64 MB - ETH	IBMNSM A.5.0
8363-Exx	Series 2200 - Ethernet	8363-EXX
8363-Txx	Series 2200 - Token-Ring	8363-TXX
8364-Exx	Series 2800 - Ethernet	8364-EXX
8364-Txx	Series 2800 - Token-Ring	8364-TXX

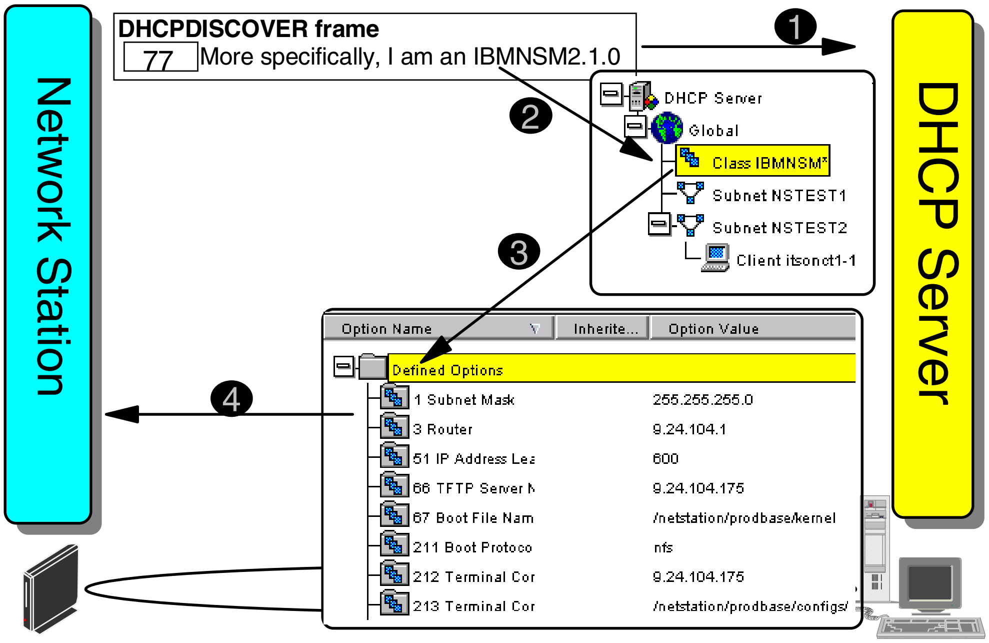
This is particularly useful in a network where the DHCP server serves a mix of Network Stations and regular PCs for example, or a mix of different types of Network Stations. It can return a different set of options based on whether the station is a PC or a Network Station, and if a Network Station, based on the type of station.

In fact, if you use the unlisted client support, this may be the only way to support mixed devices. In that case, the client cannot be identified by its MAC address. However, it can be identified by its class and served a set of options based on that class.

The AS/400 DHCP server has this class support. For an example of how to use the DHCP class support to aid in the administration of the Network Station boot administration, see 9.2.3, "Scenario 3: V1R3 clients using DHCP" on page 236, and 9.3.3, "Scenario 6: V1R3 and V2R1 clients using DHCP" on page 270.

This example is illustrated in Figure 36 where the DHCPDISCOVER frame sent to the DHCP server identifies the client as being in a class of IBMNSM2.1.0 (Series 100 Token-Ring machine with 8 MB). The server configuration has a class configured called IBMNSM*, meaning all the classes begin with IBMNSM. As a result, this client is offered all the options defined under that class, as shown in the bottom of Figure 36 (options 1 to

213). If the client had been a regular PC instead of a Network Station, it would not have identified itself as part of that class and would not be offered these options.



Option Name	Inherite...	Option Value
1 Subnet Mask		255.255.255.0
3 Router		9.24.104.1
51 IP Address Lea		600
66 TFTP Server N		9.24.104.175
67 Boot File Nam		/netstation/prodbase/kernel
211 Boot Protoco		nfs
212 Terminal Cor		9.24.104.175
213 Terminal Cor		/netstation/prodbase/configs/

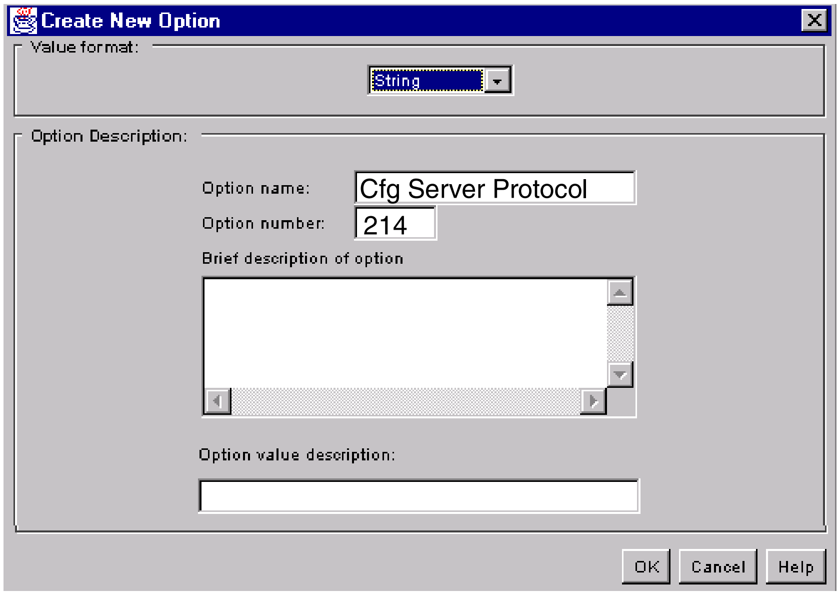
Figure 36. DHCP classes support

– Ability to add user-defined DHCP options

The Network Station uses user-defined options such as option 211 (base code server protocol). Therefore, the DHCP server must have the ability to add these options. Most DHCP servers that we know of today allow this.

Figure 37 on page 56 shows the DHCP server configuration panel (for the IBM DHCP product on a Windows NT machine) displayed when the user asks to create a new option. Here, we add user-defined DHCP option 214, which identifies the configuration server protocol.

Once this is defined, this option can be added as an option to be served to any DHCP client. The client must of course be able to recognize this option for it to take effect. Note that it does not create any problem for a client to receive options that it does not recognize since these options are simply ignored by the client.



Value format: String

Option name: Cfg Server Protocol

Option number: 214

Figure 37. Creating a user-defined DHCP option

– Ability to update a DNS server on behalf of a client

If dynamic allocation of IP addresses is used (as opposed to using fixed addresses), a station may get a different IP address every time it contacts a DHCP server. Therefore, we need the ability to dynamically update a DNS server to reflect the fact that a particular station now has a different IP address associated with its host name. The Network Station does not have the capability to send an update to a Dynamic Domain Name System (DDNS) server, but it can notify the DHCP server to send an update on its behalf.

This is illustrated in Figure 38 where the DHCP client requests an IP address from the DHCP server and asks the server to update the DNS server (1). The DHCP server returns an address to the client (2) and then sends an update to the DNS server (3), indicating the new address that should be associated with the host name mary.itso.ral.ibm.com.

From this point, any host in the network querying the DNS server for the address of mary (4) gets the address (5) that the mary.itso.ral.ibm.com host was just given by the DHCP server.

As can be seen from this example, if dynamic allocation of addresses is used, a DDNS must also be available. This is the only way to update the DNS system. A DDNS server is supplied as one of the servers available with eNetwork On Demand product that ships with the Network Station Manager product on the Windows NT platform.

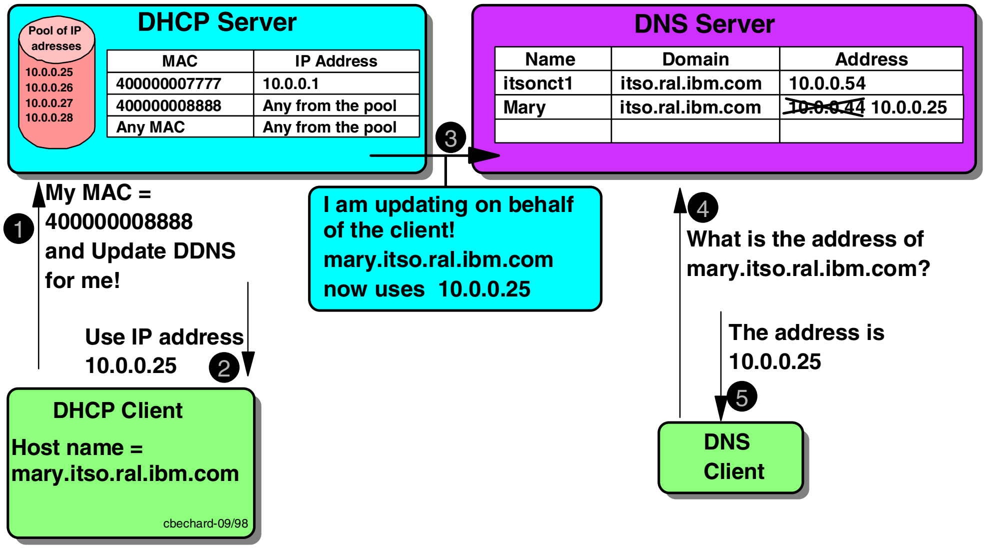

DHCP Server
Pool of IP adresses
10.0.0.25
10.0.0.26
10.0.0.27
10.0.0.28
MAC | IP Address
400000007777 | 10.0.0.1
400000008888 | Any from the pool
Any MAC | Any from the pool
DNS Server
Name | Domain | Address
itsonct1 | itso.ral.ibm.com | 10.0.0.54
Mary | itso.ral.ibm.com | ~~10.0.0.44~~ 10.0.0.25
3
1
My MAC = 400000008888 and Update DDNS for me!
I am updating on behalf of the client! mary.itso.ral.ibm.com now uses 10.0.0.25
4
What is the address of mary.itso.ral.ibm.com?
Use IP address 10.0.0.25
2
The address is 10.0.0.25
5
DHCP Client
Host name = mary.itso.ral.ibm.com
cbechard-09/98
DNS Client

Figure 38. DHCP server updating DDNS on behalf of the DHCP client

The question of whether the unlisted client facility should be used may be dictated by the security guidelines of the organization, or by the network policies concerning the management of IP addresses in the network. Consider these points:

- The advantage of using the unlisted client support is that it simplifies the management of the DHCP server by not having to maintain a configuration file with a client record for each DHCP client.
- The disadvantage of using unlisted client support is a certain loss of control over specific clients.

In many Network Station networks, the hostname may simply not be used, in which case the DHCP unlisted client support can easily be used. However, in cases where the hostname is important, using unlisted client support may not be really practical because of the fact that the Network Station does not have a fixed IP host name. For a station to have a fixed IP host name, it must have DHCP option 12, which can only be done if the client specifically identifies itself by its hardware address so that a configuration containing options specific to that client can be used.

Table 8 shows a list of the DHCP servers and their support for the features we discussed.

Table 8. Comparison of DHCP products

DHCP server feature	Windows NT Server 4.0 IBM DHCP	Windows NT Server 4.0 Microsoft DHCP	AS/400 V4R2+	AIX
Support BOOTP clients	Yes	No?	Yes	Yes
Unlisted client support	Yes	Yes	Yes	Yes
Class support	Yes	No	Yes	Yes
User-defined options	Yes	Yes	Yes	Yes
Update DDNS for client	Yes	No	No	Yes

3.4.2.4 Locate the DHCP servers

There are two primary considerations concerning the location of the DHCP servers in a network:

- Political consideration depending on corporate policies on decentralization.

  For example, in a strong centralized corporation, the corporate network administration may control the entire network and, therefore, use a single DHCP server at the central location. If it makes sense topology wise, a DHCP server may be located at each division, to manage the resources within the division while it is still under the control of the corporate network administrators.

  On the other hand, in a decentralized organization, a DHCP server may be used at the divisional level and controlled by the division’s network administrators. A DHCP server may also be present at the corporate level but only for managing resources at the corporate level.

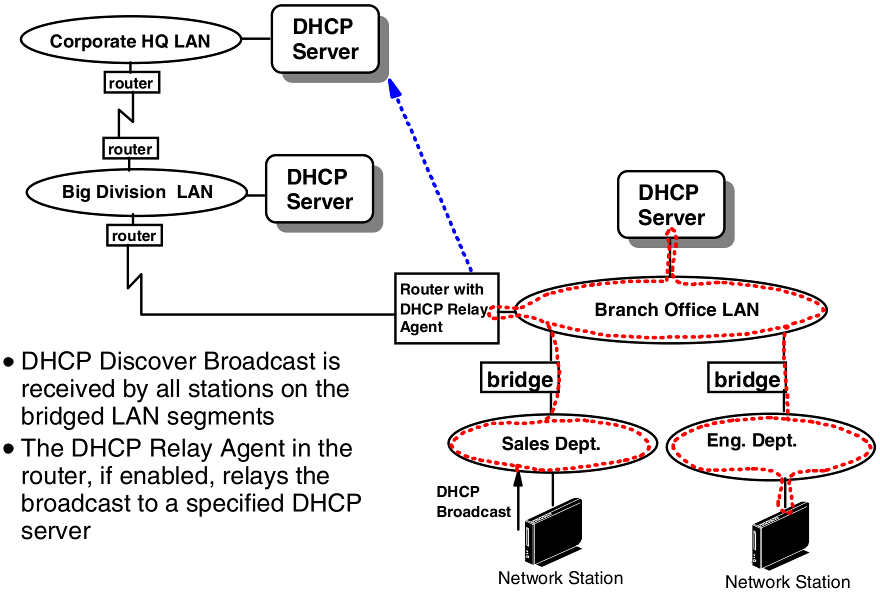
- Technical consideration depending on the topology of the network and the presence of routers and bridges

  A DHCP client makes its initial request to a DHCP server by sending a broadcast frame (since it does not yet have an IP address). Because broadcast frames typically do not cross routers, a DHCP server must be on the same LAN segment as its clients.

  However, routers that support a DHCP relay agent can be configured to accept DHCP broadcast frames and redirect them (using a unicast instead of broadcast) to a specific DHCP server anywhere in the network. This is what allows a DHCP server to be located at a corporate level for example and yet serve multiple LAN segments at the lowest levels in the network.

  For example, in Figure 39, the dotted line shows the travel of a DHCPDISCOVER broadcast issued by a Network Station in the Sales Department’s LAN segment. The broadcast travels on all three LAN segments and is received by the DHCP server on the branch office LAN, which presumably may respond depending on how it is configured. The broadcast is also received by the router on the Branch Office LAN. Because the router has a DHCP relay agent running, the agent looks up its configuration file to determine the address of the DHCP server that should be the target for this broadcast, and forwards the broadcast directly to that designated server (after placing its own IP address in the frame so that the reply will be sent to him).

  The server would also presumably respond depending on its configuration. However, it responds to the DHCP relay agent, which turns around and forwards the server’s reply to the station.



- DHCP Discover Broadcast is received by all stations on the bridged LAN segments
- The DHCP Relay Agent in the router, if enabled, relays the broadcast to a specified DHCP server

Figure 39. DHCP broadcast: DHCP Relay Agent

3.4.2.5 The number of DHCP servers to use

The three primary factors influencing this particular decision are:

- The number of centralized administration points that exist in the topology

  For the same reasons we identified above when discussing the location, there may be a need for one DHCP server per division, for example, if the corporate policy dictates that each division should manage its own network.

  In that case, the sphere of control of a DHCP server is only over the resources in the division. All branch office routers must have the ability to relay DHCP broadcasts to the division's DHCP server, as illustrated in Figure 40.

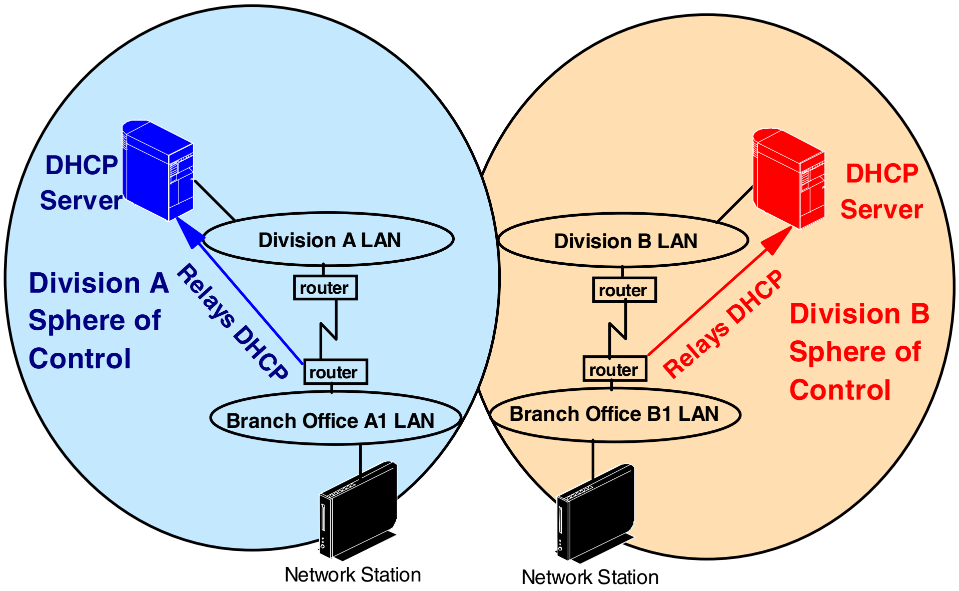


Figure 40. Divisional DHCP servers

On the other hand, if a there is to be a corporate DHCP server, all routers from all LAN segments must be able to relay DHCP broadcasts to the corporate DHCP server. Its sphere of control is over the entire corporate network, as illustrated in Figure 41.

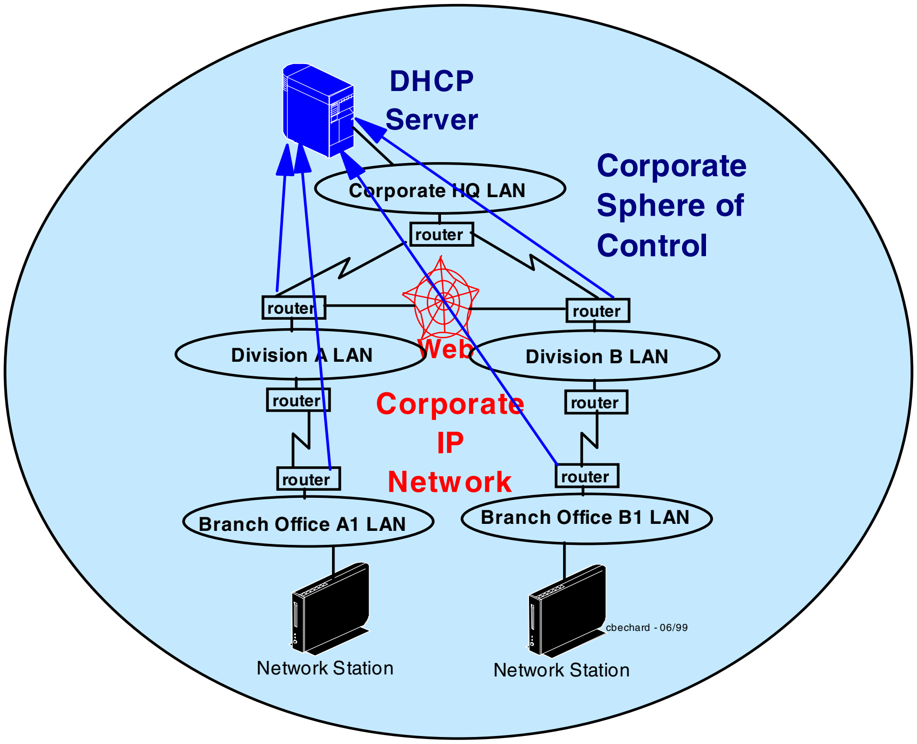


Figure 41. Corporate DHCP server

- The volume of DHCP activity that takes place, and therefore the total processing power required to handle DHCP requests

  Even in a highly centralized environment, where there would be only one DHCP server used for the entire organization, there may be reasons to use multiple physical DHCP servers when more processing power is required to handle the volume of requests. This becomes strictly a performance issue based on the DHCP traffic patterns and the processing power of the DHCP servers.

  Note that it is usually good to plan for DHCP request storms that may result from a power outage that causes many stations to send DHCP requests simultaneously.

- The amount of redundancy that you want to design into the topology in case of failures

  In both decentralized and centralized approaches, fail-safe mechanisms can be designed into the network topology to ensure continued operation in case of component failures. The amount of redundancy required determines whether one or more of the DHCP servers need to be supplemented with additional backup servers.

  This also becomes strictly a network design issue regarding redundancy. It must be evaluated in the context of the importance of these fail-safe mechanisms to the organization.

3.4.2.6 Co-existence considerations

In cases where the network contains a mix of stations running NSM V1R3 and V2R1, and all of these are managed using NSM, there are additional considerations to investigate.

First, note that the DHCP client in the V1R3 boot monitor always accepted the first acceptable DHCP offer it received if there were multiple DHCP servers on the same LAN segment. This meant that, in the case of unlisted support DHCP servers, the station could accept an offer from a DHCP server that did not serve all the options required by a network station to be able to boot properly.

In V2R1, the DHCP client only accepts offers that contain all the options that it needs to be able to boot properly. This makes it easier to mix DHCP servers offering responses to regular PCs and those offering responses to Network Stations. Therefore, you must be careful not to have multiple DHCP servers with unlisted support if V1R3 level stations are in the network.

Another problem is the co-existence of V1R3 and V2R1 stations in the DHCP server used does not support DHCP classes, such as the Microsoft DHCP server on Windows NT. If the DHCP client is not specifically identified through its MAC address, the only other way to distinguish between different types of Network Stations to send the correct value for option 67 (kernel path and file name) is to use the class of the Network Station. As far as we know, using a DHCP server with class support is the only way to permit coexistence of different types of stations when using unlisted client support.

3.4.2.7 Summary of DHCP considerations

In summary, most choices and decisions concerning DHCP are either guided by policies of centralization or decentralization or by the technical considerations derived from the network topology.

There are no easy rules that can be applied here. The key is to ensure that expertise is available in the areas of network design and administration to properly assess and analyze the needs of the enterprise.

3.4.3 Obtaining an operating system

Now that we have a DHCP facility in place that enables all our Network Stations to obtain an IP address and to communicate on the network as IP hosts, the next step is to enable them to obtain an operating system from a boot server.

Table 9 summarizes the key decisions to be made.

Table 9. Obtaining an operating system decisions

Choices	Factors to consider
Boot server platform	Choices are AS/400, RS/6000, Windows NT Server, flash card, a peer Network Station, a thin server, or actually any system that provides TFTP or NFS services.
Where to locate the servers	Proximity (how close it is) to the client, LAN media speed, network topology
Kernel download protocol	TFTP or NFS/RFS, download speed and server loading

Choices	Factors to consider
Number of servers for boot performance	Desired boot time in normal and emergency situations
Number of servers for redundancy	Desired boot time with some components having failed

3.4.3.1 Choosing a platform to use for a boot server

The answer to this question is not necessarily easy. The decision factors, in many cases, are similar to those we considered for the DHCP server.

However, for the boot server, the main decision criteria in most cases is the physical proximity factor (how close the server is to the client) between the boot server and its Network Station clients. This is because the size of the operating system file that we need to download is a few megabytes. We need to consider a facility that allows the file to be downloaded in a reasonable amount of time, without saturating the available network bandwidth to the point where nothing else can function.

Let us examine the possible platforms:

- The AS/400, RS/6000, or Windows NT server are traditional platforms that can be used as boot servers. In the case of the Windows NT server, you can use Windows NT Server 4.0 or the Terminal Server Edition of Windows NT Server 4.0. Note that an S/390 can only be used with the previous release of NSM (V1R3) and is no longer an option with V2R1.

  Whether these servers should be dedicated as boot servers depends mainly on their size and capabilities, on the number of Network Stations that they are asked to support, and on the other functions that they perform.

  For example, in a small network with few stations, it may be reasonable to expect that the server could be used for other functions. Caution must be exercised not to affect the stability of a server. In many cases, the more advanced functions a server performs, the lass stable it usually is, at least in small systems.

  In theory, Network Stations should not download their operating system on a regular basis since many remain powered on permanently. However, you must consider the case of power outages where the possibility exists that a large percentage of the stations may need to reboot at the same time, and analyze the possible impact of this peak activity.

  In large networks, the considerations are the same, but they apply to individual servers that serve a segment of the population of Network Stations.

  The advantage of using smaller boot servers, such as PCs, is that their lower cost allows the distribution of boot servers farther into the network, closer to their clients. The disadvantage is that it gives us more units to manage and maintain.

  Larger boot servers may be able to handle more clients, but they may have to be located farther from their clients, which may shift the cost of network bandwidth. In most cases, the boot server is not the bottleneck, but rather the network is. Therefore, an S/390 is not necessarily faster than a Windows NT system, but it is certainly more stable.

In summary, there are no easy or pre-established answers in this scenario. A network design and performance analysis must be performed to determine the optimal solution given a specific set of conditions.

- Flash cards are devices on which a copy of the operating system and other files, such as font files and native applications modules, can be stored. These devices can be used as a local storage device by inserting them into a Network Station.

  This allows a Network Station to rapidly load its operating system locally without having to use any network bandwidth. Remember that booting a station over a WAN link, although possible, is not recommended because of the large amount of data that needs to be transferred at boot time.

  The advantage is the speed of booting and the minimal impact on the network.

  However, the disadvantages are with the cards. They represent an additional cost, especially in terms of having to manage the distribution of the cards and the level of the software that is recorded on the cards.

  For V1R3, there are no tools that exist to manage flash cards and their contents. With V2R1, the situation is better because NSM now includes a configuration task that allows the administrator to specify which components are to be recorded on a flash card and when the flash cards should be updated.

  Actually, the use of flash cards negates many of the benefits inherent to thin clients where the software is managed and maintained in a central location (the boot server). *Exercise caution in choosing this option*.

- Peer booting is the ability to boot one Network Station from another Network Station that is equipped with a flash card.

  The advantages of this particular solution is that not every station needs to be equipped with a flash card. This reduces the cost of the cards and the number of cards that must be managed.

  The amount of bandwidth required is probably less of a concern since this is all local LAN traffic. However, there is a consideration in the number of stations that must be dedicated to act as boot servers. In other words, a Network Station can only support a restricted number of peer stations (10 to 15 is usually considered reasonable). Therefore, there may be a need to use more than one dedicated Network Station. On the other hand, compared to the cost of a PC server to use as a boot server, there may still be a cost advantage from an equipment point of view.

- Thin Servers are network components, such as the IBM 2212 Access Utility and the newer Whistle InterJet, that have the ability to act as a boot server by caching some of the files that are normally downloaded from a boot server. For more information about the Whistle InterJet, see the following Web site:
  `http://www.whistle.com/`

  In other words, the client makes its request from the thin server instead of the boot server. The thin server is responsible for getting the proper level of the files from the boot server in cases where it does not have the files or if the files are outdated (Figure 42 on page 64).

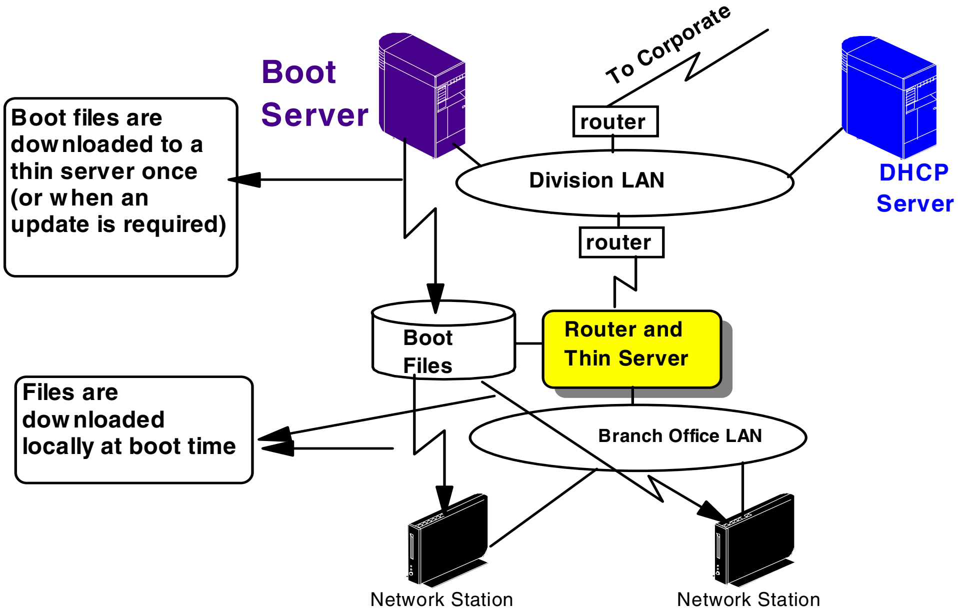


Figure 42. Using a thin server

The advantage is that thin servers, which normally have other functions such as routing, are typically located deeper into the network. Therefore, they are much closer to such clients as Network Stations. Load time and bandwidth utilization can therefore be optimized, without losing any of the advantages inherent to a central boot server.

3.4.3.2 Locating a boot server

As we already indicated in some of the previous summary discussions, the goal is to locate a boot server as close as possible to the clients. If not physically, we hope to locate the boot server at least in terms of bandwidth availability so that the download of the operating system occurs as fast as possible.

Let's look at a few typical or common cases.

Figure 43 shows an ideal example of a boot server located on each LAN segment where there are Network Stations. This scenario is viable when there is a large enough number of stations per LAN segment and where the server can be a relatively low cost server such as a PC or a thin server.

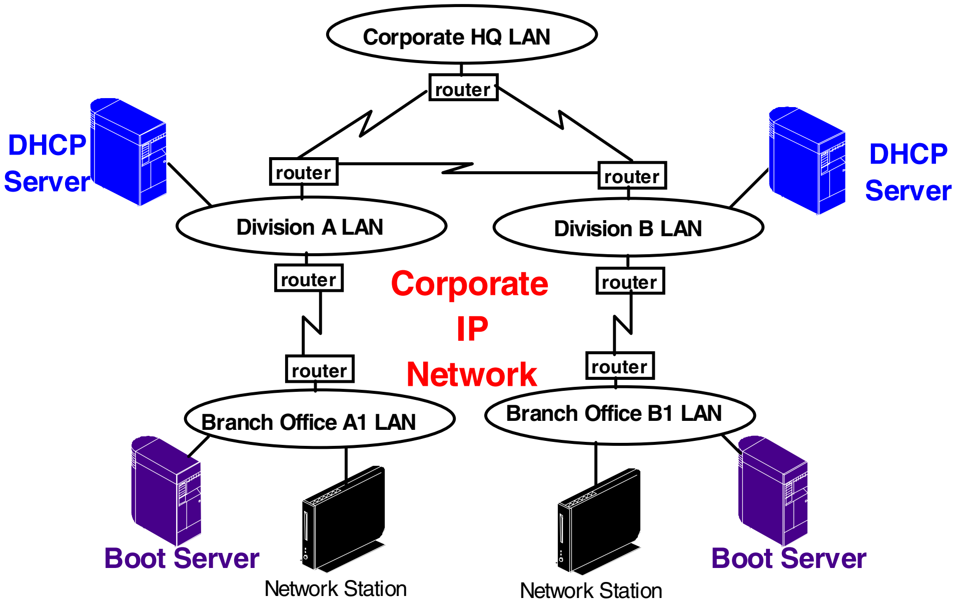


Figure 43. Local boot servers

Locating the boot servers at the division level instead, as illustrated in Figure 44, is not recommended. The presence of a WAN link considerably increases the boot time for a Network Station. For example, booting a Network Station across a 56 KB WAN connection may easily take from 10 to 20 minutes. This may only be acceptable if the WAN link between the routers is a high-speed link and if there is only a small number of stations in the branch office LAN.

Otherwise, consider using routers with thin server capability, flash cards, or peer booting.

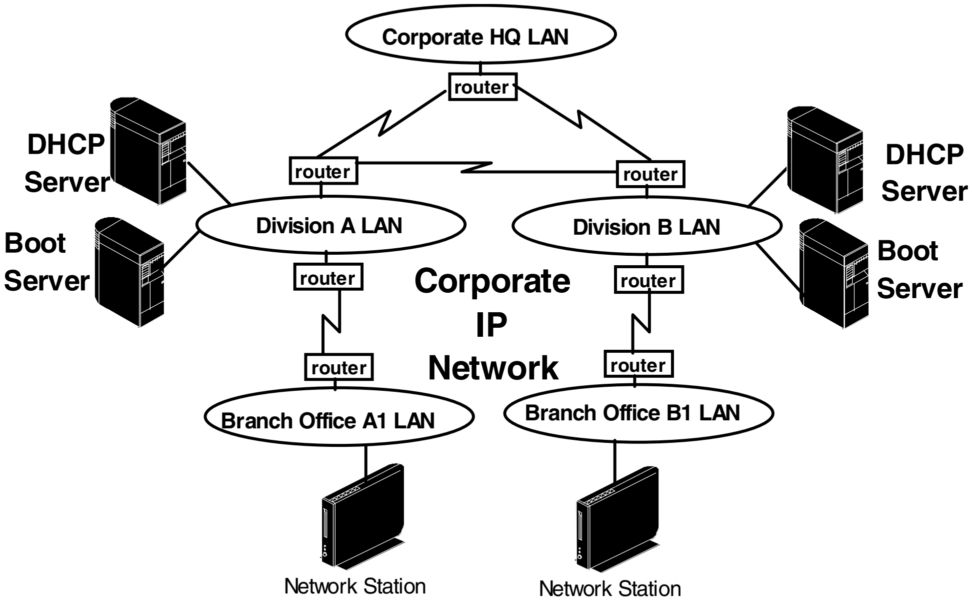


Figure 44. Remote boot servers

3.4.3.3 Which download protocol to use

The protocols that can be used to download the operating system are TFTP, NFS, and RFS. TFTP is not actually a remote file system, but a simple file transfer protocol. NFS and RFS are remote file system protocols and RFS is specific to the AS/400 system only.

Table 10. Kernel download protocols

Protocol	Windows NT	AIX	AS/400
TFTP	Yes	Yes	Yes
NFS	Yes	Yes	No
RFS	No	No	Yes

The choice of using TFTP or NFS is only for the download of the kernel. After that, NFS or RFS is required in all cases.

There are some performance reasons why TFTP may need to be considered in cases where, for example, the CPU load on a particular server is greater by using NFS.

Since performance issues can be complicated and require a lot of discussion, we have elected not to elaborate on this subject in this redbook.

3.4.3.4 The number of boot servers that are needed

There are two main factors to consider when designing for the optimal number of boot servers:

- What performance do you expect when all workstations are booting at the same time or when only a certain percentage of the stations are booting?

  The boot performance or the amount of time required for a station to boot is typically calculated as the time between power on and when a user can enter their user name and password.

  This boot time is influenced primarily by:

  – The speed and capacity of the connection between the station and the boot server and its current utilization from other applications. This is usually the bottleneck.

  – The number of stations that are simultaneously booting on the same media.

  – The capacity of the boot server and the number of stations that are simultaneously booting from the same server.

  In a normal operational environment, you do not expect all stations to boot at the same time because Network Stations are typically not powered off every day. However, they may be kept powered on because of their very low power consumption. If they are powered on every morning, this would likely be staggered over a certain period of time, such as between 8:00 a.m. and 9:00 a.m. when people come to work.

  However, there may be cases where a power failure in a particular facility would cause all stations to boot at the same time when the power comes back on. If that happens in the middle of the night and boot time increases dramatically due to the surge of stations booting at the same time, the impact is minimal, so long as all stations are finished booting when the day starts.

However, if this happens during the work day, the impact could be more severe. This should be a design point to consider when choosing the number of boot servers to be made available.

Performance numbers are not easily discussed without providing a significant amount of details on the specific environment that was used. Every little factor might produce a difference in the reported numbers (we do not provide performance data in this redbook).

- How much redundancy is required for fail-safe operation?

  In other words, if the main boot server goes down, consider whether other boot servers will be available to provide the same service.

  The boot monitor can be configured to automatically seek a second and a third boot server in the event that the primary boot server does not respond. As with all fail-safe or redundancy design, the primary goal is to provide an alternative while not necessarily expecting the same level of performance during an outage as is expected during normal operations.

  Only in cases of mission critical applications does the redundancy design have to perform at the same level as normal operations.

  In normal cases, you may consider combining redundancy with some performance considerations by designing with two boot servers for example, but splitting the load between the two servers and having these servers back each other up. Therefore, you direct half the population of stations to boot from server A (but designate B as the backup server) and the other half from server B (designating A as the backup server).

3.4.4 Obtaining terminal configuration files

Terminal configuration files contain the configuration parameters that determine the base operational characteristics of a particular station. These files are obtained from a terminal configuration server and are typically managed by the Network Station Manager application.

Table 11 summarizes the key decisions to be made.

Table 11. Terminal configuration server decisions

Choices	Factors to consider
Terminal configuration server platform	Choices are AS/400, RS/6000, Windows NT Server, flash card, a peer Network Station, or a thin server.
Platform of the server	Any platform that can run the Network Station Manager application. Choice may depend on existing and available equipment.
Location of the server	Easily located across a WAN link. Most likely determined by which group has the management responsibility or by other policies or topology considerations.
Terminal identifier	Choices are MAC address, IP address in decimal notation, or IP address in hex notation. MAC address is the only permanent identifier and the recommended identifier.

3.4.4.1 The type of server that can be used

The terminal configuration server can reside on any server that can run the Network Station Manager application. The choices are the AS/400, RS/6000, or

PC server (as well as the S/390 if using Network Station Manager prior to V2R1). The choice of platform will likely be influenced by the existing equipment at the location where you intend to place the configuration server.

3.4.4.2 Location of the terminal configuration server

Since the files to be downloaded are relatively small (compared to the size of the files that are downloaded from a boot server), the terminal configuration server can, in most cases, easily be located across a WAN link if required (Figure 45). This also provides the capability of centrally managing all configuration files.

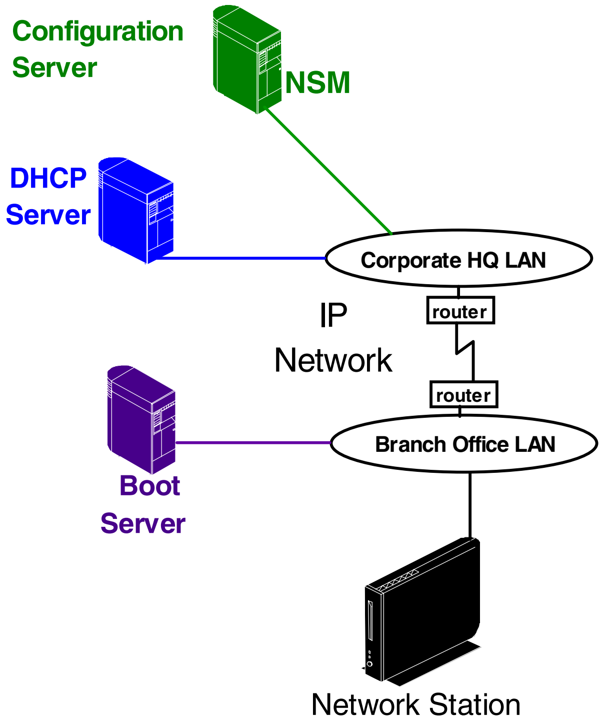


Figure 45. Terminal configuration server

This server can be located at the corporate level, if required, if the policies dictate that the terminal configuration files are to be managed at that level. On the other hand, a terminal configuration server could be located at the division level, one per division, and managed by the division network administrators.

The terminal configuration server does not have to be on a separate server by itself, and it can reside on the same server as the boot server. However, in that case, the Network Station Manager application needs to reside also on the boot server to change the configuration files on that server, or the files can be copied from a central NSM server shown in Figure 46.

Note that these files, because they contain system wide configuration parameters, are fairly stable. They are not changed often after the initial installation compared with the user configuration and preferences files, for example, which could change every day as users store their preferences.

The configuration files can also reside and be configured on another server where the Network Station Manager application resides. Then, they can be distributed by the network administrator to boot servers for the purpose of being downloaded to client stations (Figure 46).

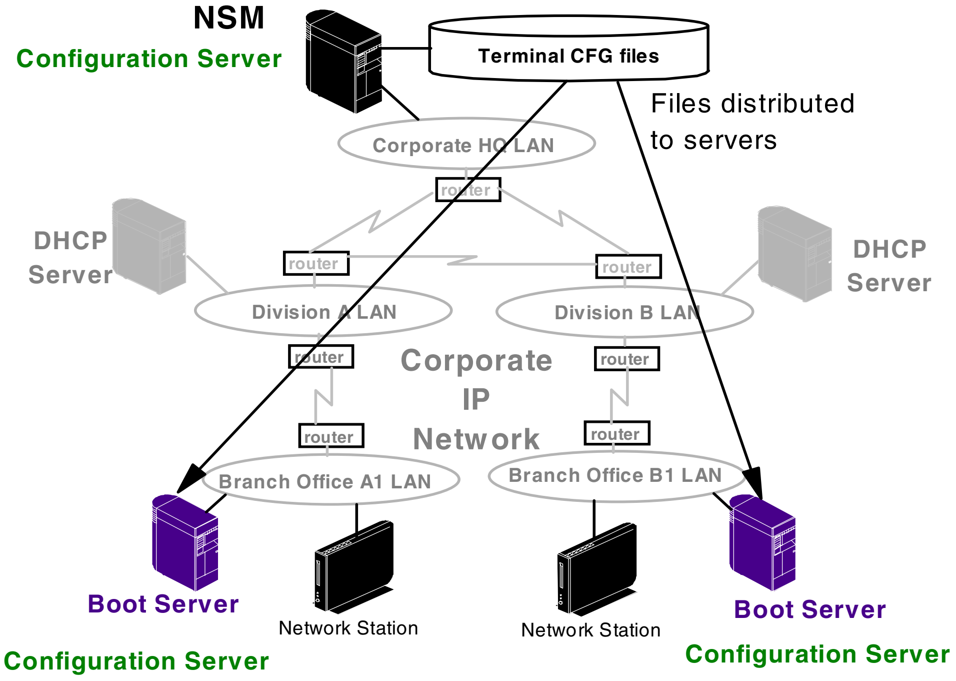


Figure 46. Distributing configuration files

3.4.4.3 Choosing the terminal identifier to use

When the station initially downloads its system configuration files, it can also download a terminal specific configuration file, if such a file exists.

In V1R3, it does this by first requesting a file with a name based on its MAC address. If that file does not exist, it tries a file name based on its IP address in the decimal notation (xx.xx.xx.xx), then a file name based on its IP address in hexadecimal notation, and finally a file name based on its IP host name.

This terminal specific configuration file is created by the Network Station Manager application when the administrator configures a parameter specific to the Network Station. At this point, the administrator is asked to select the workstation identifier.

The MAC address is the only piece of data that is permanent and that never changes. It is also the identifier used by the DHCP client to identify itself to the DHCP server.

However, in many cases, we simply do not want to keep track of MAC addresses, so we can use the IP address, but only in the case where the IP address is fixed. It cannot be used in cases where we use DHCP with dynamic address allocation. The same station does not always have the same address.

This is not necessarily an easy choice, but if we have to use terminal specific configuration files, then a choice must be made.

3.4.5 Contacting an authentication server

The next step in the boot process is the authentication of the user. In this step, you validate that the user name of the person logging on to a Network Station is authorized and that the password is correct.

For V2R1 (and for previous NSM releases), the authentication server also functions as the preferences server and the home server. Even though these functions can be logically separated, this separation has not yet been implemented in this level of the software.

Since the choice of separating these three functions is not yet implemented, we discuss the combination of these three servers.

Table 12 summarizes the key decisions to be made.

Table 12. Authentication server decisions

Choices	Factors to consider
Platform for the server	Same as those for the terminal configuration server
Location of the server	Same as those for the terminal configuration server
Location of user accounts	Policies, existing account information, and additional network traffic if located on another server

3.4.5.1 The type of server that can be used

The server platforms that can be used are the same as those discussed previously for the terminal configuration server. From this point on, we use the term *authentication server* to designate the authentication server itself, and the *preferences server*, and the *home server*, unless there is a need to specifically designate one of these three functions.

The authentication server must be a server where the Network Station Manager product can be installed because it needs:

- The Network Station Login server daemon to respond to requests coming from the Network Station Login clients when the user enters data in the login panel
- The Network Station Manager application to configure the group and user configuration files or profiles
- The NFS or RFS server component to allow Network Station clients to access files on the home server

3.4.5.2 Locating the authentication server

Here we have characteristics and conditions similar to those for the terminal configuration server. That is, the files to be downloaded are fairly small, making it possible to locate the server across WAN links. The network administration policies in place are likely to be the deciding factor in choosing the location of the authentication server.

In fact, since the authentication server actually manages user accounts, user preference files, and user home directories, it should be located and administered by the group or function that as the responsibility to manage these users.

In our sample corporation, whether we locate it at the corporate level or at the division levels is most likely dictated more by the existing network policies for user administration than by technical considerations.

Figure 47 illustrates an authentication server at the corporate level.

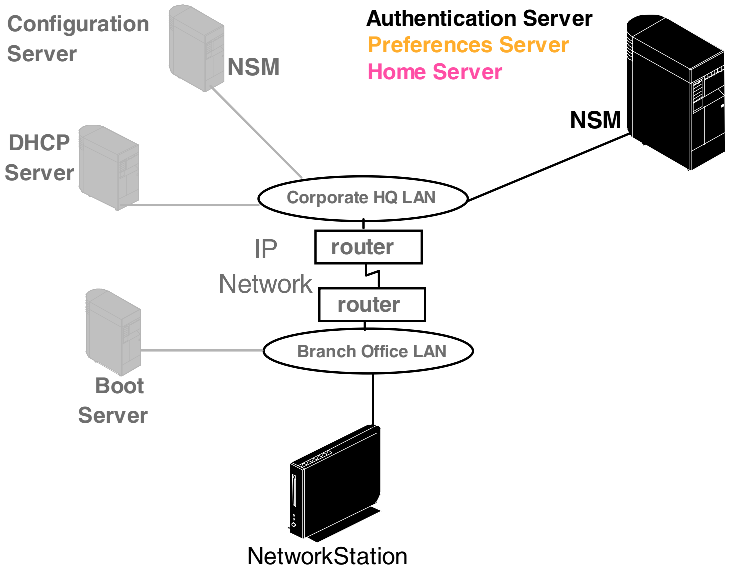


Figure 47. Authentication server

3.4.5.3 Locating user accounts

Note that we defined the authentication server as the machine where the Network Station Login server daemon resides. It is the responsibility of the login daemon to interact with the security system that is in place for these accounts on the server, but actual user account information could be located elsewhere.

For example, in a Windows NT environment, actual user accounts could be defined and located on a Windows NT Primary Domain Controller which is on a different machine than the Windows NT server used as the authentication server. In that case, the global group or groups that contain Network Station user accounts on the Primary Domain Controller are simply included in the local group on the authentication server. This is the group that the network station login server daemon checks when a request to authenticate a user is received, as shown in Figure 48 on page 72.

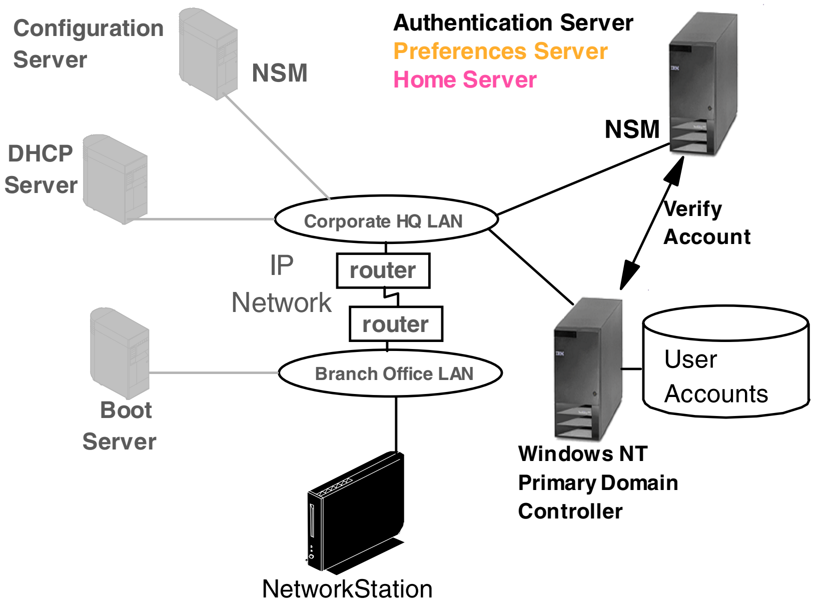


Figure 48. User accounts and the authentication server

This is an additional element of network design to be taken into consideration since additional network traffic is generated by the authentication server having to contact the PDC for validating users.

In the case where we want to delegate the user administration responsibility to the division's network administrators, it makes more sense to have an authentication server in each division. At this point, it may make sense to include the configuration server function as well on the same server (Figure 49).

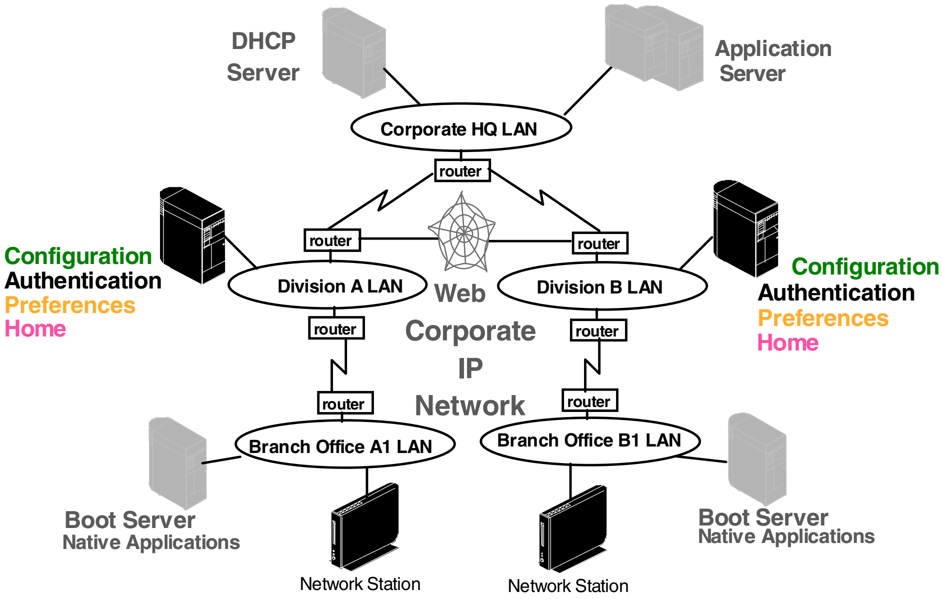


Figure 49. Authentication servers at the division level

3.4.5.4 User preferences server

The preferences server is where group specific and user specific configuration data is stored. Therefore, it requires that the Network Station Manager reside on that server to manage these configuration parameters.

User preferences configuration files are usually always on the same server as the authentication server since there are no NVRAM or DHCP options to separate the user configuration server from the authentication server.

3.4.5.5 Home server

The home server is where the user's home directory is located. Remember that there is no local storage on the Network Station. Therefore, when the user needs to store a particular piece of data, it is automatically stored in the home directory that belongs only to that user.

The home server is currently located on the authentication server. There is no facility that we know of to separate the home server from the authentication server.

3.4.6 Loading native applications

The native applications server is the server from which native application modules such as the 3270 emulator, 5250 emulator, or browser are downloaded. This is done for autostart at boot time or downloaded on demand when the user requests to start the application from the Network Station's desktop.

The key decision to be made is in regard to the location of the active application server. One factor to consider is that it must be the same as the boot server, although this is not a choice at this time.

3.4.6.1 Size of application modules

The application modules are located in the prodbase-mods subdirectory in a V1R3 system. Most modules are located in the /prodbase/X86/usr/bin directory in a V2R1 system.

Some of these applications sometimes be larger than the download of the operating system. The application server could have the same (or more) data to deliver to the client network stations, so the location of the application server is as important as the boot server.

Consider these points when comparing to the boot server:

- Once a Network Station has booted and downloaded its kernel, it may not do so again for quite a long time, that is until the next boot. However, applications can be loaded many times during the day as the user starts and stops applications.
- When a large number of stations boot at the same time, they create a large peak demand on the network and on the boot servers until all stations are up and running. The demand for application loading is more likely to be spread across the day because it is related to the users' activity level.

  There is also an initial peak and surge at boot time for downloading application code, in addition to the kernel, if many applications are configured to automatically be started at boot time. On the other hand, that load would be spread over time in sync with the users logging on.

Part of the network design effort should include an estimate of the pattern and frequency of application loading for a particular set of users if bandwidth is critical.

3.4.6.2 Locating the native applications server

With the V2R1 level of Network Station Manager code, the separation of the boot server and native application server has not been implemented. Therefore, the native application server (Figure 50) is always the same as the boot server, and all the considerations we discussed previously for the boot server apply equally.

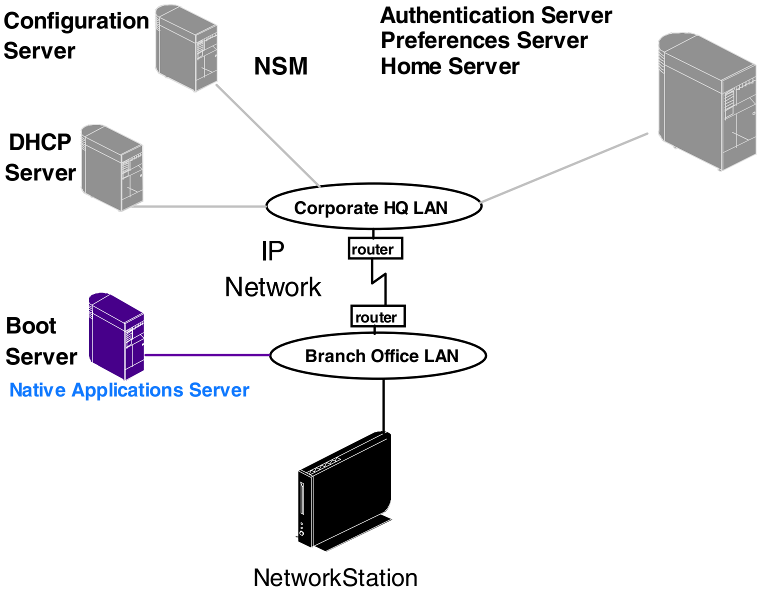


Figure 50. Native applications server

Note that the native applications server does not require the Network Station Manager application since it does not manage any configuration files.

3.4.7 Contacting applications servers

At this point, the user has their desktop up and running and the Network Station is fully functional. All the user needs to do is to start using applications.

Table 13 summarizes the key decisions to be made.

Table 13. Application servers

Choices	Factors to consider
Use native applications or applications on a MetaFrame type server	The features and functions required and the impact on the network of using one versus the other.
Autostart applications	Autostarts only applications that are always in use by the user
Close applications	Closed applications that will not be used for a significant period of time

Choices	Factors to consider
Use pre-configured sessions	Strictly a user-defined choice
Use Kiosk mode	If using a lobby environment or single application. Choose true kiosk mode (V2R1) or suppressed login (V1R3)
Domain Name Server	Access to a DNS server is required to resolve IP host names, if IP hostnames are used.
Proxies	If accessing host in an external network across a firewall, proxy servers are required.
Printers	Where are printers located; whether they are local or remote; which print datastream to use

The application modules (the code that executes on the Network Station) are downloaded from the native applications server as seen in the previous section. The actual target of the application is an application server somewhere out in the network. This can be seen in Figure 51 on page 76. Consider these examples:

- A 3270 emulator typically has an S/390 host as the target, although it may often use an intermediate gateway to reach the actual target host.
- A 5250 emulator session has an AS/400 system as the target host.
- A Web browser typically goes out to either the intranet or the Internet to access a variety of target IP hosts.
- A VTxxx emulator session may go to any IP host, either as a Telnet session or any other VTxxx session.
- An Independent Computing Architecture (ICA) session goes out to a WinFrame or MetaFrame server (multi-user Windows NT Server) to use Windows applications.
- An X terminal session typically goes out to a UNIX host or a WinCenter server (another way of reaching Windows applications on a multi-user Windows NT server instead of using ICA).
- A local application can print to a local or remote printer through the Line Printer Requestor (LPR) and Line Printer Daemon (LPD) daemons.
- You may also have home grown Java applications that need access to file servers, print servers, and so on.

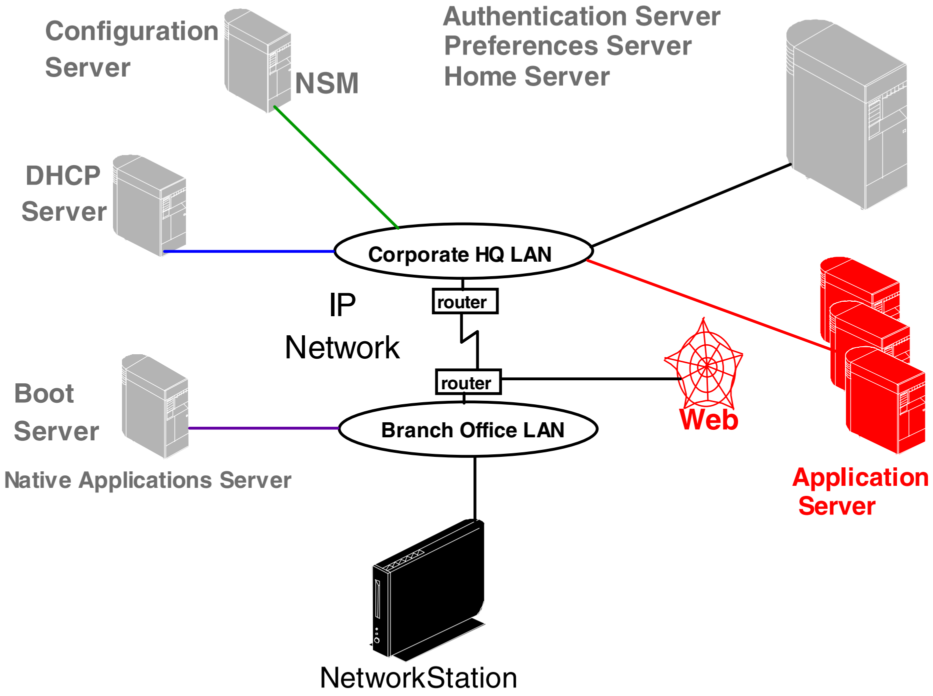


Figure 51. Application servers

3.4.7.1 Use native applications or applications on a Windows server

This section offers a few considerations to take into account when designing how the user accesses the applications server.

There are cases where certain applications can be run either natively or a similar application be used on a Windows server. For example, if the user needs a 3270 emulator, the choice is to use the native 3270 emulator available on the Network Station or to use the Personal Communications product (among others) on a Windows server through an ICA session.

The decision, in this case, is usually a trade-off between two factors:

- From a network traffic perspective, it is much more efficient to use the native emulator than to use PCOMM on the Windows server. The amount of traffic generated to run PCOMM on the Windows server and send the display output to the Network Station Monitor through the ICA session is a lot more than to use the native emulator.
- The only case where using the emulator on the Windows server instead of the native emulator should be considered is if the functions provided by the native emulator does not meet the end user's needs because they need special feature not supported natively.

3.4.7.2 Autostarting the application or letting the user initiate

If the user will always use a particular application, such as a 3270 emulator session to a CICS host, for example, it is preferable to configure the user desktop so that the application is always started after the user logs on. The advantage is that it makes it easier for the user.

In general, applications that are not used immediately should not be autostarted because they take up valuable memory resources even when not used but still reside in RAM. Remember that the Network Station is a real memory system and code loaded in memory is not swapped out to disk. Therefore, it is preferable to load applications only when they are required.

Should the user be instructed or encouraged to close applications that are no longer in use? We all have the habit, on PCs, to start applications and to leave them up when they are no longer immediately used. We know we might need it again later and it will be faster to access it if we leave it on the desktop. We also know it will get swapped out if not used. On a Network Station, the disadvantage is that a loaded application takes up valuable memory space. If there is enough memory available, there is no harm. On the other hand, closing an application means that it will have to be reloaded from the native applications server the next time it is required, which uses network bandwidth and takes more time.

It is probably best to design the amount of memory of a station to permit the simultaneous use of all the typical applications that a user always needs during the course of the day, so that they can leave those started all day. The other infrequent applications can then be started and closed when required.

3.4.7.3 Choosing to pre-configure target sessions

If a user, when starting a 3270 session, for example, always goes to the same target host and never starts a session with another host, it is preferable to give them an icon that starts the session directly with that host. This is opposed to a generic session where the user must enter the destination host name.

There is little impact of pre-configuring specific sessions. Not doing so only means that the user has more icons to choose in their applications folder.

3.4.7.4 Running in kiosk mode versus normal mode

The decision to run in kiosk mode really depends on the usage that will be made of the particular station.

There are three reasons for running a station in kiosk mode:

- The station is to be used in a lobby environment by anybody that is set up to run a specific application, such as a browser. It is a single purpose, single application machine, where we want to prevent it from being used for any other purpose.
- The station is to be used by a single user, but this user only requires one specific environment and never uses any other.

  For example, the station is used to replace an old 3270 terminal and the only display that the user needs to see after power on is the 3270 logo of their host VM session.
- You want to reduce the number of logins that a user has to perform. A station running in kiosk mode requires the user to perform a Network Station login.

In both cases, running in kiosk mode represents a simpler and more secure environment.

There are two ways to run in kiosk mode:

- **Suppressed login mode**: This is the mode that is used in NSM V1R3. The login process still takes place, but in an automated fashion, using a user name and password that has been pre-configured in a file instead of presenting a panel to the user asking for a user name and password. This is why it is called suppressed login, referring to the suppression of the display of the login panel as opposed to the suppression of the login process itself.
- **True kiosk mode**: This mode is a new feature of V2R1. The difference with the suppressed login mode is that there is actually no authentication of a user and no file containing kiosk user ISs and passwords. The access to the server is done in read-only mode, there is no desktop, and a single application gets auto-started and auto-restarted if necessary.

3.4.7.5 Configure a DNS for name resolution

In most cases, access to a Domain Name Server (DNS) is required in order to resolve IP host names into IP addresses. Most typical IP networks today are already setup with a Domain Name System.

In that case, the only decision to be made is whether to obtain the DNS configuration data (IP address of a DNS server and default IP domain name) from the terminal configuration server or from the DHCP server.

We prefer the DHCP server method because it is more flexible, and we can more easily control the information. However, in cases where DHCP is not used (NVRAM), the configuration server method is the only remaining choice.

What if you do not have a DNS system in place? If the environment is a small intranet network with few hosts, the host names can always be configured in one of the configuration files on the terminal configuration server (hosts.nsm for V1R3 and /prodbase/{ppc or X86}/etc/hosts for V2R1) so that all stations have a way of resolving specific pre-determined IP host names.

A typical situation is even in situations where there is a DNS system available. It may not contain the names of all clients such as Network Stations, but only the names of print servers and file servers, or other servers, because these are accessed frequently by clients. Clients may not typically communicate directly with each other.

In some cases, in V1R3, this may cause some slight performance problems in cases where DNS lookups are used. For example, at boot time, the station usually does a DNS reverse name lookup for the boot server and for its own address. Also, when the station receives a print request, it does a DNS reverse name lookup for the sending host and for itself.

If host names for clients are not used, dummy names may simply be placed in the hosts file so that the DNS request is satisfied right away.

3.4.7.6 Configuring proxies for access to external networks

If the stations are on an intranet and they need access to external networks by going through a firewall, there is a need to configure either proxy servers or a SOCKS server. Figure 52 explains the difference between proxy servers and SOCKS servers.

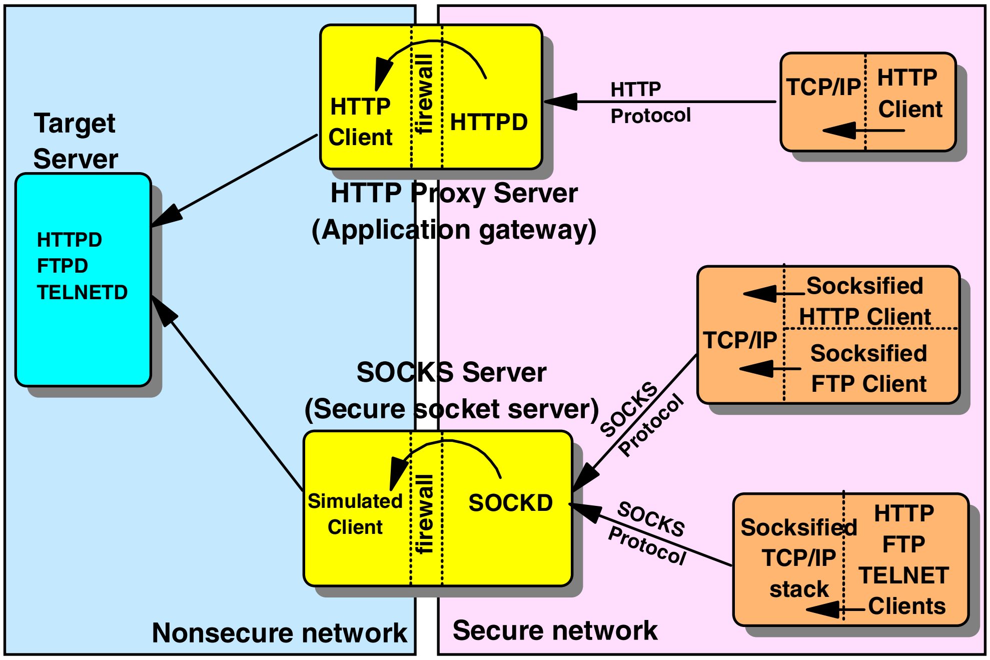


Figure 52. SOCKS and PROXY servers

In the top portion of Figure 52, we see on the right-hand side an HTTP client, such as a Web browser, located in the secure network part. It needs to communicate with the HTTPD service on the target server located in the nonsecure (public) network.

The client specifies the address of an HTTP proxy server. That server actually functions as an application gateway. An HTTPD daemon receives HTTP requests from clients on the secure side of the network. It also functions as an HTTP client on the nonsecure side of the network, effectively becoming the actual client of the target HTTP server (and acting on behalf of the real client, which is on the secure side of the network).

Therefore, as far as the target HTTP server is concerned, it is only aware of the HTTP proxy server client. It has no knowledge of the real client where the original HTTP request actually originated.

In the bottom portion of the diagram, a SOCKS server is used instead of a proxy server. In this case, the HTTP client contains a SOCKS client that communicates with a SOCKS server to transmit the actual HTTP request. On receipt of the request, the SOCKS server transmits the request across the firewall in a secure manner so that the target is also unaware of the actual real client.

In a proxy server, the HTTP application actually executes on the proxy server. In the case of a SOCKS server, the HTTP application remains on the actual client, and the SOCKS server provides a secure passthru pipe.

In the case of a SOCKS client, the client application itself can be “socksified” and communicate with the socks server. Or, the entire TCP/IP stack can also be socksified, which then permits all applications to communicate with a SOCKS server.

3.4.7.7 Access to local and remote printers

Applications running on the Network Station can send print output either to a Network Station attached printer (local printer) or to any other IP host that supports LPD (TCP/IP printing), including another Network Station. A local printer can be attached to the parallel port or to the serial port of the Network Station.

The Network Station can also receive print requests from any other IP hosts that support LPR and print locally. It cannot reroute this output received from a remote host to another remote printer because it actually does not have any local spooling capability due to the lack of local disk storage.

In Figure 53, we see that an application on the Network Station can print to a local printer (1). Also, if a Network Station does not have its own printer attached, it can send printed output to a printer attached to a peer station (2). Equally, it can send printed output to any remote printer such as a printer on the branch office LAN (3), as shown, or a printer attached to a remote host (4).

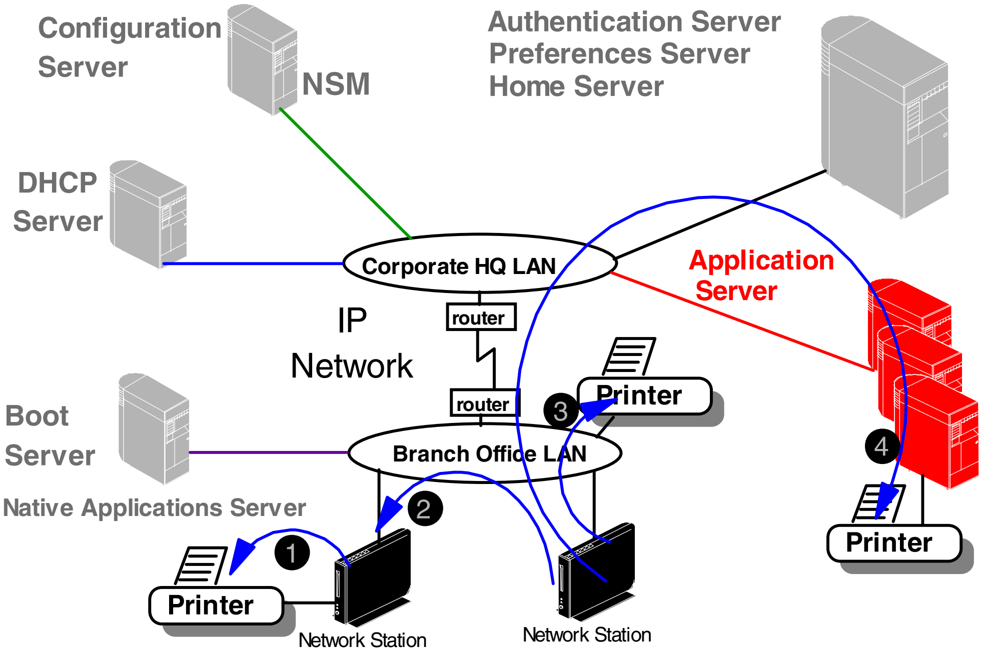


Figure 53. Printing from a Network Station

How does that work? Figure 54 summarizes the major printing components on the Network Station. When an application makes a print request, it is presented with a printer selection panel on which appear all the printers that have been defined as accessible to this station (as configured in Network Station Manager).

If a local printer is chosen, the output is sent to the local Print API. If a remote printer is chosen, the request is sent to the LPR daemon (LPRD), which routes the request to the selected remote printer or print server.

Finally, a print request coming from another IP host, such as another Network Station for example, is received by the LPD daemon which routes the request to the local printer.

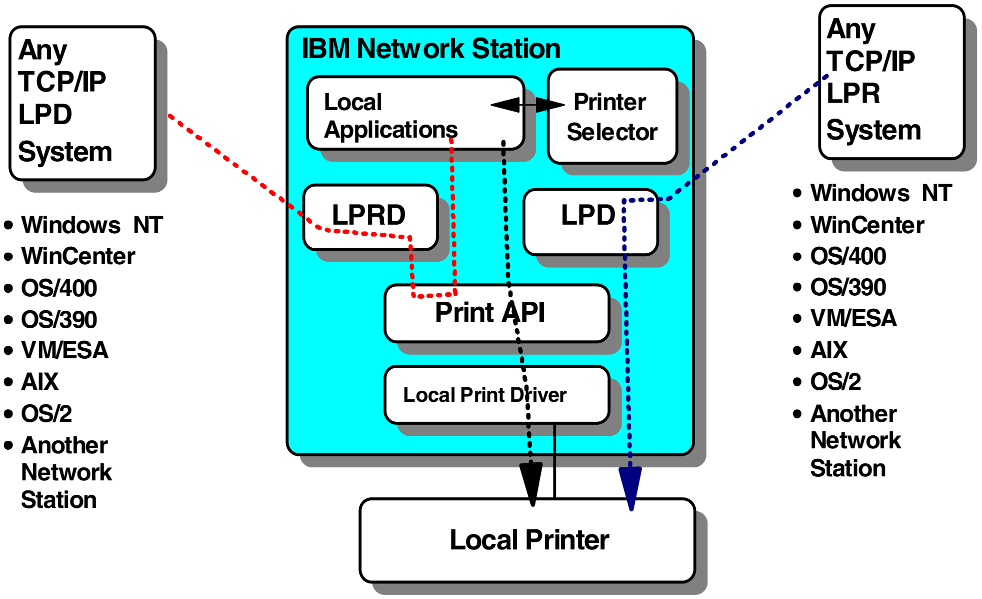


Figure 54. Printing overview

Most local applications on the Network Station support Postscript output. Only the 3270 and 5250 emulators also support PCL, as indicated in Table 14.

Table 14. Native applications print output capabilities

Application	V1R3	V2R1
Browser	Postscript	Postscript
Java Application	Postscript	Postscript
3270 Emulator	Postscript, PCL, ASCII	Postscript, PCL, ASCII
5250 Emulator	Postscript, PCL,ASCII	Postscript, PCL, ASCII
VTxxx Emulator	ASCII	Postscript, PCL, ASCII

If you have mainly PCL capable printers and you still want to use these with the browser, for example, you can use a Print Transform utility on a host such as an AS/400 host.

This is illustrated in Figure 55 on page 82 where an application generates Postscript, and sends it to a specific print queue on the AS/400 host. Here it is directed to be transformed to PCL output, which is rerouted to an output queue that redirects the PCL output to the Network Station. This effectively allows a PostScript generated output to be sent to a PCL printer.

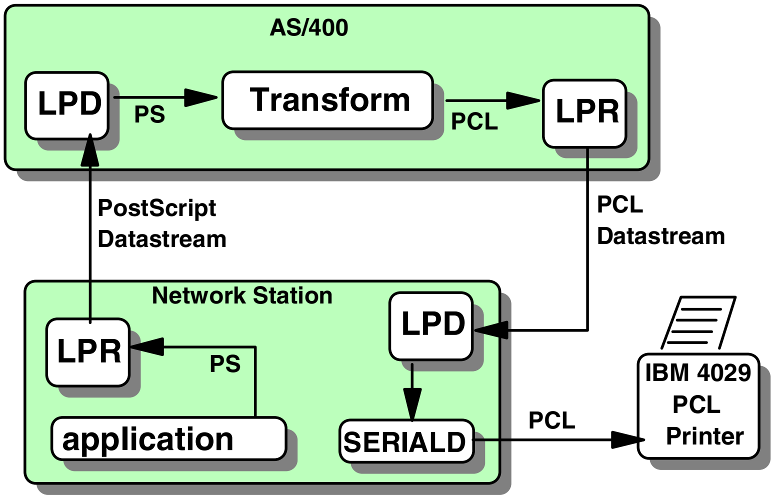


Figure 55. Using Print Transform on a remote host

Chapter 4. Installation and server setup

The installation of the V2R1 Network Station Manager is for the most part a straight forward task.

Note: In the AS/400 environment, there is a new graphical V2R1 Setup Wizard available which is a plug-in to the AS/400 Operations Navigator. This GUI interface can be used to configure the AS/400 environment for the Network Stations. The rest of this chapter looks at this new feature for V2R1 Network Station Manager.

For installation and server setup instructions, please refer to the IBM Network Station Manager manuals shown in Table 15. All updates to these manuals can be found at: `http://www.pc.ibm.com/us/networkstation/tech_library.html`

Table 15. Installation and server setup references

Information name	Information description
Installing IBM Network Station Manager for AS/400, SC41-0684	Describes the installation and simple configuration of an AS/400 Network Station environment. It is shipped with the IBM Network Station Manager licensed program.
Installing IBM Network Station Manager for RS/6000, SC41-0685	Describes the installation and simple configuration of an RS/6000 Network Station environment. It is shipped with the IBM Network Station Manager licensed program.
Installing IBM Network Station Manager for Windows NT, SC41-0688	Describes the installation and simple configuration of a Windows NT Network Station environment. It is shipped with the IBM Network Station Manager licensed program.
Using IBM Network Station Manager, SC41-0690	Describes the basic tasks for managing user desktops through the IBM Network Station Manager program. It is shipped with the IBM Network Station Manager licensed program.
IBM Network Station Advanced Information V2R1	Describes tasks and information beyond a basic installation and configuration of your Network Station environment. This information is only available at: `http://www.pc.ibm.com/us/networkstation/tech_library.html`

4.1 AS/400 V2R1 installation: The basics

Installing the V2R1 code on your server system involves many steps. In general, it is a good idea to have both the V2R1 CD and the Group PTF CD available before you start installing the 5648C07 (V2R1) product. The Group PTF (SF99083) contains PTFs for both the OS/400 and the IBM Network Station Manager (5648C07).

SF99083 can be ordered electronically with the AS/400 command:

```
SNDPTFORD SF99083
```

If the order is successful, you should receive the CD in a few days, or longer, considering from where it is shipped.

Once you have both the V2R1 code and the group PTF CDs, you will be ready to start the installation. As an overview, the following steps are performed:

1. Install the Group PTF CD (SF99083) on your system. This ensures that any pre-requisite PTFs, required for the V2R1 installation, are loaded.
2. IPL the AS/400 system if some PTFs, from step 1, require an IPL to be applied.
3. Install the V2R1 code with the Restore Licensed Program (`RSTLICPGM`) command. You may need to run this command twice depending on the number of license program options you are planning to install.
4. Install the Group PTF CD (SF99083) on your system. This loads and applies the PTFs that apply specifically to the 5648C07 product.
5. Determine if the AS/400 V2R1 Setup Wizard needs to be run. Refer to the next section.

Note

These steps are only a general guideline. To install the V2R1 code successfully, refer to *Using IBM Network Station Manager V2R1*, SC41-0690. This manual is also available on the Web at:
`http://www.pc.ibm.com/us/networkstation/tech_library.html`

Refer to the following additional resources:

- *Installing IBM Network Station Manager for AS/400*, SC41-0684
- *Client Access Express For Windows Setup*, SC41-5507
- Informational APAR II11759
- The following sites on the Internet:
  - `http://www.pc.ibm.com/us/networkstation/tech_library.html`
  - `http://www.as400.ibm.com/clientaccess/`
  - `http://www.as400.ibm.com/infocenter`

4.2 V2R1 Setup Wizard: When to use

When the V1R3 IBM Network Station Manager code was available for the AS/400 system, a Setup Assistant program was included. This Setup Assistant was a tool for setting up the AS/400 system for use with the Network Stations. Although its use was recommended, this Setup Assistant program was not mandatory to run. If the system administrator chose not to run the Setup Assistant program, then those program tasks would need to be run manually. Although it is not mandatory to run the V2R1 Setup Wizard in every IBM Network Station environment, it is normally recommended. See the exceptions listed in the following paragraphs.

Note

The AS/400 Setup Assistant in Version 1 Release 3 is beyond the scope of this redbook. If you require information on this topic, refer to *IBM Network Station Manager Installation and Use*, SC41-0664, and *AS/400 IBM Network Station - Getting Started*, SG24-2153.

With the introduction of the V2R1 code, a Network Station Setup Wizard program is included to assist with configuring the AS/400 environment for your Network Stations. If the Setup Wizard is run, certain tasks will be done on your AS/400 system. If the Setup Wizard, for any number of reasons, is not run, the system administrator will need to ensure that the Setup Wizard tasks are invoked manually.

If you are currently running the V1R3 IBM Network Station Manager code on your system and you need to install the V2R1 IBM Network Station Manager code, it is time to decide if the AS/400 Setup Wizard needs to be run. You should choose to run the Setup Wizard if you have one of these environments:

- Network Station clients using only the NVRAM method of booting
- Network Station clients using both the NVRAM and BOOTP methods of booting
- Network Station clients using only the BOOTP method of booting

If you have clients currently booting with DHCP, you may be in one of these situations when installing V2R1 Network Station Manager on your system:

1. Network Station clients are being added to a new DHCP subnet (one that is *not* already defined in you DHCP configuration).
2. Network Station clients are being added to an existing DHCP configured subnet.

If your environment fits into point 1, you should run the V2R1 Setup Wizard. If your environment fits into point 2, you can decide whether you are going to run the V2R1 Setup Wizard.

Section 9.3.3, “Scenario 6: V1R3 and V2R1 clients using DHCP” on page 270, demonstrates such an environment where a new 2800 model is installed on the existing LAN and DHCP is the boot protocol being used.

4.3 Installing the AS/400 Setup Wizard

For a successful installation of the Wizard, complete the following process:

1. Before installing the AS/400 Setup Wizard on your PC, you should check that Client Access Express V4R4 has the required Service Pack installed. To verify the service pack level, you need to view the Client Access properties. This can be achieved by first double-clicking the **IBM AS400 Client Access** icon located on the windows desktop. Double-click the **Client Access Properties** icon.
2. Now that you have accessed the properties, select the **General** tab. Under the General tab, you see the Service level ID (Service Pack version).

As shown in Figure 56, you need a PC loaded with the required software.

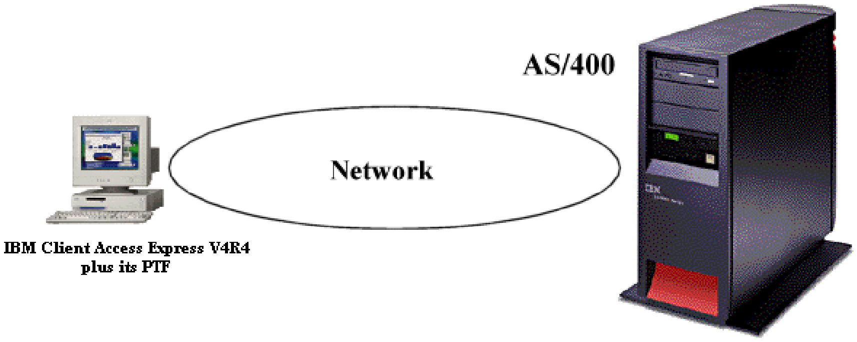


Figure 56. PC with Client Access Express attached to the AS/400 system via a network

3. Double-click the **IBM AS/400 Client Access** icon (Figure 57). The window shown in Figure 58 appears.

> **Note**
>
> When installing Client Access Express, we normally recommend that you temporarily disable any anti-virus programs you have on Windows 95 (such as Norton AntiVirus). Ensure that it is removed from your Start Up programs and that the "auto-protect" feature is disabled until after you have completed the installation of Client Access Express.

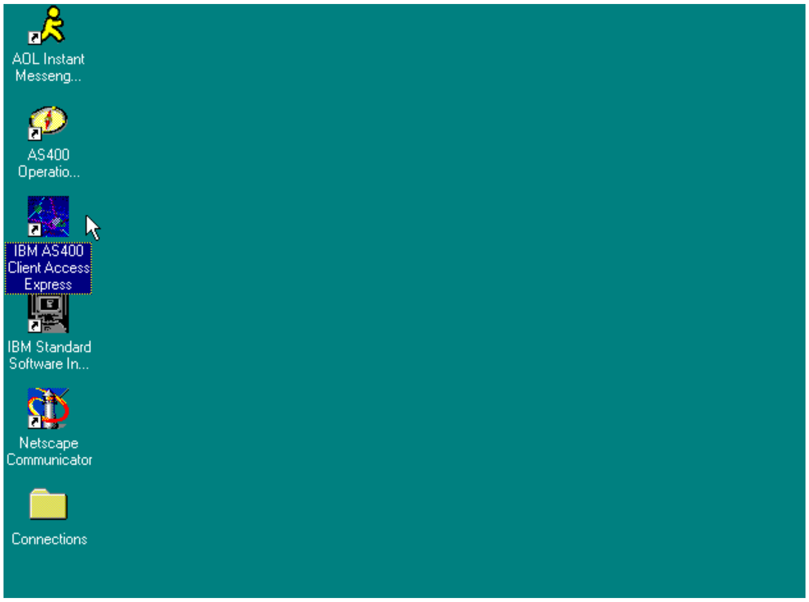


Figure 57. Verifying the Client Access service pack level

4. Double-click the **IBM Client Access Properties** icon.

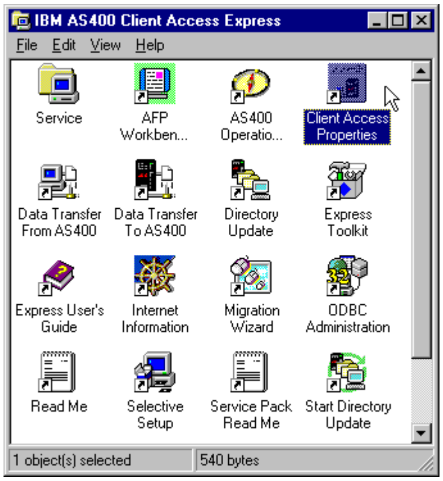
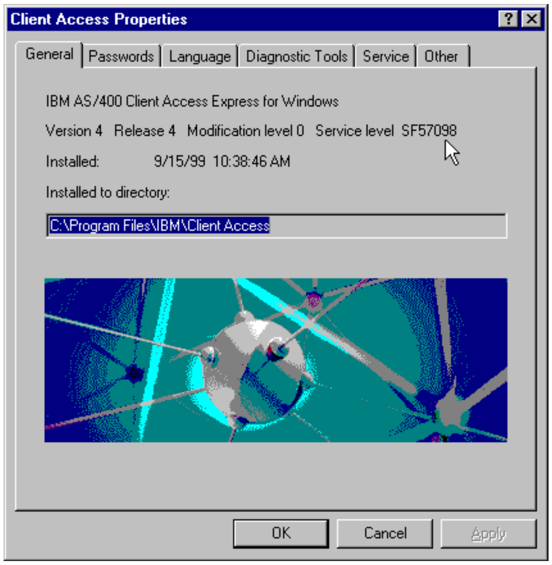


Figure 58. Accessing the IBM Client Access Properties.

Figure 59 displays the properties of the IBM Client Access. By checking its Service Level ID (SF57098), you can determine which service pack is installed. In this example, the service level is SF57098, which corresponds to Service Pack 2.



IBM AS/400 Client Access Express for Windows

Version 4 Release 4 Modification level 0 Service level SF57098

Installed: 9/15/99 10:38:46 AM

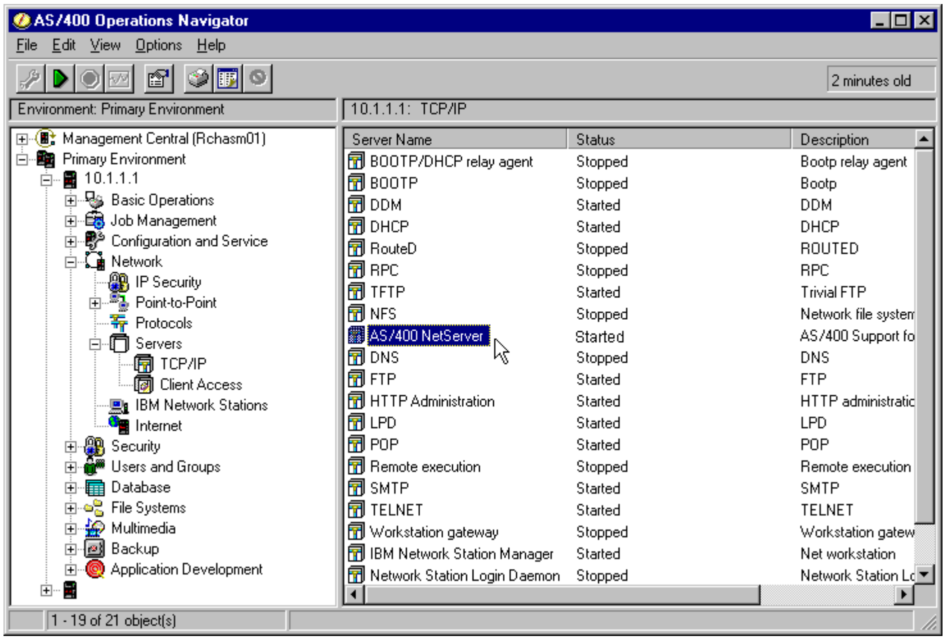
Installed to directory:

C:\Program Files\IBM\Client Access

Figure 59. IBM Client Access Properties

5. Start AS/400 NetServer by following these steps:

   a. Open Operations Navigator.
   b. Expand the system.
   c. Expand **Network** and then **Servers**. Double-click **TCP/IP**.
   d. Under Server Name, look for **AS/400 NetServer** (Figure 60 on page 88). Verify that its status is Started. If the status is Stopped, right-click on **AS/400 NetServer**, and choose **Start**.



Server Name	Status	Description
BOOTP/DHCP relay agent	Stopped	Bootp relay agent
BOOTP	Stopped	Bootp
DDM	Started	DDM
DHCP	Started	DHCP
RouteD	Stopped	ROUTED
RPC	Stopped	RPC
TFTP	Started	Trivial FTP
NFS	Stopped	Network file system
AS/400 NetServer	Started	AS/400 Support fo
DNS	Stopped	DNS
FTP	Started	FTP
HTTP Administration	Started	HTTP administratio
LPD	Started	LPD
POP	Started	POP
Remote execution	Stopped	Remote execution
SMTP	Started	SMTP
TELNET	Started	TELNET
Workstation gateway	Stopped	Workstation gatew
IBM Network Station Manager	Started	Net workstation
Network Station Login Daemon	Stopped	Network Station Lo

Figure 60. Verifying that NetServer is started

6. To install the AS/400 Setup Wizard, perform the following tasks:

   a. From the Windows desktop, click the **Start** button on the menu bar.

   b. Select **Programs->IBM AS/400 Client Access Express->Selective Setup** (Figure 61).

   c. You are then presented with a Selective Setup screen that allows you to add or remove components (not shown). Click **Next**.

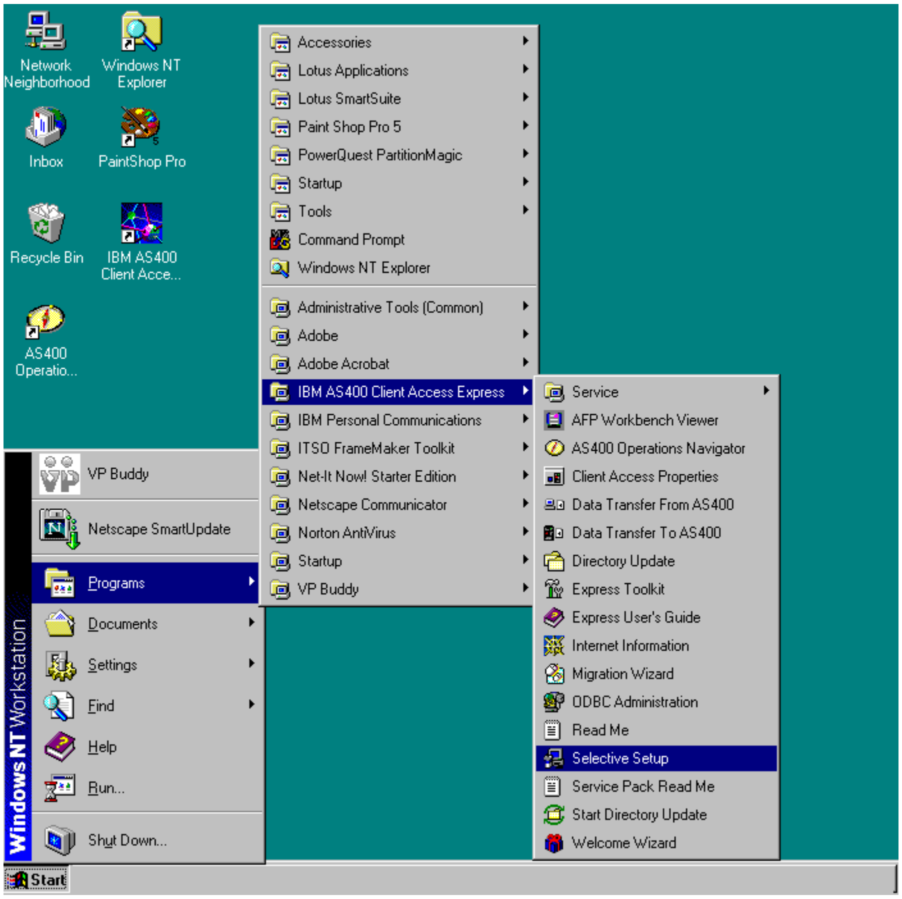


Figure 61. Accessing AS/400 Client Access Selective Setup

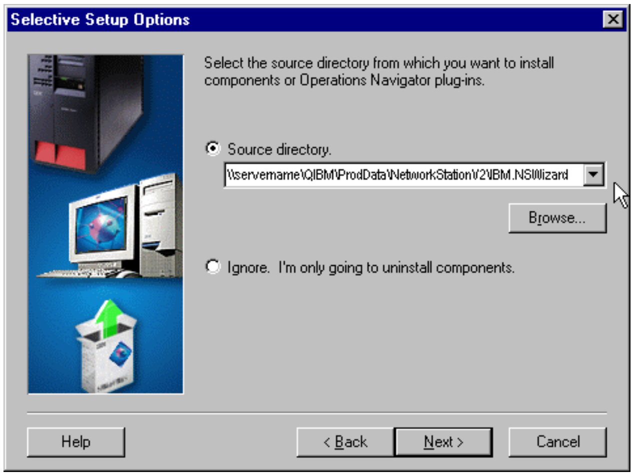
7. When prompted, specify the source directory from which the AS/400 Setup Wizard is going to be installed, as shown in Figure 62 on page 90. The source directory path is:

   `\\servername\QIBM\ProdData\NetworkStationV2\IBM.NSWizard`

   Here, *servername* is either the IP address of the AS/400 interface or its host name. Sometimes you may need to use the Windows Map Network Drive utility before Selective Setup can access the path that you are trying to specify.

   Selective Setup then checks for presently installed components (not shown).

   Click the **Next** button.


Selective Setup Options

Select the source directory from which you want to install components or Operations Navigator plug-ins.

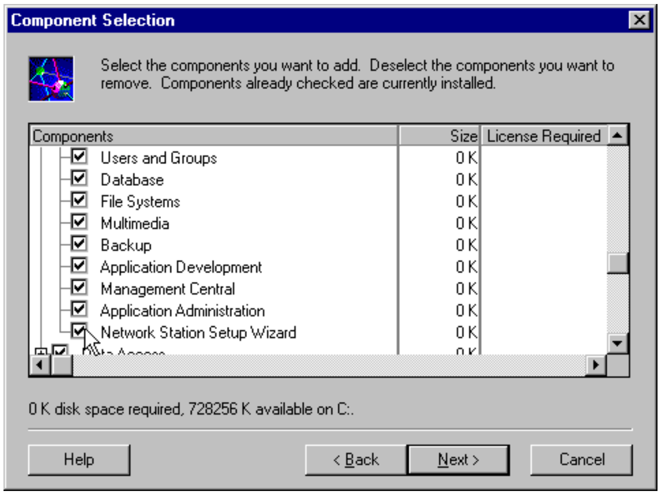
● Source directory.

\\servername\QIBM\ProdData\NetworkStation\V2\IBM.NS\Wizard

○ Ignore. I'm only going to uninstall components.

Figure 62. Specifying the path from which the IBM Setup Wizard is going to be installed

8. At the Component Selection dialog (Figure 63), we expand the AS/400 Operations Navigator. Under AS/400 Operations Navigator, select the **Network Station Setup Wizard** box.


Component Selection

Select the components you want to add. Deselect the components you want to remove. Components already checked are currently installed.

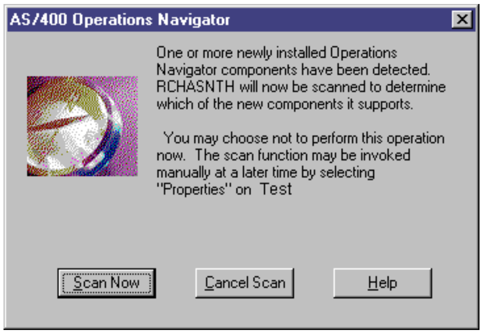
Components	Size	License Required
☑ Users and Groups	0 K	
☑ Database	0 K	
☑ File Systems	0 K	
☑ Multimedia	0 K	
☑ Backup	0 K	
☑ Application Development	0 K	
☑ Management Central	0 K	
☑ Application Administration	0 K	
☑ Network Station Setup Wizard	0 K	

0 K disk space required, 728256 K available on C:.

Figure 63. Selecting the Network Station Setup Wizard

Click **Next**

9. Click **Scan Now** to let the Operations Navigator scan (detect) the new plug-in (AS/400 Setup Wizard) (Figure 64).



One or more newly installed Operations Navigator components have been detected. RCHASNTH will now be scanned to determine which of the new components it supports.

You may choose not to perform this operation now. The scan function may be invoked manually at a later time by selecting "Properties" on Test

Figure 64. Scanning for Plug-Ins

If you decide to cancel the scan, click **Cancel Scan**. You can perform it at a later time by accessing the AS/400 properties display, selecting the **Plug-Ins** tab and clicking the **Rescan** button.

4.4 Using the Network Station Setup Wizard on your AS/400 system

On the AS/400 platform, the green-screen Setup Assistance (STRNSSA) is now replaced by the Network Station Setup Wizard, which is a plug-in to the AS/400 Operations Navigator. The Network Station Setup Wizard is a GUI utility that runs on a PC loaded with V4R4 Client Access Express For Windows, plus its service pack. The Wizard is used to configure the AS/400 environment for the Network Stations.

Table 16 displays the differences between Setup Assistance (STRNSSA) and the Wizard.

Table 16. Differences between the Network Station Setup Wizard and Setup Assistance

Network Station Setup Wizard	Setup Assistance (STRNSSA)
Configures TCP/IP	Configures TCP/IP
Configures DHCP	Configures BOOTP
Can be executed several times to create additional subnets	Could only be fully executed once
Is a GUI interface	Performs through a native 5250 application

Configuring TCP/IP and DHCP settings are Network Station Setup Wizard’s primary functions. Figure 65 on page 92 illustrates some of the tasks that the AS/400 Setup Wizard is designed to perform in our AS/400 system to ensure a successful setup of the Network Station Manager.

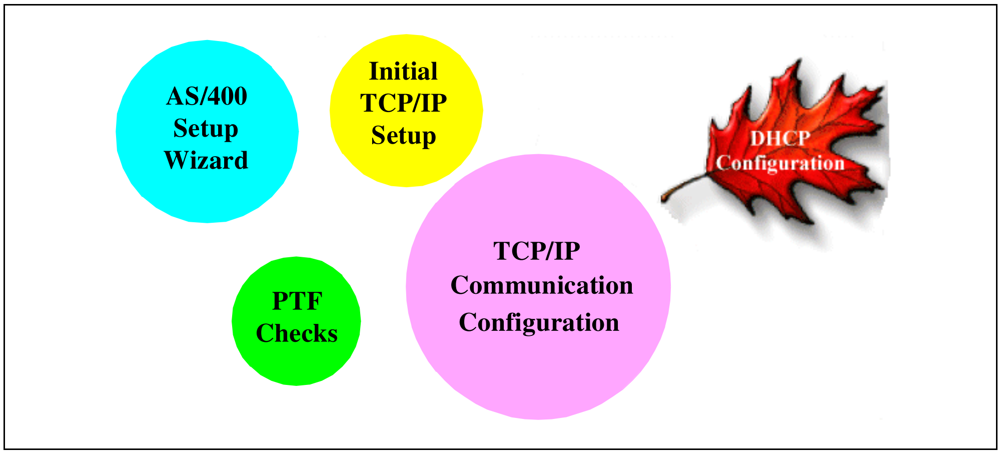


Figure 65. AS/400 Setup Wizard tasks

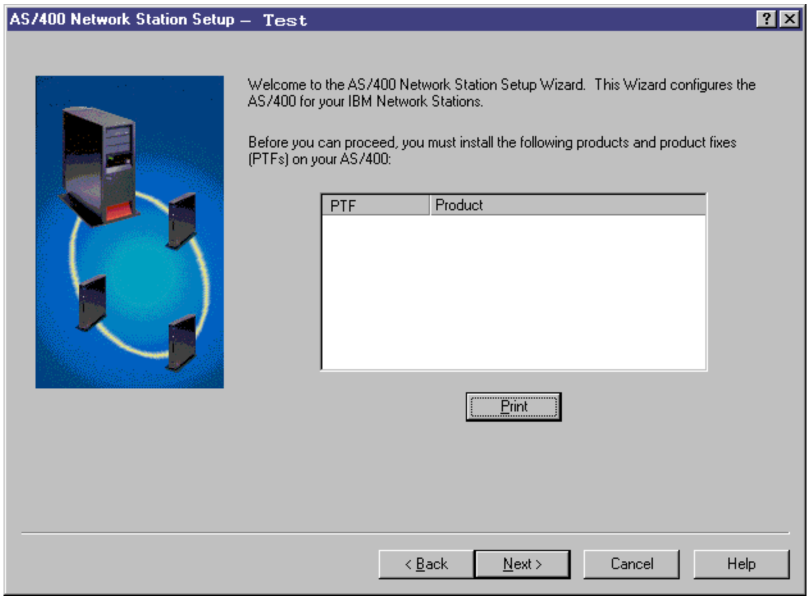
To understand the scope of the Setup Wizard, the following sections describe the various tasks that it can handle. As documented in the example provided in 4.5, “Navigating with the Setup Wizard through a sample configuration” on page 107, when used in a real environment, the wizard most likely presents a subset of its screens.

4.4.1 Checking for required PTFs

The display shown in Figure 66 does not appear if all the required PTFs are installed on the AS/400 system. You can print the list of missing PTFs to a printer connected to your PC if required.

Reminder

Installing the Group PTF CD (SF99083) on your system prior to running the Network Station Setup Wizard is a good way to ensure that any pre-requisite PTFs required for the V2R1 installation are already loaded.



Welcome to the AS/400 Network Station Setup Wizard. This Wizard configures the AS/400 for your IBM Network Stations.

Before you can proceed, you must install the following products and product fixes (PTFs) on your AS/400:

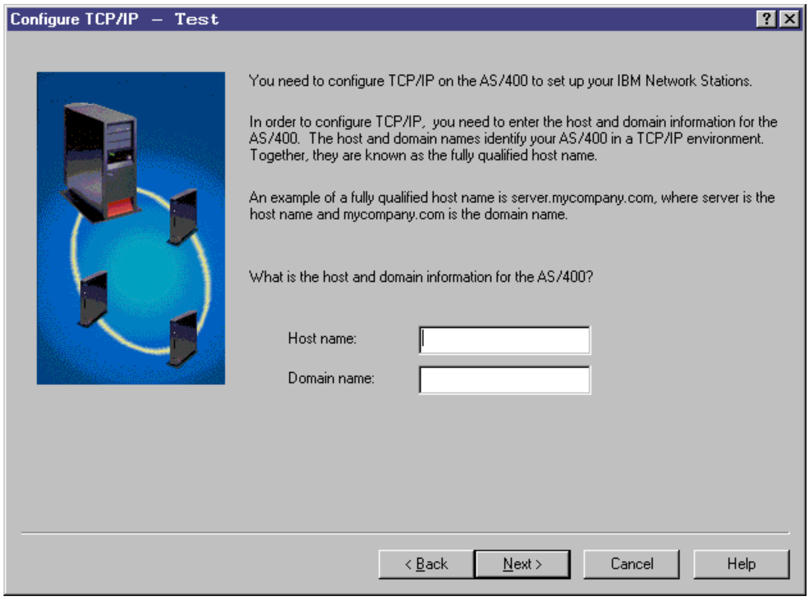
Figure 66. AS/400 Setup Wizard checking for required PTFs

4.4.2 Setting up an initial AS/400 system TCP/IP configuration

These AS/400 initial TCP/IP parameters settings include:

- Setting the AS/400 Host and Domain names. For example, the Host name could be NetServer and the Domain name could be mycompany.com. Refer to Figure 67 on page 94.
- Setting Domain Name servers using the dotted decimal format, for example, 10.100.1.10. See Figure 68 on page 94.

Note: The displays shown in Figure 67 and Figure 68 on page 94 only appear if the AS/400 system is connected through the Operations Console and TCP/IP has never been setup.



You need to configure TCP/IP on the AS/400 to set up your IBM Network Stations.

In order to configure TCP/IP, you need to enter the host and domain information for the AS/400. The host and domain names identify your AS/400 in a TCP/IP environment. Together, they are known as the fully qualified host name.

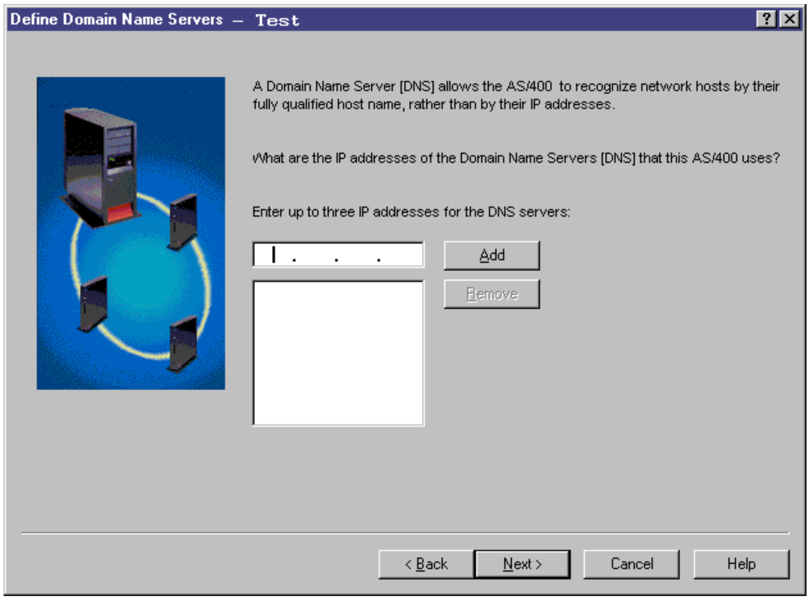
An example of a fully qualified host name is server.mycompany.com, where server is the host name and mycompany.com is the domain name.

What is the host and domain information for the AS/400?

Host name:

Domain name:

Figure 67. AS/400 Setup Wizard asking for the host and domain names



A Domain Name Server [DNS] allows the AS/400 to recognize network hosts by their fully qualified host name, rather than by their IP addresses.

What are the IP addresses of the Domain Name Servers [DNS] that this AS/400 uses?

Enter up to three IP addresses for the DNS servers:

Figure 68. AS/400 Setup Wizard asking for the IP addresses of Domain Name Servers

4.4.3 Setting up a TCP/IP communication configuration

The Wizard assists in configuring TCP/IP communication parameters in the AS/400 system so that the Network Stations can successfully communicate with it. Some of the tasks that the Wizard helps with are:

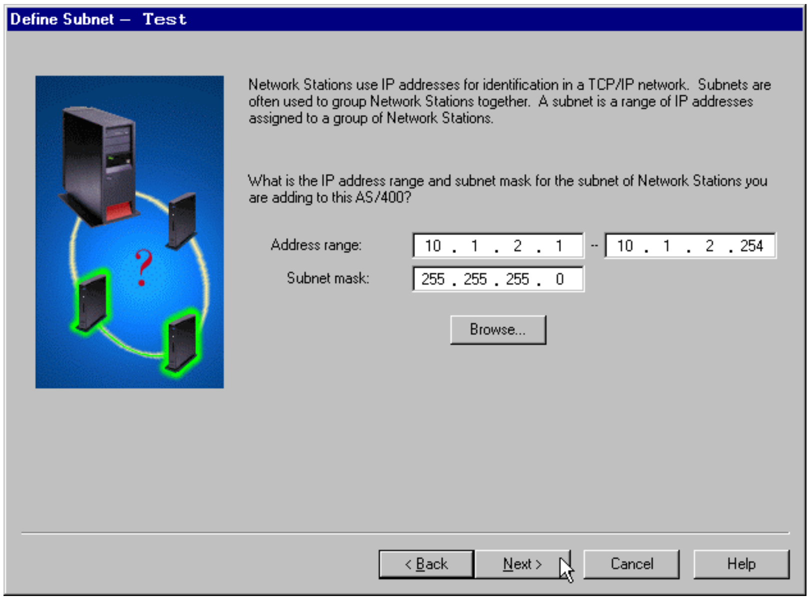
1. Defining an IP address range and subnet mask for the Network Stations in the AS/400 system (Figure 69).
2. Specifying how the Network Stations are going to be connected to the AS/400 system, either directly connected to or through a router (Figure 71 on page 96).

3. Creating a new line description (using Create Line Desc (Ethernet) (CRTLINETH) or Create Line Desc (Token-Ring) (CRTLINTRN)) and varying it using the Vary Configuration (VRYCFG) command. You are also given the choice of using an already existing line description. Refer to Figure 72 on page 97 and Figure 73 on page 97.
4. Creating a new Network Server Description (CTRNWSD) and varying it on using the Vary Configuration (VRYCFG) command. This is done if the Wizard detects that the hardware resource is an Integrated Netfinity Server. See Figure 76 on page 99.
5. Defining a new TCP/IP Interface (ADDTCPIFC). This is where you define the IP address and subnet mask of the AS/400 interface that will be used for this subnet. See Figure 77 on page 99.
6. Adding Host Table Entries (ADDTCPHTE) for the above interface.
7. Adding gateways with the Add TCP/IP Route (ADDTCPRTE) command. See Figure 78 on page 100 and Figure 79 on page 100.
8. Defining a boot-up method for the Network Stations (NVRAM, BOOTP, or DHCP). See Figure 81 on page 101.

4.4.3.1 Defining an IP range and subnet mask

Figure 69, shows the IP range that is going to be used to determine the TCP/IP interface and to build DHCP subnet. It should include an address for the TCP/IP interface if connecting directly to the AS/400 system.

You can click **Browse** to see the valid ranges for existing TCP/IP interfaces and DHCP subnets. The display shown in Figure 70 on page 96 appears.



Define Subnet – Test

Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

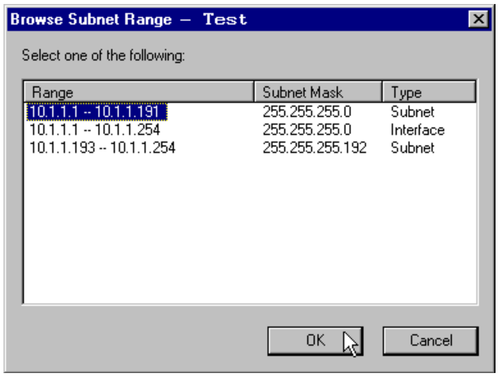
What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

Address range: 10 . 1 . 2 . 1 -- 10 . 1 . 2 . 254

Subnet mask: 255 . 255 . 255 . 0

Figure 69. Defining an IP range and subnet mask

Once you select the desired range, click **OK** to copy the range to the previous screen where the IP range and subnet mask are being defined.



Browse Subnet Range – Test

Select one of the following:

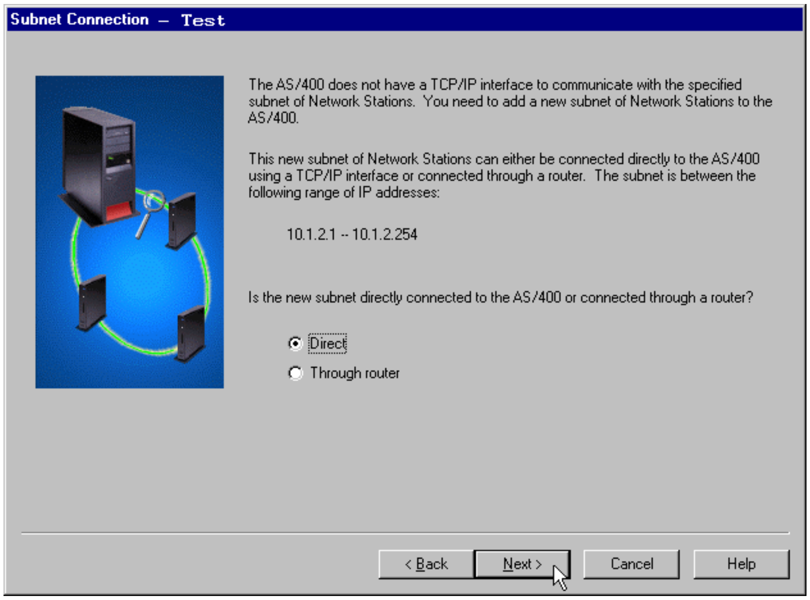
Range	Subnet Mask	Type
10.1.1.1 -- 10.1.1.191	255.255.255.0	Subnet
10.1.1.1 -- 10.1.1.254	255.255.255.0	Interface
10.1.1.193 -- 10.1.1.254	255.255.255.192	Subnet

Figure 70. Browsing a predefined subnet range

4.4.3.2 Selecting the type of subnet connection

As shown in Figure 71, the AS/400 Setup Wizard asks how the new subnet is going to be connected to the AS/400 system.

If the new subnet is going to be directly connected to the AS/400 system, the Wizard determines whether a TCP/IP interface is needed. If you decide that the new subnet is going to be connected to the AS/400 through a router, the Wizard does not ask any questions about creating a TCP/IP interface. The next task would be to select the startup method. If you select DHCP, the router option is required.



Subnet Connection – Test

The AS/400 does not have a TCP/IP interface to communicate with the specified subnet of Network Stations. You need to add a new subnet of Network Stations to the AS/400.

This new subnet of Network Stations can either be connected directly to the AS/400 using a TCP/IP interface or connected through a router. The subnet is between the following range of IP addresses:

10.1.2.1 -- 10.1.2.254

Is the new subnet directly connected to the AS/400 or connected through a router?

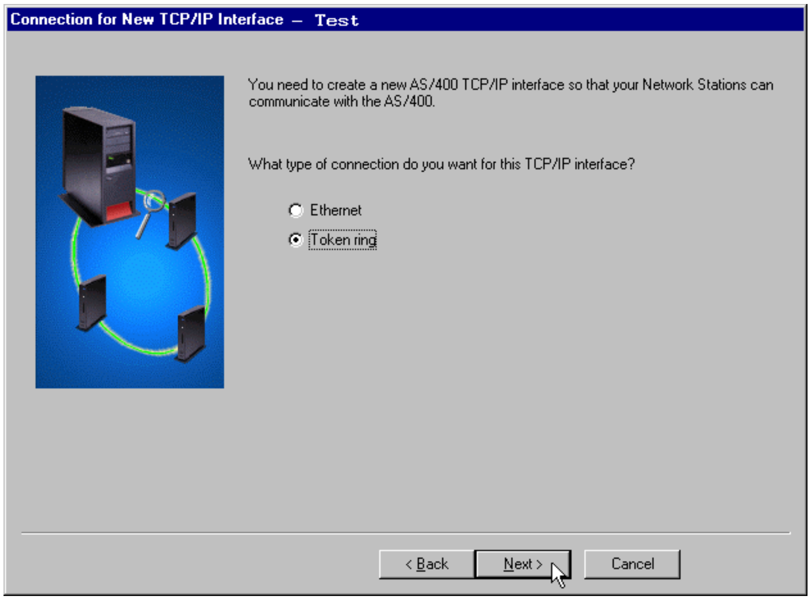
● Direct

○ Through router

Figure 71. Specifying how the Network Stations are connected to the AS/400 system

4.4.3.3 Using a new or existing line description

As shown in Figure 72, the AS/400 Setup Wizard asks for the type of interface you want. It only configures TCP/IP for Ethernet or Token-Ring, but not Twinax. If a type is not available on the AS/400 system, it is grayed out.



Connection for New TCP/IP Interface – Test

You need to create a new AS/400 TCP/IP interface so that your Network Stations can communicate with the AS/400.

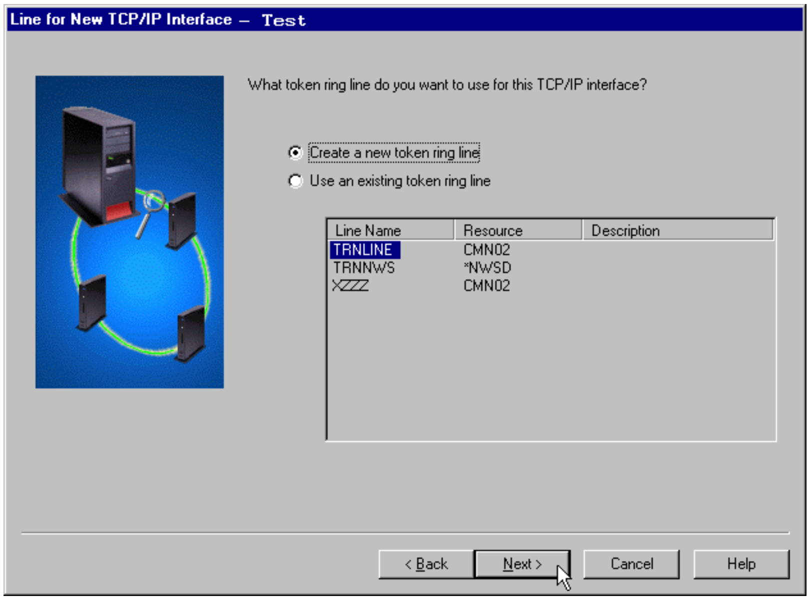
What type of connection do you want for this TCP/IP interface?

○ Ethernet

● Token ring

Figure 72. The AS/400 Setup Wizard asking for the type of interface to be created

On the display shown in Figure 73, you can see that the AS/400 Setup Wizard gives you the opportunity to create a new line or select an existing one. A list of lines previously specified and available for TCP/IP configuration are displayed. If there are none, Figure 73 is skipped and you are asked to create a line (Figure 74 on page 98).



Line for New TCP/IP Interface – Test

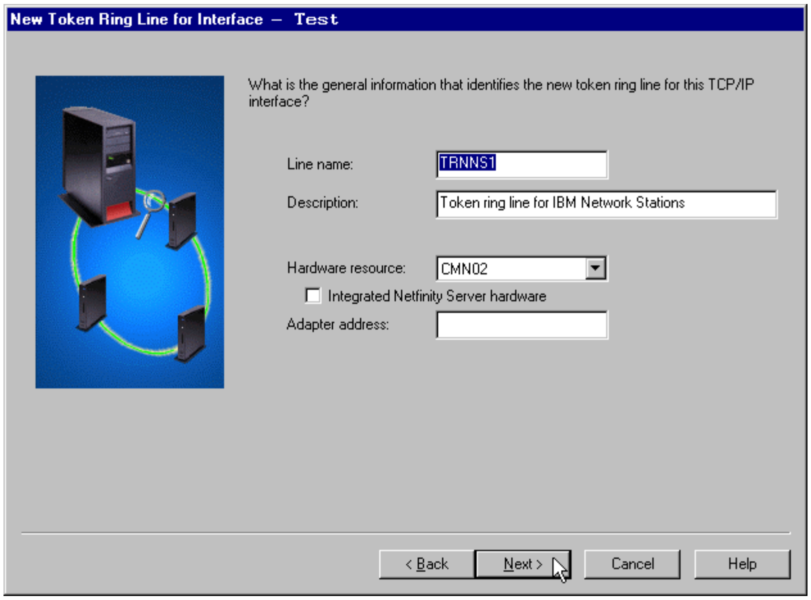
What token ring line do you want to use for this TCP/IP interface?

● Create a new token ring line

○ Use an existing token ring line

Line Name	Resource	Description
TRNLINE	CMN02	
TRNNWS	*NWSD	
XZZZ	CMN02	

Figure 73. Creating a new line or selecting an existing one


New Token Ring Line for Interface – Test

What is the general information that identifies the new token ring line for this TCP/IP interface?

Line name: TRNNS1

Description: Token ring line for IBM Network Stations

Hardware resource: CMN02

□ Integrated Netfinity Server hardware

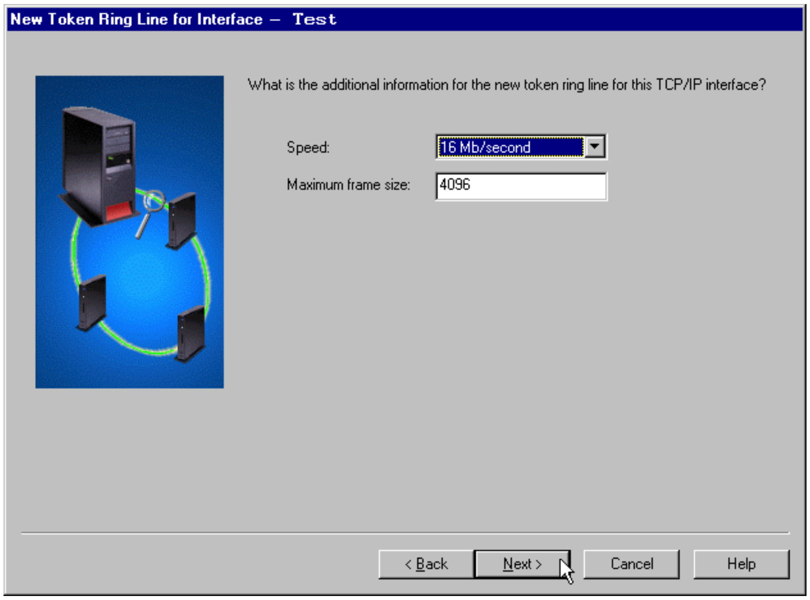
Adapter address:

Figure 74. The AS/400 Setup Wizard: Creating a line description

The creation of a line is spread across two configuration screens. Figure 74 displays the contents of the first screen. On the second screen, you provide the speed and maximum frame size as shown in Figure 75.

If the Wizard detects that the hardware resource is an Integrated Netfinity Server, the check box is selected. Otherwise, you must deselect it. Then, the Wizard proceeds to create a Network Server in the AS/400 (Figure 76).

Figure 75 displays the contents of the second configuration screen for a Token-Ring. If this was an Ethernet line, you would be asked to select the Protocol Standard (Ethernet version 2, IEE 802.3, or both).


New Token Ring Line for Interface – Test

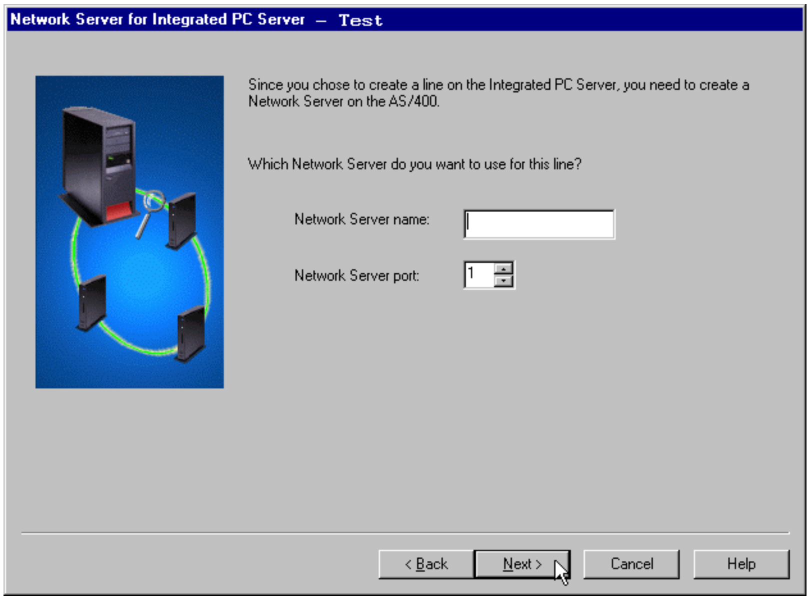
What is the additional information for the new token ring line for this TCP/IP interface?

Speed: 16 Mb/second

Maximum frame size: 4096

Figure 75. Defining the speed of the line and its maximum frame size

The display in Figure 76 only appears if the Wizard detects that the hardware resource is an Integrated Netfinity Server. The Wizard creates the associated Network Server Description for the Integrated Netfinity Server. You can do this manually by using the Create Network Server Description (`CRTNWSD`) command directly on the AS/400 system.



Network Server for Integrated PC Server – Test

Since you chose to create a line on the Integrated PC Server, you need to create a Network Server on the AS/400.

Which Network Server do you want to use for this line?

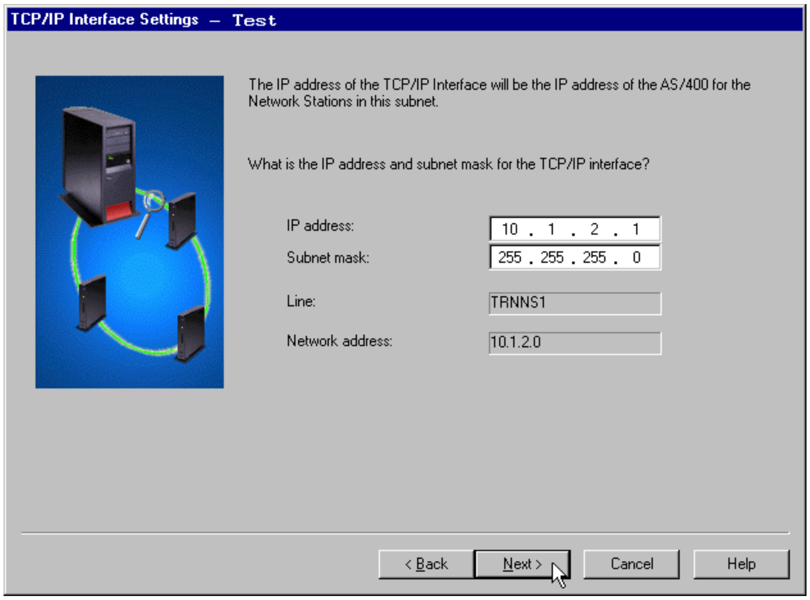
Network Server name:

Network Server port: 1

Figure 76. Creating a Network Server on the AS/400 system

4.4.3.4 Defining interfaces and gateways

As shown in Figure 77, you only specify some of the basic interface configuration parameters. By default, the Wizard fills in the TCP/IP interface address with the first IP address of the previously specified IP range provided by the user.



TCP/IP Interface Settings – Test

The IP address of the TCP/IP Interface will be the IP address of the AS/400 for the Network Stations in this subnet.

What is the IP address and subnet mask for the TCP/IP interface?

IP address: 10 . 1 . 2 . 1

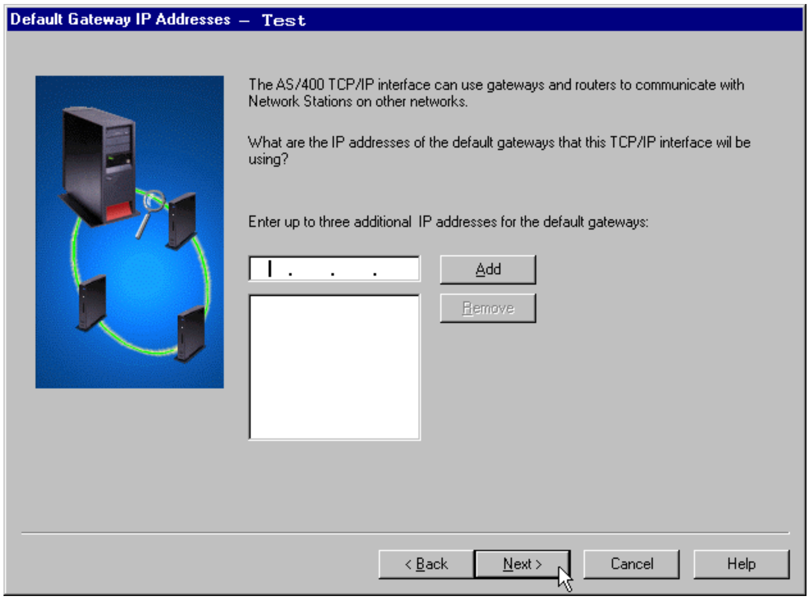
Subnet mask: 255 . 255 . 255 . 0

Line: TRNNS1

Network address: 10.1.2.0

Figure 77. Selecting the IP address and subnet mask for the AS/400 interface

You can add gateways by typing the IP address of the gateway in the field provided and then clicking on the **Add** button (Figure 78).



Default Gateway IP Addresses – Test

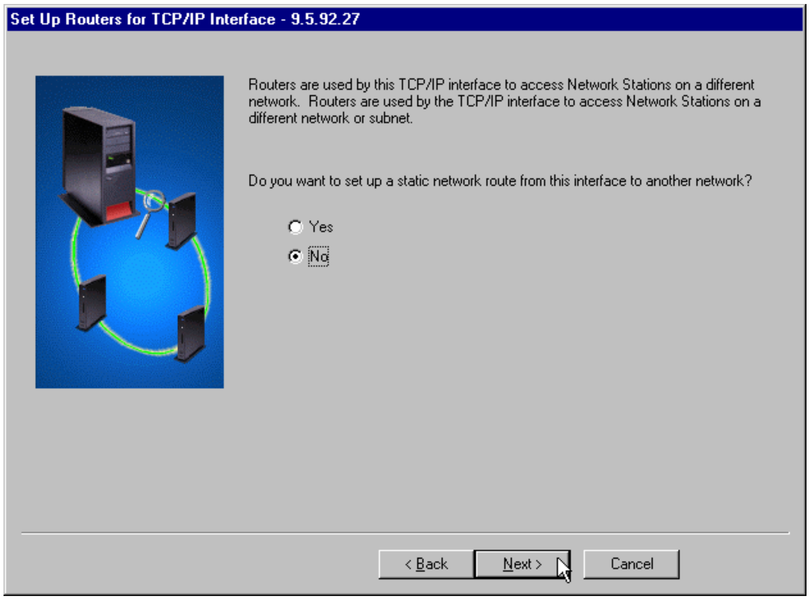
The AS/400 TCP/IP interface can use gateways and routers to communicate with Network Stations on other networks.

What are the IP addresses of the default gateways that this TCP/IP interface wil be using?

Enter up to three additional IP addresses for the default gateways:

Figure 78. Defining gateways

As shown in Figure 79, you can specify additional network routers. By default, this parameter is set to no. If you decide to specify Static Route, providing the information required in Figure 80 is your next task.



Set Up Routers for TCP/IP Interface - 9.5.92.27

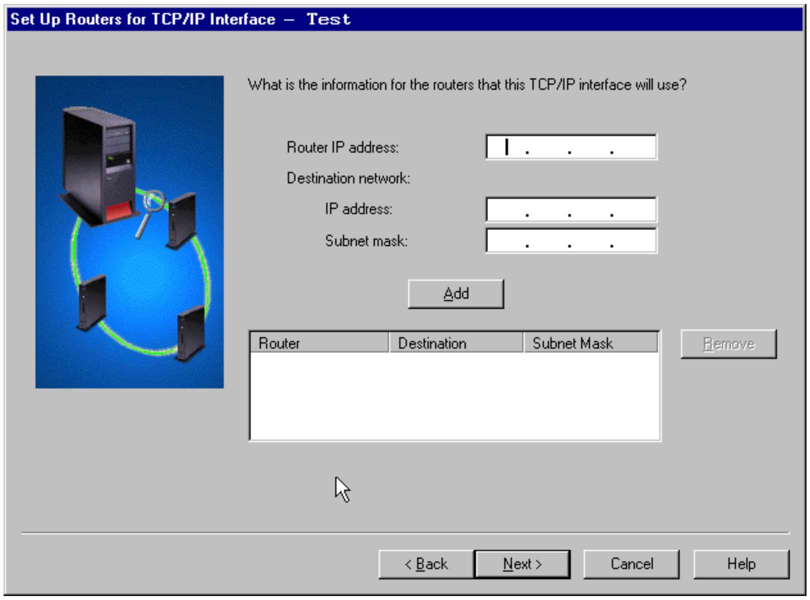
Routers are used by this TCP/IP interface to access Network Stations on a different network. Routers are used by the TCP/IP interface to access Network Stations on a different network or subnet.

Do you want to set up a static network route from this interface to another network?

○ Yes
● No

Figure 79. Specifying routers.

The display in Figure 80 is only shown if Static Network Route is selected. Then, you are asked to specify the required information. Click **Add** to save it. This Information is displayed on the route table contained in this display.



Set Up Routers for TCP/IP Interface – Test

What is the information for the routers that this TCP/IP interface will use?

Router IP address: . . .

Destination network:

IP address: . . .

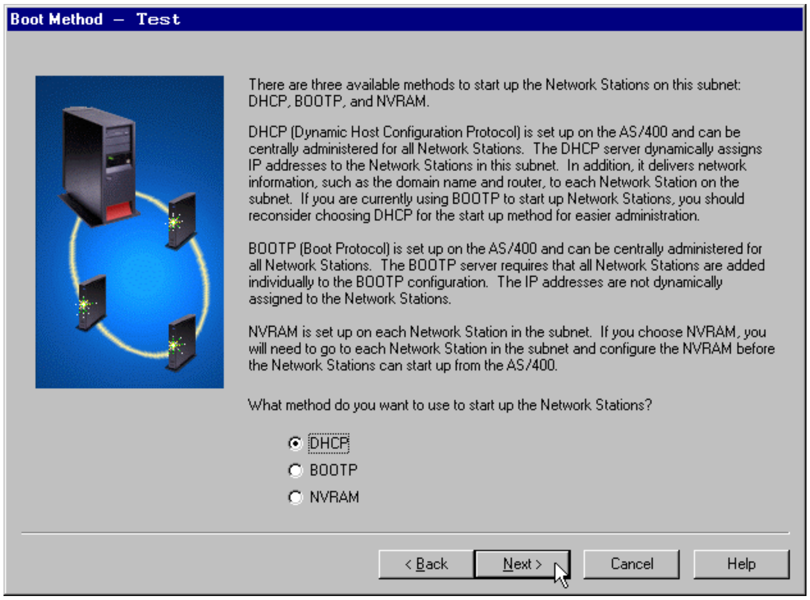
Subnet mask: . . .

Router	Destination	Subnet Mask

Figure 80. Providing the Wizard with router information

4.4.3.5 Defining the boot method NVRAM, BOOTP, or DHCP

As shown in Figure 81, the AS/400 Setup Wizard offers three startup (boot) methods, but it only assists with the DHCP configuration (Figure 84 on page 103).



Boot Method – Test

There are three available methods to start up the Network Stations on this subnet: DHCP, BOOTP, and NVRAM.

DHCP (Dynamic Host Configuration Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The DHCP server dynamically assigns IP addresses to the Network Stations in this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station on the subnet. If you are currently using BOOTP to start up Network Stations, you should reconsider choosing DHCP for the start up method for easier administration.

BOOTP (Boot Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The BOOTP server requires that all Network Stations are added individually to the BOOTP configuration. The IP addresses are not dynamically assigned to the Network Stations.

NVRAM is set up on each Network Station in the subnet. If you choose NVRAM, you will need to go to each Network Station in the subnet and configure the NVRAM before the Network Stations can start up from the AS/400.

What method do you want to use to start up the Network Stations?

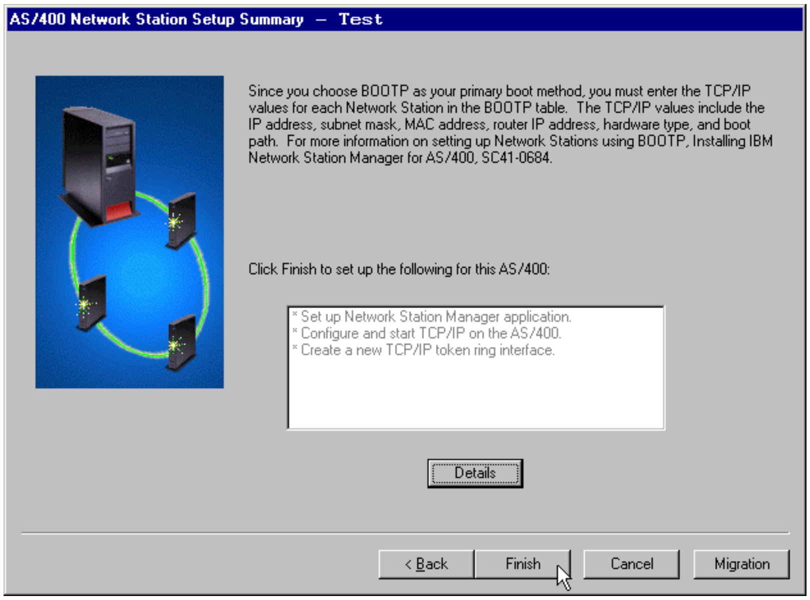
● DHCP
○ BOOTP
○ NVRAM

Figure 81. Bootup methods for the Network Station to startup

If BOOTP or NVRAM is selected, the AS/400 Setup Wizard displays the Setup Summary window as shown in Figure 82 on page 102.

This panel is only displayed if you select BOOTP as your startup method. Consult the manual *Installing Network Station Manager for AS/400*, SC41-0684, to manually configure BOOTP because the Wizard does not assist in configuring this option.

If you click the Finish button, the Wizard performs all the tasks displayed on the list. If more detailed information is needed, you can click **Details** (Figure 83).

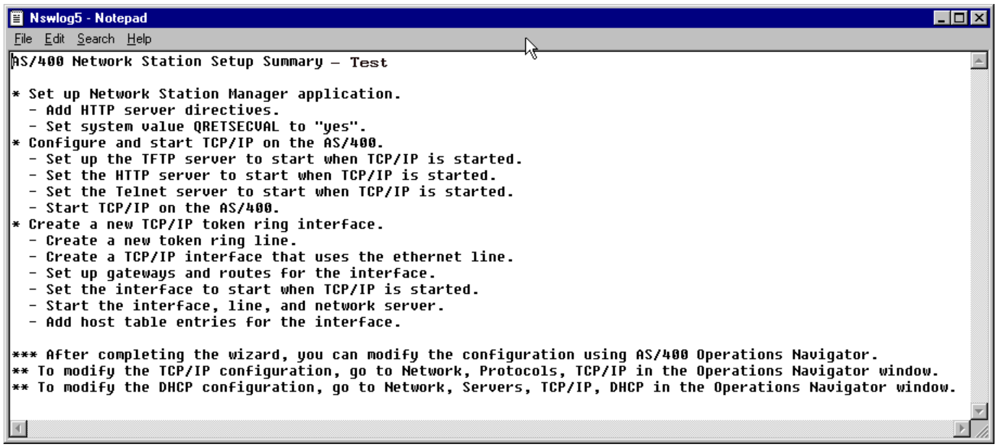


Since you choose BOOTP as your primary boot method, you must enter the TCP/IP values for each Network Station in the BOOTP table. The TCP/IP values include the IP address, subnet mask, MAC address, router IP address, hardware type, and boot path. For more information on setting up Network Stations using BOOTP, Installing IBM Network Station Manager for AS/400, SC41-0684.

Click Finish to set up the following for this AS/400:

* Set up Network Station Manager application.
* Configure and start TCP/IP on the AS/400.
* Create a new TCP/IP token ring interface.

Figure 82. AS/400 Setup Wizard summary



```
AS/400 Network Station Setup Summary – Test

* Set up Network Station Manager application.
  - Add HTTP server directives.
  - Set system value QRETSECVAL to "yes".
* Configure and start TCP/IP on the AS/400.
  - Set up the TFTP server to start when TCP/IP is started.
  - Set the HTTP server to start when TCP/IP is started.
  - Set the Telnet server to start when TCP/IP is started.
  - Start TCP/IP on the AS/400.
* Create a new TCP/IP token ring interface.
  - Create a new token ring line.
  - Create a TCP/IP interface that uses the ethernet line.
  - Set up gateways and routes for the interface.
  - Set the interface to start when TCP/IP is started.
  - Start the interface, line, and network server.
  - Add host table entries for the interface.

*** After completing the wizard, you can modify the configuration using AS/400 Operations Navigator.
** To modify the TCP/IP configuration, go to Network, Protocols, TCP/IP in the Operations Navigator window.
** To modify the DHCP configuration, go to Network, Servers, TCP/IP, DHCP in the Operations Navigator window.
```

Figure 83. AS/400 Network Station Setup Summary

4.4.4 Assistance in configuring the AS/400 systems DHCP

If you want our Network Stations to use DHCP as their boot startup method, the Wizard will assist you in configuring it. The Wizard performs some of the following tasks with the information you provide:

1. Migrating BOOTP clients to our new DHCP configuration (Figure 84).
2. Disabling BOOTP from auto starting with:

   ```
   CHGBPA AUTOSTART(*NO)
   ```

3. Stopping the BOOTP server with:

   ```
   ENDTCPSVR SERVER(*BOOTP)
   ```

4. Creating the required DHCP Option templates.

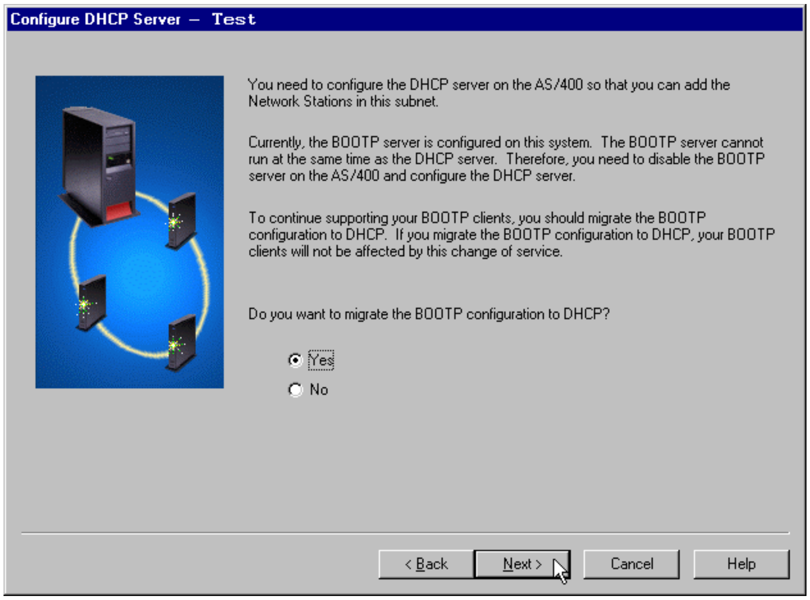
5. Creating the DHCP subnet (Figure 69 on page 95).
6. Adding the bootstrap server option to the subnet.
7. Adding the DHCP required options to the subnet.
8. Adding the required DHCP classes to the subnet.
9. Adding the DHCP excluded address.
10. Migrating BOOTP clients to be new DHCP clients if specified.
11. Setting DHCP server to auto start with:

    ```
    CHGDHCPA AUTOSTART(*YES).
    ```

12. Starting the DHCP server with:

    ```
    STRTCPSVR SERVER(*DHCP).
    ```

The display in Figure 84 is only shown if you select DHCP as your startup method. Through this display, you can migrate your BOOTP configuration to DHCP. The Wizard will not change anything about the BOOTP information when migrating. Whether your answer is Yes or No, the next task is shown in the display in Figure 85 on page 104.



Configure DHCP Server – Test

You need to configure the DHCP server on the AS/400 so that you can add the Network Stations in this subnet.

Currently, the BOOTP server is configured on this system. The BOOTP server cannot run at the same time as the DHCP server. Therefore, you need to disable the BOOTP server on the AS/400 and configure the DHCP server.

To continue supporting your BOOTP clients, you should migrate the BOOTP configuration to DHCP. If you migrate the BOOTP configuration to DHCP, your BOOTP clients will not be affected by this change of service.

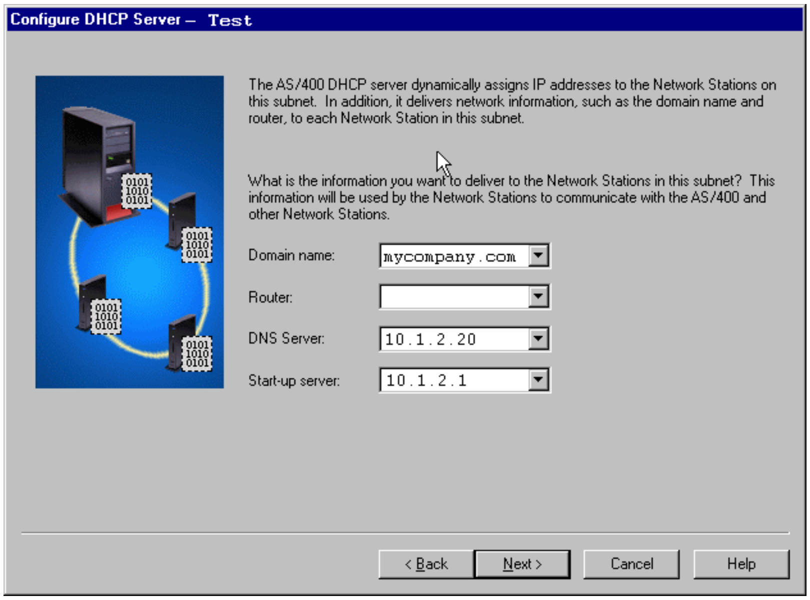
Do you want to migrate the BOOTP configuration to DHCP?

● Yes

○ No

Figure 84. Migrating the BOOTP configuration to DHCP

The Information in Figure 85 is saved as one of the options for the subnet that the Wizard is helping to create. The router information is required only if this subnet range accesses the AS/400 system through a router. Figure 86 on page 104 shows our next task.



Configure DHCP Server – Test

The AS/400 DHCP server dynamically assigns IP addresses to the Network Stations on this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station in this subnet.

What is the information you want to deliver to the Network Stations in this subnet? This information will be used by the Network Stations to communicate with the AS/400 and other Network Stations.

Domain name: mycompany.com

Router:

DNS Server: 10.1.2.20

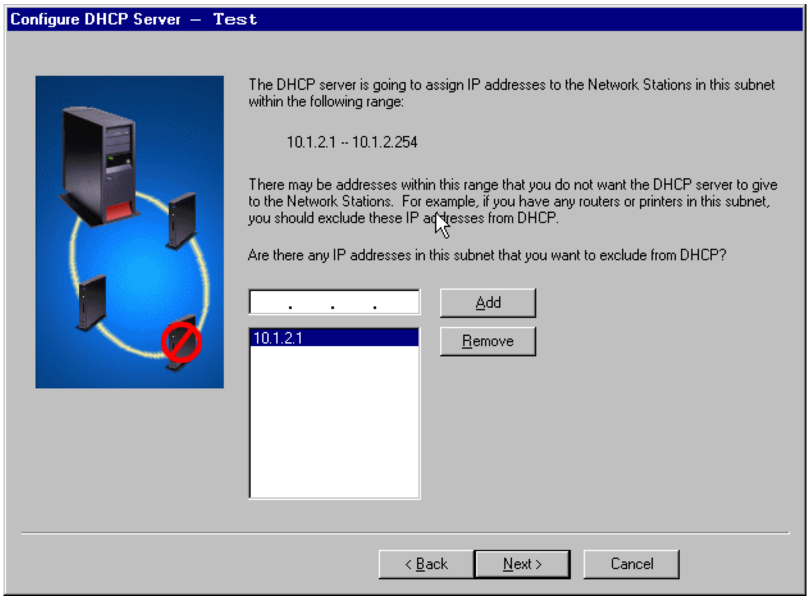
Start-up server: 10.1.2.1

Figure 85. Providing DHCP with a domain name, router IP, DNS server, and startup server

You can exclude IP addresses from DHCP so that it does not assign them to the Network Stations. By default, the IPs of the following components are excluded:

- Interface
- Gateways
- Routers.

Clicking **Next**. The display shown in Figure 87 appears.



Configure DHCP Server – Test

The DHCP server is going to assign IP addresses to the Network Stations in this subnet within the following range:

10.1.2.1 -- 10.1.2.254

There may be addresses within this range that you do not want the DHCP server to give to the Network Stations. For example, if you have any routers or printers in this subnet, you should exclude these IP addresses from DHCP.

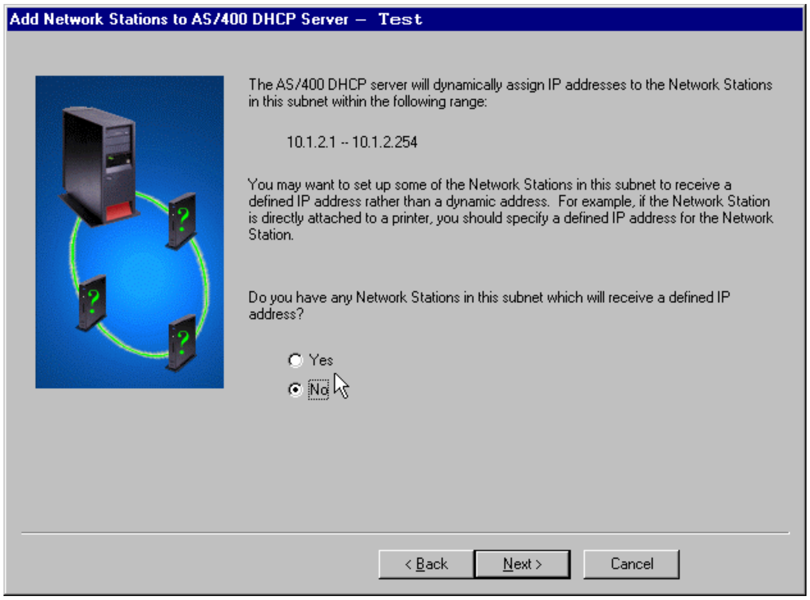
Are there any IP addresses in this subnet that you want to exclude from DHCP?

10.1.2.1

Figure 86. Excluding IP addresses from being used by DHCP

As shown in Figure 87, you can use dynamic or static IP addressing for the Network Stations. By default, this parameter is set to No. Click **Next**. We are presented with the display shown in Figure 89 on page 106.

If you decide to use static IP addressing for the Network Stations, your next task is to provide the Wizard with the required information as shown in Figure 88.



Add Network Stations to AS/400 DHCP Server – Test

The AS/400 DHCP server will dynamically assign IP addresses to the Network Stations in this subnet within the following range:

10.1.2.1 -- 10.1.2.254

You may want to set up some of the Network Stations in this subnet to receive a defined IP address rather than a dynamic address. For example, if the Network Station is directly attached to a printer, you should specify a defined IP address for the Network Station.

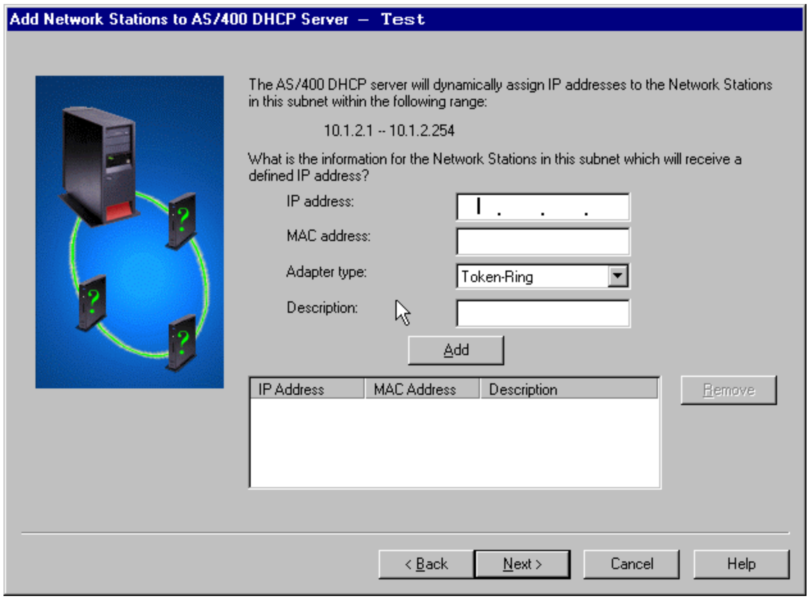
Do you have any Network Stations in this subnet which will receive a defined IP address?

○ Yes
● No

Figure 87. Defining Dynamic or Static IP addressing for the Network Stations

As shown in Figure 88, you are asked to associate an MAC address with an IP address. Then, click **Add**. Be careful to enter the correct information to avoid future configuration problems (for example, the incorrect MAC address).

After this task is finished, click **Next.** The display shown in Figure 89 on page 106 appears.



Add Network Stations to AS/400 DHCP Server – Test

The AS/400 DHCP server will dynamically assign IP addresses to the Network Stations in this subnet within the following range:

10.1.2.1 -- 10.1.2.254

What is the information for the Network Stations in this subnet which will receive a defined IP address?

IP address: . . .

MAC address:

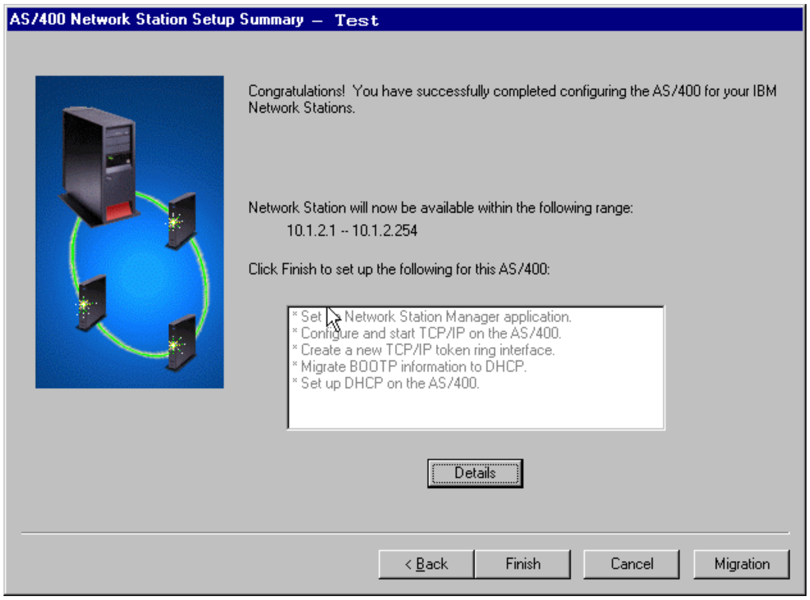
Adapter type: Token-Ring

Description:

IP Address	MAC Address	Description

Figure 88. Specifying a static IP address for Network Stations

As shown in Figure 89, the configuration of the AS/400 system for the Network Stations is completed. Clicking **Finish**. The AS/400 Setup Wizard performs all necessary tasks for a successful installation.



Congratulations! You have successfully completed configuring the AS/400 for your IBM Network Stations.

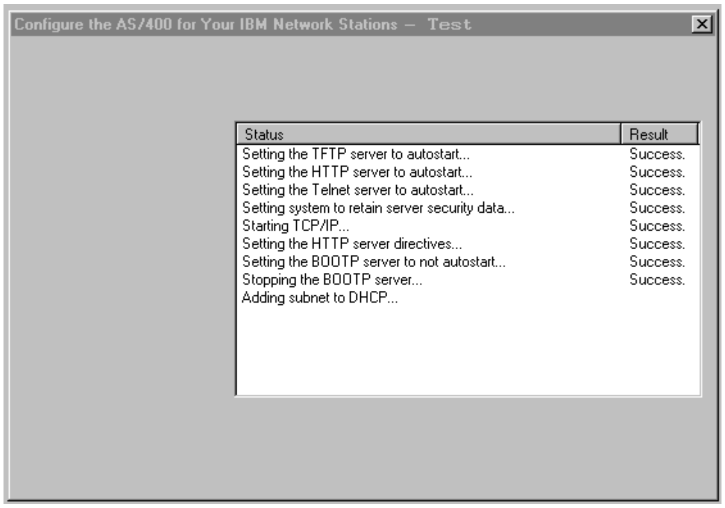
Network Station will now be available within the following range:
10.1.2.1 -- 10.1.2.254

Click Finish to set up the following for this AS/400:

- Set up Network Station Manager application.
- Configure and start TCP/IP on the AS/400.
- Create a new TCP/IP token ring interface.
- Migrate BOOTP information to DHCP.
- Set up DHCP on the AS/400.

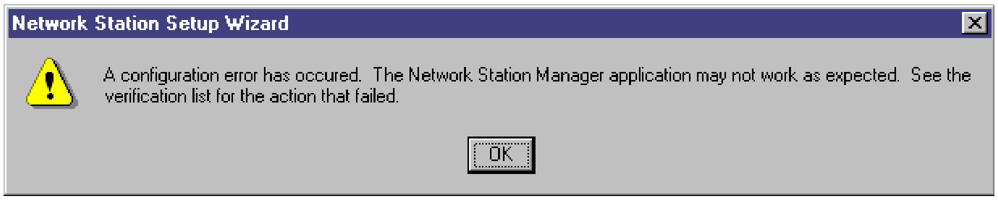
Figure 89. AS/400 Network Station Setup Summary for DHCP

Figure 90 shows the Wizard performing the final configuration tasks on the AS/400 system. If an error is encountered, the Wizard displays a warning message (Figure 91). Click **Help** for recovery information.



Status	Result
Setting the TFTP server to autostart...	Success.
Setting the HTTP server to autostart...	Success.
Setting the Telnet server to autostart...	Success.
Setting system to retain server security data...	Success.
Starting TCP/IP...	Success.
Setting the HTTP server directives...	Success.
Setting the BOOTP server to not autostart...	Success.
Stopping the BOOTP server...	Success.
Adding subnet to DHCP...	

Figure 90. AS/400 Setup Wizard performing the final configuration tasks on the AS/400 system


Network Station Setup Wizard

A configuration error has occured. The Network Station Manager application may not work as expected. See the verification list for the action that failed.

Figure 91. AS/400 Setup Wizard warning message for an unsuccessful setup

4.4.5 Behind the scenes tasks performed by the AS/400 Setup Wizard

In carrying out these tasks, the Wizard makes sure that a successful Network Station Manager setup takes place. These behind the scenes tasks include:

1. Setting the TFTP server to auto start using:

   ```
   CHGTFTPA AUTOSTART(*YES)
   ```

2. Setting the HTTP server to auto start using:

   ```
   CHGHTTPA AUTOSTART(*YES)
   ```

3. Setting the Telnet server to auto start using:

   ```
   CHGTELNA AUTOSTART(*YES)
   ```

4. Setting the system to retain server security data using:

   ```
   CHGSYSVAL SYSVAL(QRETSVRSEC) VALUE('1')
   ```

5. Starting the TCP/IP using:

   ```
   STRTCP STRSVR(*YES) STRIFC(*YES)
   ```

6. Setting HTTP server directives using:

   ```
   WRKHTTPCFG
   Host Name nsmHostName
   Enable POST
   Enable GET
   Map   /networkstationv2/admin /QYTCV2/QYTCMAIN.PGM
   Pass /networkstationv2/* /QIBM/ProdData/HTTP/Protect/NetworkStationV2/*
   Pass /flashconfigs/* /QIBM/UserData/NetworkStationV2/flash/ImageConfigs/*
   Exec /QYTCV2/* /QSYS.LIB/QYTCV2.LIB/*
   ```

7. Stopping the HTTP server using:

   ```
   ENDTCPSVR SERVER(*HTTP)
   ```

8. Writing new HTTP Directives.

9. Starting the HTTP server using:

   ```
   STRTCPSVR SERVER(*HTTP)
   ```

10. Starting the V2R1 Network Station Login daemon server.

    - If the V1R3 server is installed, you must stop the current server using:

      ```
      CALL QYTC/QYTCUSVR ('ENDTCPSVR ')
      ```

    - To start the V2R1 NSLD server, use:

      ```
      CALL QYTCV2/QYTCUSVR ('STRTCPSVR ')
      ```

4.5 Navigating with the Setup Wizard through a sample configuration

As you saw in the preceding sections, the Setup Wizard can present a large number of panels. This may seem confusing but, luckily, one of the first displays that the Setup Wizard presents to you contains a Planning Form. This Planning Form can be printed and then updated with your own network topology and TCP/IP network attributes.

This is exactly what we so in this section. That is, we print off the planning form and then update the example network and TCP/IP network attributes by hand on the form. We then scan the form back in for you to examine it as you review the panels presented by the Setup Wizard. Depending on the complexity of your network, many of the Setup Wizard panels are not even shown to you because the information is already configured on your system.

For our example, we are going to setup the Network Station Manager on an AS/400 system where TCP/IP is already configured. This AS/400 system does not have access to the Internet, and all the Network Stations are in the same subnet as the AS/400.

To start the Network Station Setup Wizard on your PC, perform the following steps:

1. Maximize the AS/400 Operation Navigator by double-clicking its desktop icon (Figure 92).

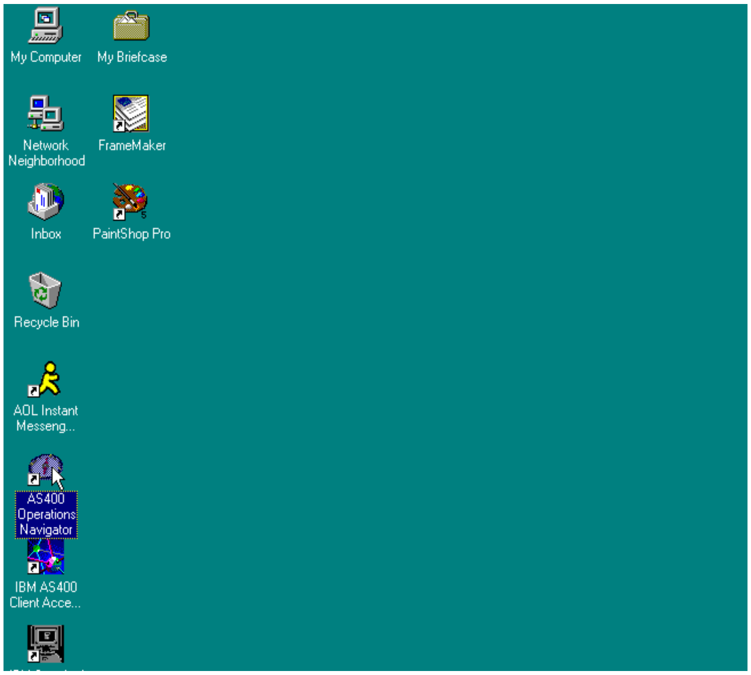


Figure 92. Opening the AS/400 Operations Navigator

2. Access the AS/400 system where the Network Station Manager is installed by double-clicking its interface (**10.1.1.1**) as shown in Figure 93.

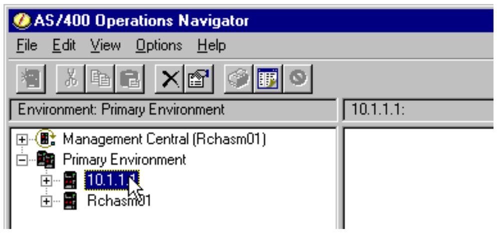
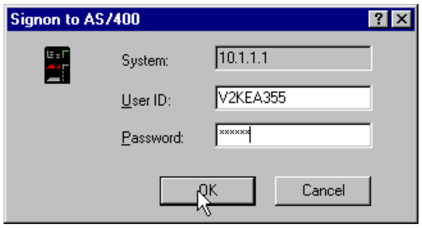

AS/400 Operations Navigator
File Edit View Options Help
Environment: Primary Environment
10.1.1.1:
Management Central (Rchasm01)
Primary Environment
10.1.1.1
Rchasm01

Figure 93. Expanding the AS/400 interface

3. Log onto the AS/400 system by entering your user ID and password. Click **OK** (Figure 94).



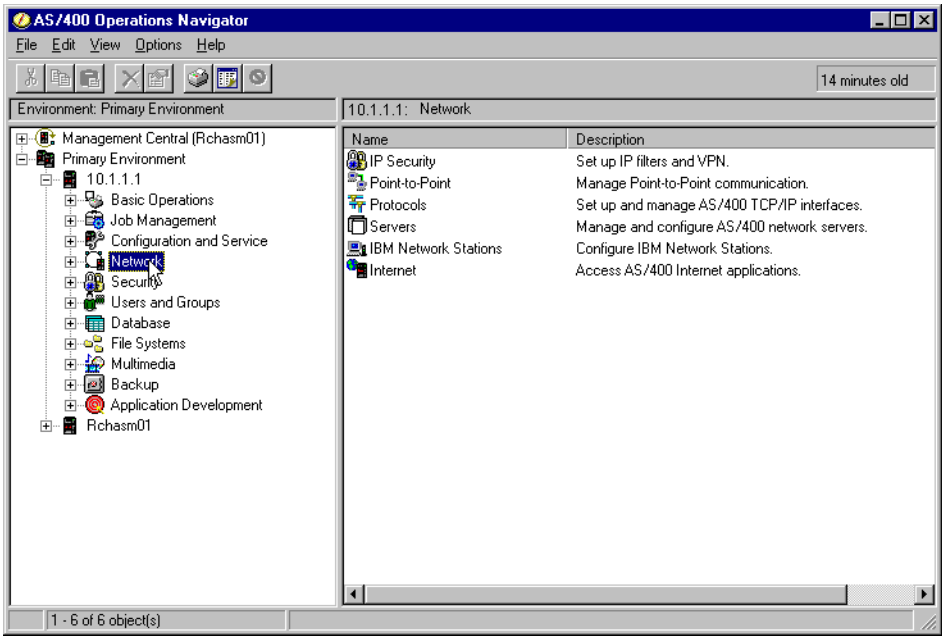
System: 10.1.1.1

User ID: V2KEA355

Password: ******

Figure 94. Logging on to the AS/400 system

4. As shown in Figure 95, you have accessed the AS/400 tasks directory. Click **Network** to expand its contents.



Name	Description
IP Security	Set up IP filters and VPN.
Point-to-Point	Manage Point-to-Point communication.
Protocols	Set up and manage AS/400 TCP/IP interfaces.
Servers	Manage and configure AS/400 network servers.
IBM Network Stations	Configure IBM Network Stations.
Internet	Access AS/400 Internet applications.

Figure 95. Expanding the contents of the Network icon

5. Select **IBM Network Station**, and right-click. Then, select **Add Network Stations to AS/400** (Figure 96 on page 110).

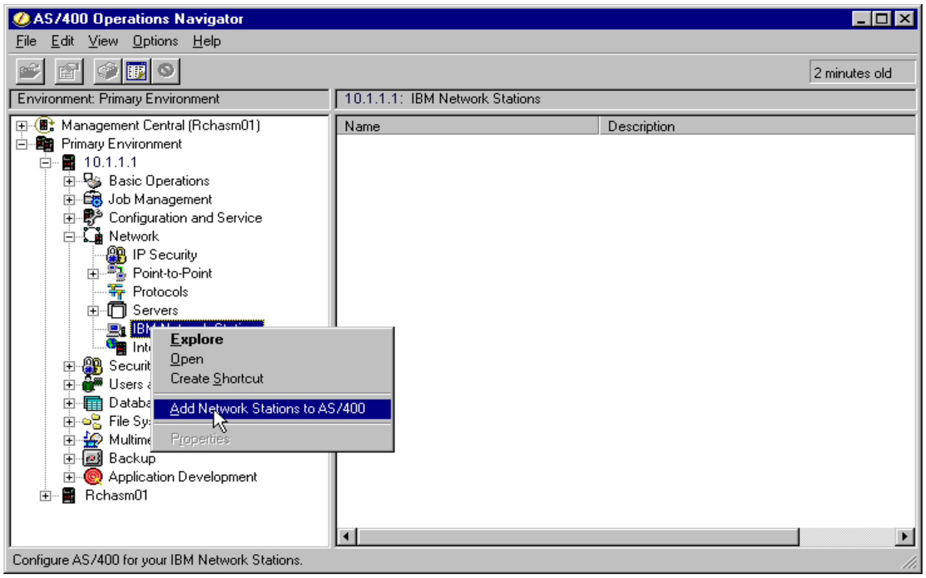
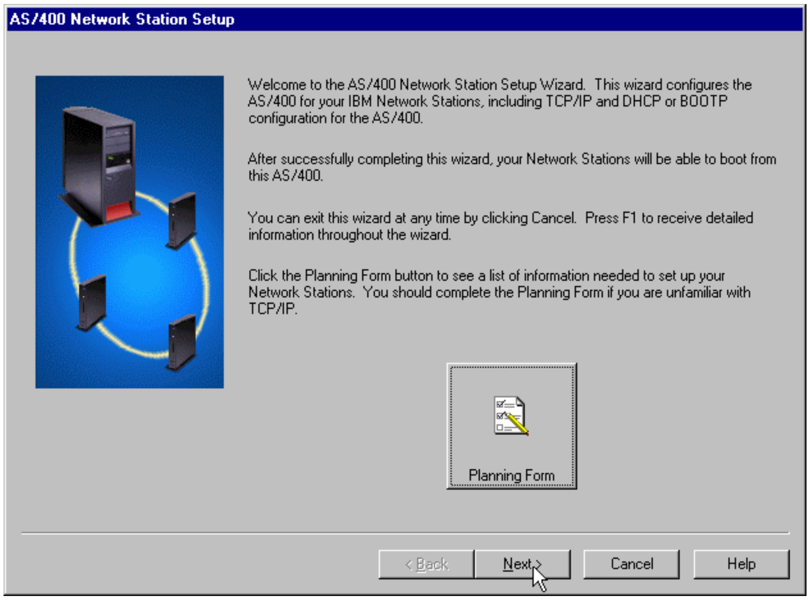

AS/400 Operations Navigator
File Edit View Options Help
2 minutes old
Environment: Primary Environment
10.1.1.1: IBM Network Stations
Management Central (Rchasm01)
Primary Environment
10.1.1.1
Basic Operations
Job Management
Configuration and Service
Network
IP Security
Point-to-Point
Protocols
Servers
Name
Description
Explore
Open
Create Shortcut
Add Network Stations to AS/400
Properties
Application Development
Rchasm01
Configure AS/400 for your IBM Network Stations.

Figure 96. Accessing the AS/400 Network Station Setup Wizard

6. Figure 97 shows the main window of the AS/400 Network Station Setup Wizard. Click the **Planning Form** button to access the Planning Form.



Welcome to the AS/400 Network Station Setup Wizard. This wizard configures the AS/400 for your IBM Network Stations, including TCP/IP and DHCP or BOOTP configuration for the AS/400.

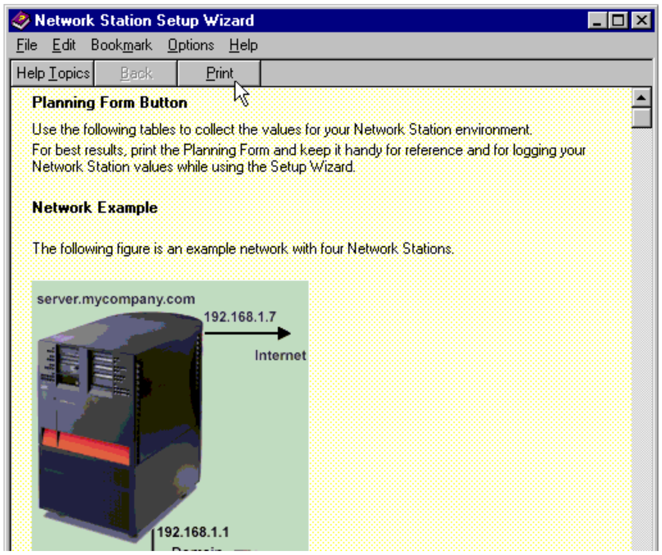
After successfully completing this wizard, your Network Stations will be able to boot from this AS/400.

You can exit this wizard at any time by clicking Cancel. Press F1 to receive detailed information throughout the wizard.

Click the Planning Form button to see a list of information needed to set up your Network Stations. You should complete the Planning Form if you are unfamiliar with TCP/IP.

Figure 97. Main screen of the AS/400 Network Station Setup Wizard

The Planning Form is shown in Figure 98. Here, you can view and Print the form.



Planning Form Button

Use the following tables to collect the values for your Network Station environment.

For best results, print the Planning Form and keep it handy for reference and for logging your Network Station values while using the Setup Wizard.

Network Example

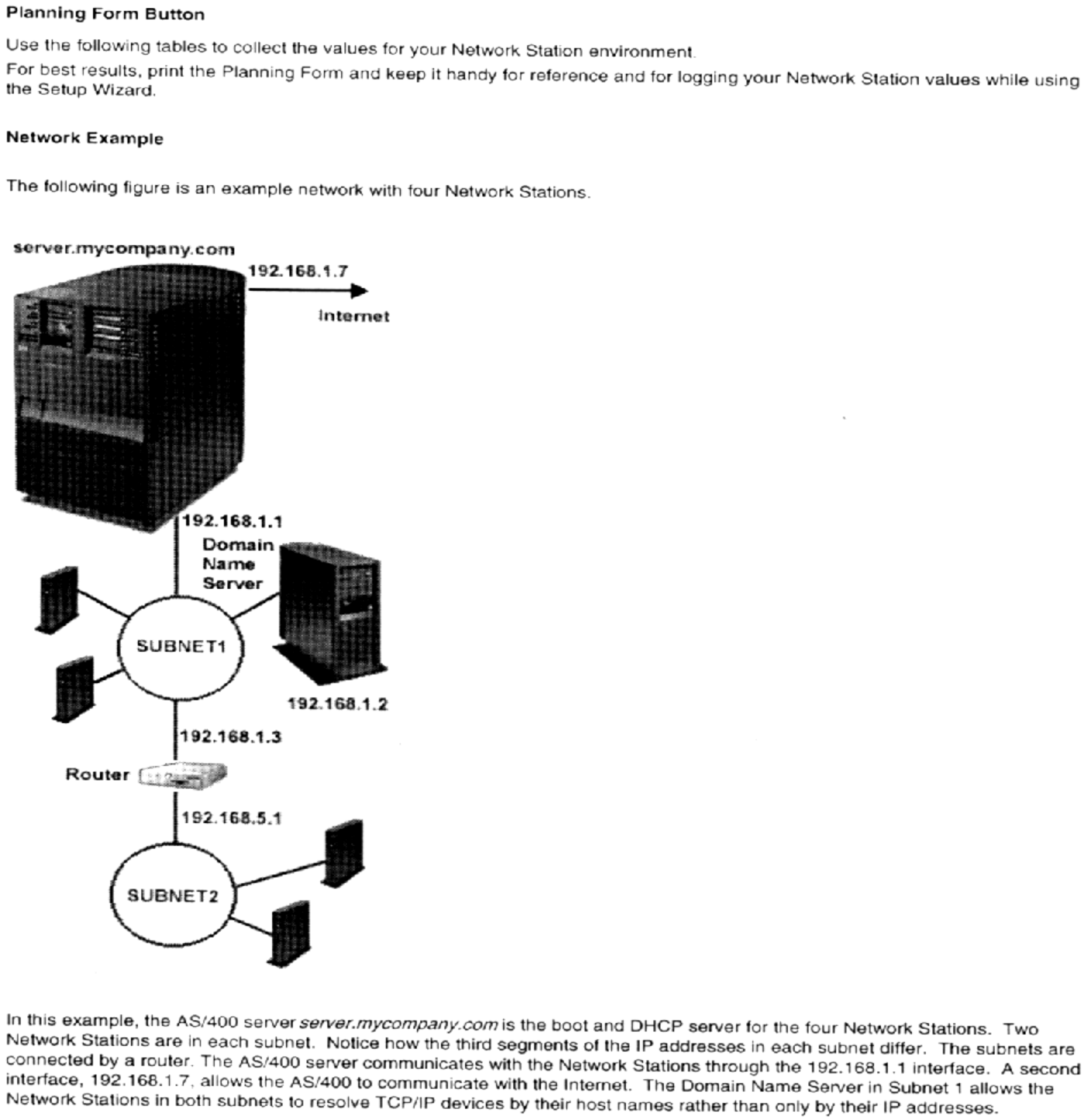
The following figure is an example network with four Network Stations.

Figure 98. Printing the Planning Form

Stop right there!

Since the purpose of this chapter is to introduce the Network Station Setup Wizard by going through a sample AS/400 configuration, we print, modify, and display the Planning Form that represents our sample AS/400 network. The printouts are shown in Figure 99 on page 112 through Figure 102 on page 115.

Take the time to review our hand markup of the Planning Form. It is important that you understand our network before proceeding with the Setup Wizard panels that follow.



Planning Form Button

Use the following tables to collect the values for your Network Station environment.

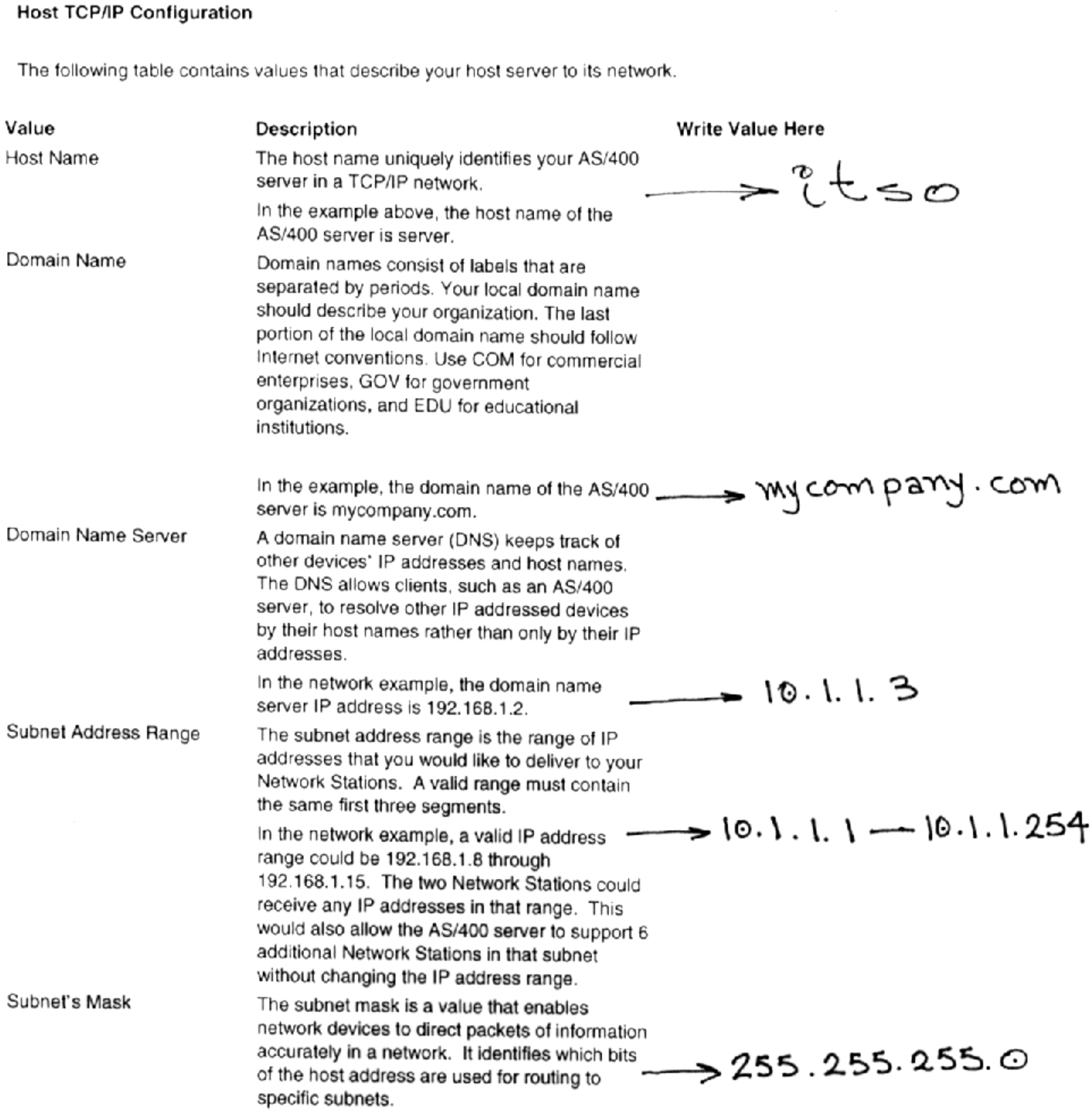
For best results, print the Planning Form and keep it handy for reference and for logging your Network Station values while using the Setup Wizard.

Network Example

The following figure is an example network with four Network Stations.

In this example, the AS/400 server *server.mycompany.com* is the boot and DHCP server for the four Network Stations. Two Network Stations are in each subnet. Notice how the third segments of the IP addresses in each subnet differ. The subnets are connected by a router. The AS/400 server communicates with the Network Stations through the 192.168.1.1 interface. A second interface, 192.168.1.7, allows the AS/400 to communicate with the Internet. The Domain Name Server in Subnet 1 allows the Network Stations in both subnets to resolve TCP/IP devices by their host names rather than only by their IP addresses.

Figure 99. Hand edited Planning Form (Part 1 of 4): Network Example

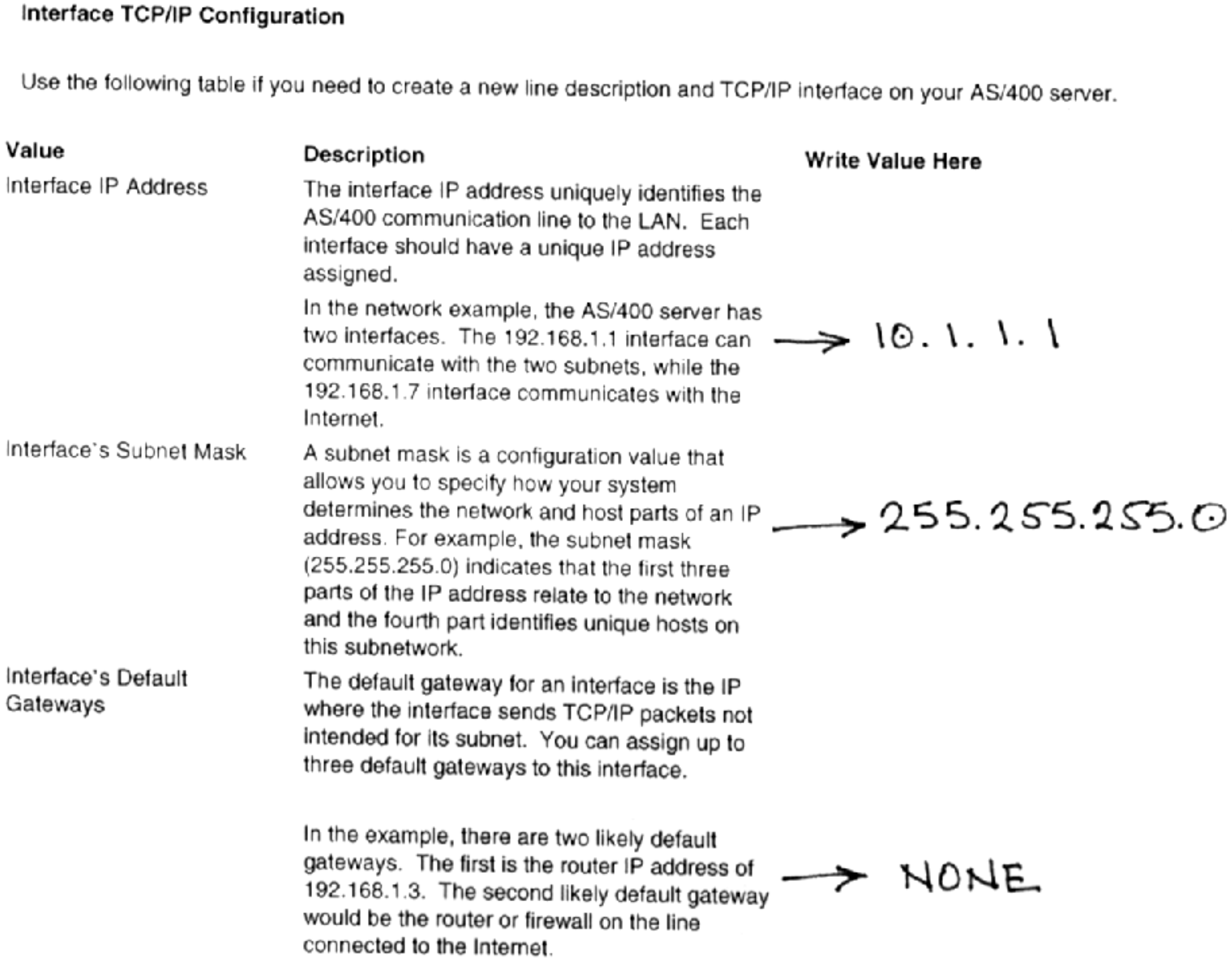


Host TCP/IP Configuration

The following table contains values that describe your host server to its network.

Value	Description	Write Value Here
Host Name	The host name uniquely identifies your AS/400 server in a TCP/IP network. In the example above, the host name of the AS/400 server is server.	itso
Domain Name	Domain names consist of labels that are separated by periods. Your local domain name should describe your organization. The last portion of the local domain name should follow Internet conventions. Use COM for commercial enterprises, GOV for government organizations, and EDU for educational institutions. In the example, the domain name of the AS/400 server is mycompany.com.	mycompany.com
Domain Name Server	A domain name server (DNS) keeps track of other devices' IP addresses and host names. The DNS allows clients, such as an AS/400 server, to resolve other IP addressed devices by their host names rather than only by their IP addresses. In the network example, the domain name server IP address is 192.168.1.2.	10.1.1.3
Subnet Address Range	The subnet address range is the range of IP addresses that you would like to deliver to your Network Stations. A valid range must contain the same first three segments. In the network example, a valid IP address range could be 192.168.1.8 through 192.168.1.15. The two Network Stations could receive any IP addresses in that range. This would also allow the AS/400 server to support 6 additional Network Stations in that subnet without changing the IP address range.	10.1.1.1 — 10.1.1.254
Subnet's Mask	The subnet mask is a value that enables network devices to direct packets of information accurately in a network. It identifies which bits of the host address are used for routing to specific subnets.	255.255.255.0

Figure 100. Hand edited Planning Form (Part 2 of 4): Host TCP/IP Configuration

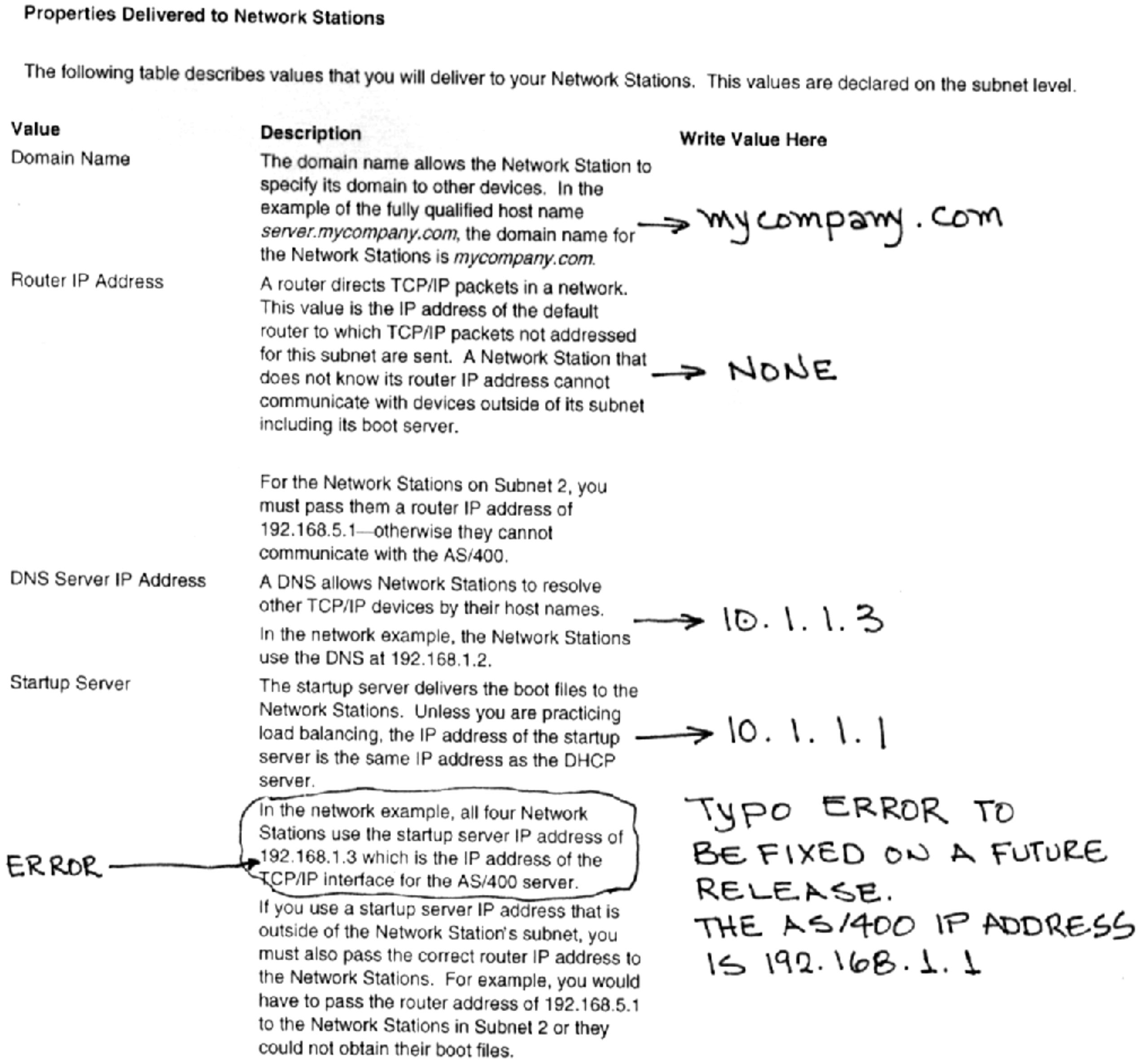


Interface TCP/IP Configuration

Use the following table if you need to create a new line description and TCP/IP interface on your AS/400 server.

Value	Description	Write Value Here
Interface IP Address	The interface IP address uniquely identifies the AS/400 communication line to the LAN. Each interface should have a unique IP address assigned.	
	In the network example, the AS/400 server has two interfaces. The 192.168.1.1 interface can communicate with the two subnets, while the 192.168.1.7 interface communicates with the Internet.	→ 10.1.1.1
Interface's Subnet Mask	A subnet mask is a configuration value that allows you to specify how your system determines the network and host parts of an IP address. For example, the subnet mask (255.255.255.0) indicates that the first three parts of the IP address relate to the network and the fourth part identifies unique hosts on this subnetwork.	→ 255.255.255.0
Interface's Default Gateways	The default gateway for an interface is the IP where the interface sends TCP/IP packets not intended for its subnet. You can assign up to three default gateways to this interface.	
	In the example, there are two likely default gateways. The first is the router IP address of 192.168.1.3. The second likely default gateway would be the router or firewall on the line connected to the Internet.	→ NONE

Figure 101. Hand edited Planning Form (Part 3 of 4): Interface TCP/IP Configuration



Properties Delivered to Network Stations

The following table describes values that you will deliver to your Network Stations. This values are declared on the subnet level.

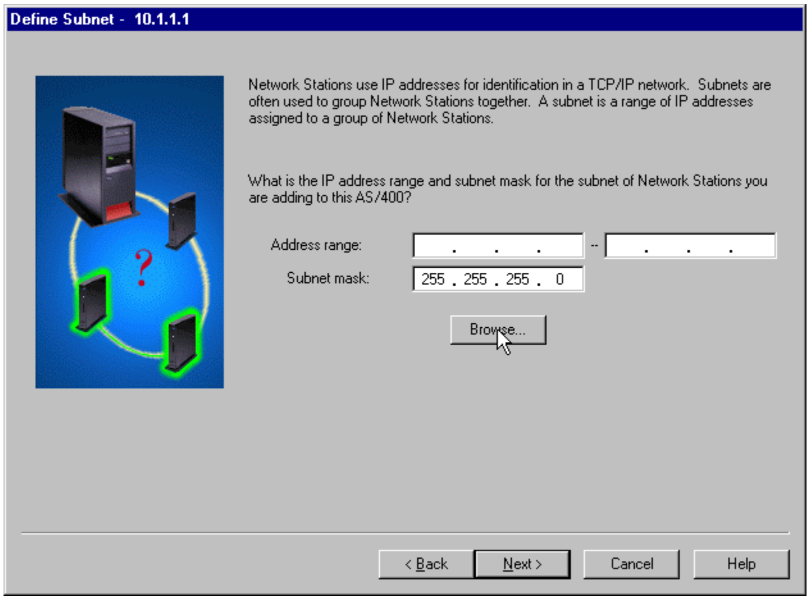
Value	Description	Write Value Here
Domain Name	The domain name allows the Network Station to specify its domain to other devices. In the example of the fully qualified host name *server.mycompany.com*, the domain name for the Network Stations is *mycompany.com*.	→ mycompany.com
Router IP Address	A router directs TCP/IP packets in a network. This value is the IP address of the default router to which TCP/IP packets not addressed for this subnet are sent. A Network Station that does not know its router IP address cannot communicate with devices outside of its subnet including its boot server. For the Network Stations on Subnet 2, you must pass them a router IP address of 192.168.5.1—otherwise they cannot communicate with the AS/400.	→ NONE
DNS Server IP Address	A DNS allows Network Stations to resolve other TCP/IP devices by their host names. In the network example, the Network Stations use the DNS at 192.168.1.2.	→ 10.1.1.3
Startup Server ERROR →	The startup server delivers the boot files to the Network Stations. Unless you are practicing load balancing, the IP address of the startup server is the same IP address as the DHCP server. In the network example, all four Network Stations use the startup server IP address of 192.168.1.3 which is the IP address of the TCP/IP interface for the AS/400 server. If you use a startup server IP address that is outside of the Network Station's subnet, you must also pass the correct router IP address to the Network Stations. For example, you would have to pass the router address of 192.168.5.1 to the Network Stations in Subnet 2 or they could not obtain their boot files.	→ 10.1.1.1 TYPO ERROR TO BE FIXED ON A FUTURE RELEASE. THE AS/400 IP ADDRESS IS 192.168.1.1

Figure 102. Hand edited Planning Form (Part 4 of 4): Properties Delivered to Network Stations

7. Your first task is to provide an IP range and subnet mask for the Network Station to use as shown in Figure 103 on page 116.

   If you already have a predefined range and subnet mask. Click **Browse**, make your selection, and click **OK** to continue. Refer to Figure 104 on page 116.

   Otherwise, enter the IP range and subnet mask. Then, click **Next** as shown in Figure 105 on page 117.



Define Subnet - 10.1.1.1

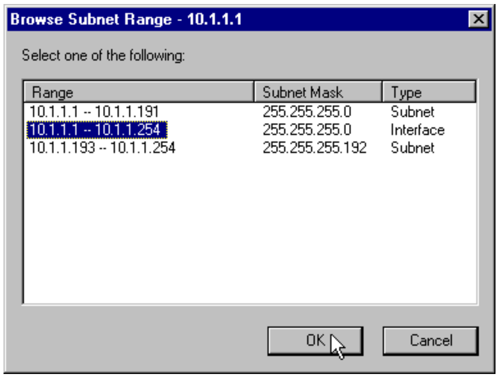
Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

Address range: . . . -- . . .

Subnet mask: 255 . 255 . 255 . 0

Figure 103. Defining an IP range and subnet mask for the Network Stations

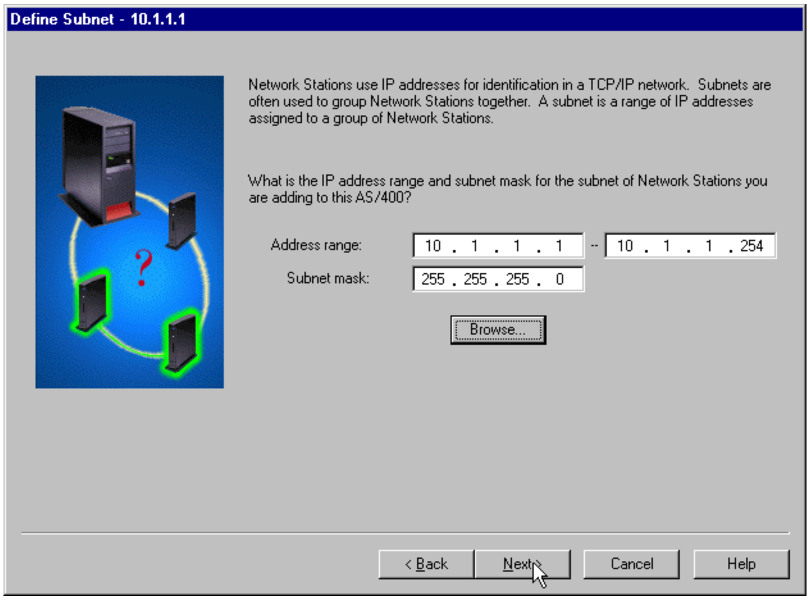


Browse Subnet Range - 10.1.1.1

Select one of the following:

Range	Subnet Mask	Type
10.1.1.1 -- 10.1.1.191	255.255.255.0	Subnet
10.1.1.1 -- 10.1.1.254	255.255.255.0	Interface
10.1.1.193 -- 10.1.1.254	255.255.255.192	Subnet

Figure 104. Selecting a predefined IP range and subnet mask



Define Subnet - 10.1.1.1

Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

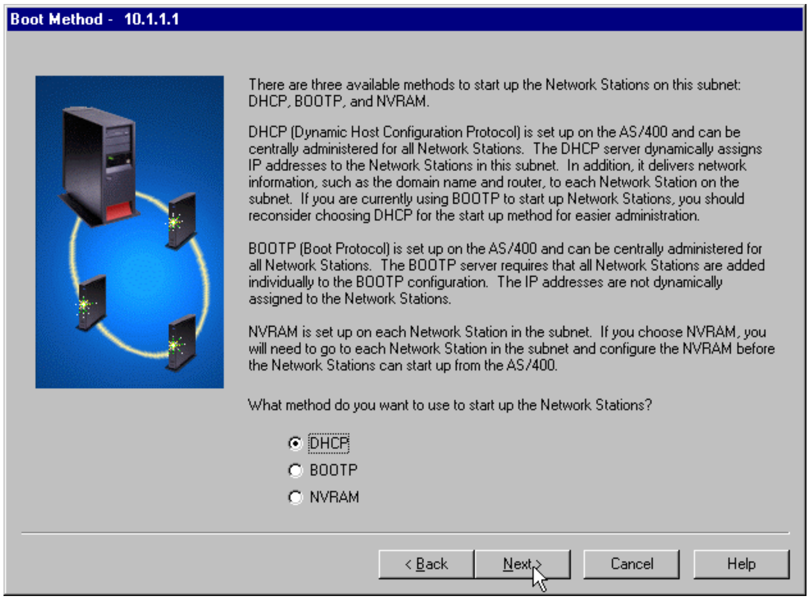
What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

Address range: 10 . 1 . 1 . 1 -- 10 . 1 . 1 . 254

Subnet mask: 255 . 255 . 255 . 0

Figure 105. Defining an IP range and subnet mask for the Network Stations

8. Select the startup method that the Network Stations are going to use. In this sample configuration, we select **DHCP**. Click **Next**, as shown in Figure 106.



Boot Method - 10.1.1.1

There are three available methods to start up the Network Stations on this subnet: DHCP, BOOTP, and NVRAM.

DHCP (Dynamic Host Configuration Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The DHCP server dynamically assigns IP addresses to the Network Stations in this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station on the subnet. If you are currently using BOOTP to start up Network Stations, you should reconsider choosing DHCP for the start up method for easier administration.

BOOTP (Boot Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The BOOTP server requires that all Network Stations are added individually to the BOOTP configuration. The IP addresses are not dynamically assigned to the Network Stations.

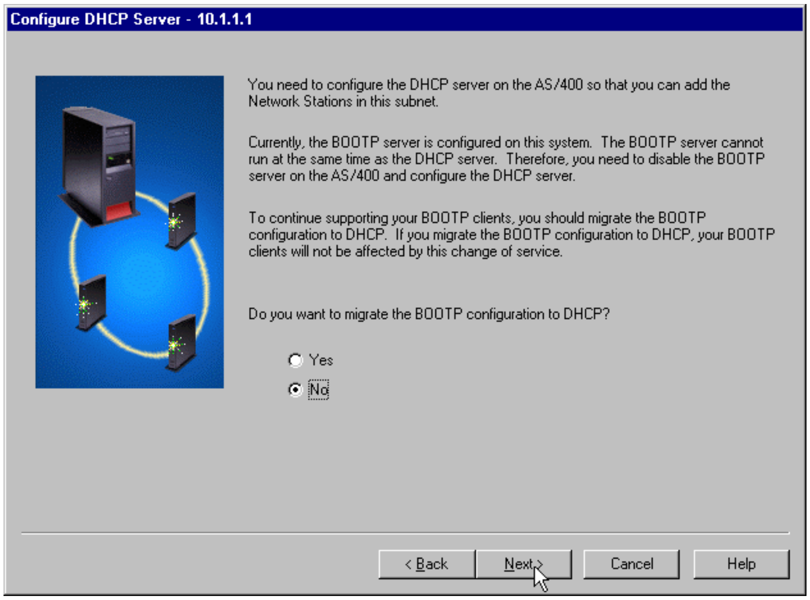
NVRAM is set up on each Network Station in the subnet. If you choose NVRAM, you will need to go to each Network Station in the subnet and configure the NVRAM before the Network Stations can start up from the AS/400.

What method do you want to use to start up the Network Stations?

● DHCP
○ BOOTP
○ NVRAM

Figure 106. Selecting the startup method for the Network Stations

9. As part of configuring DHCP on the AS/400 system, you are asked if you want to migrate previous BOOTP configurations. In this sample configuration, select **No**. Then, click **Next**. Refer to Figure 107 on page 118.



Configure DHCP Server - 10.1.1.1

You need to configure the DHCP server on the AS/400 so that you can add the Network Stations in this subnet.

Currently, the BOOTP server is configured on this system. The BOOTP server cannot run at the same time as the DHCP server. Therefore, you need to disable the BOOTP server on the AS/400 and configure the DHCP server.

To continue supporting your BOOTP clients, you should migrate the BOOTP configuration to DHCP. If you migrate the BOOTP configuration to DHCP, your BOOTP clients will not be affected by this change of service.

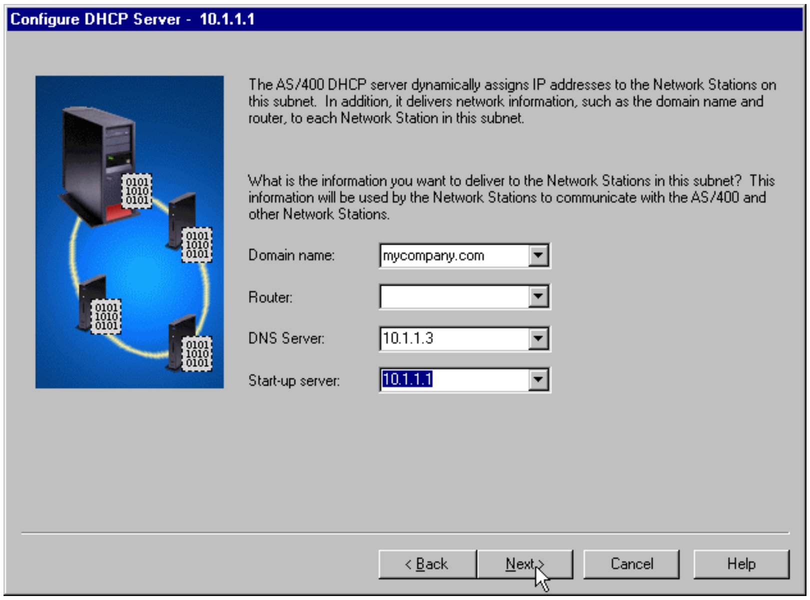
Do you want to migrate the BOOTP configuration to DHCP?

○ Yes

● No

Figure 107. Selecting whether to migrate previous BOOTP configurations

10.Enter the Domain Name, Router, DNS server and Start-up server information for the Network Station to communicate with the AS/400 and other Network Stations. Then, click **Next**. Figure 108 which shows our sample configuration information.



Configure DHCP Server - 10.1.1.1

The AS/400 DHCP server dynamically assigns IP addresses to the Network Stations on this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station in this subnet.

What is the information you want to deliver to the Network Stations in this subnet? This information will be used by the Network Stations to communicate with the AS/400 and other Network Stations.

Domain name: mycompany.com

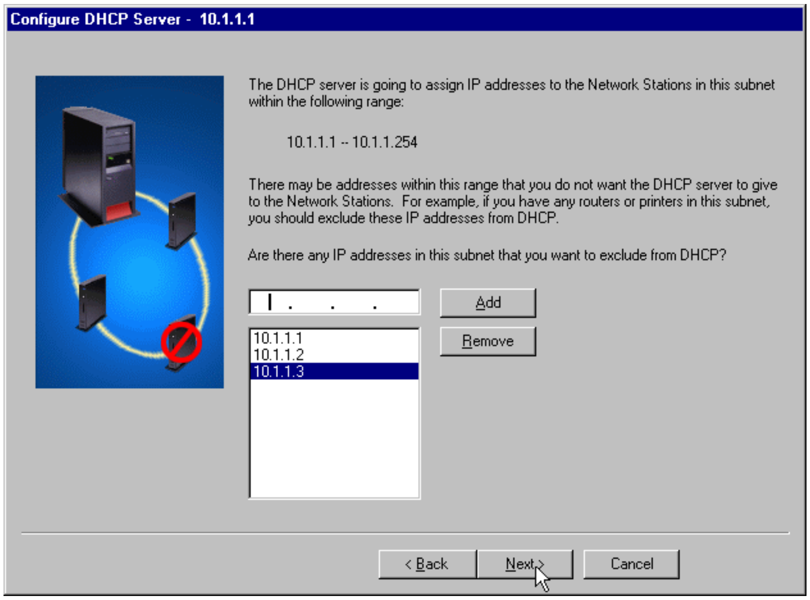
Router:

DNS Server: 10.1.1.3

Start-up server: 10.1.1.1

Figure 108. Providing information for the Network Stations to communicate with the Network

11.Exclude any IP addresses that you do not want DHCP to assign to the Network Stations. As shown in Figure 109, the IP address of the Router, DNS server and Start-up server, are already excluded. Click **Next** to continue.



Configure DHCP Server - 10.1.1.1

The DHCP server is going to assign IP addresses to the Network Stations in this subnet within the following range:

10.1.1.1 -- 10.1.1.254

There may be addresses within this range that you do not want the DHCP server to give to the Network Stations. For example, if you have any routers or printers in this subnet, you should exclude these IP addresses from DHCP.

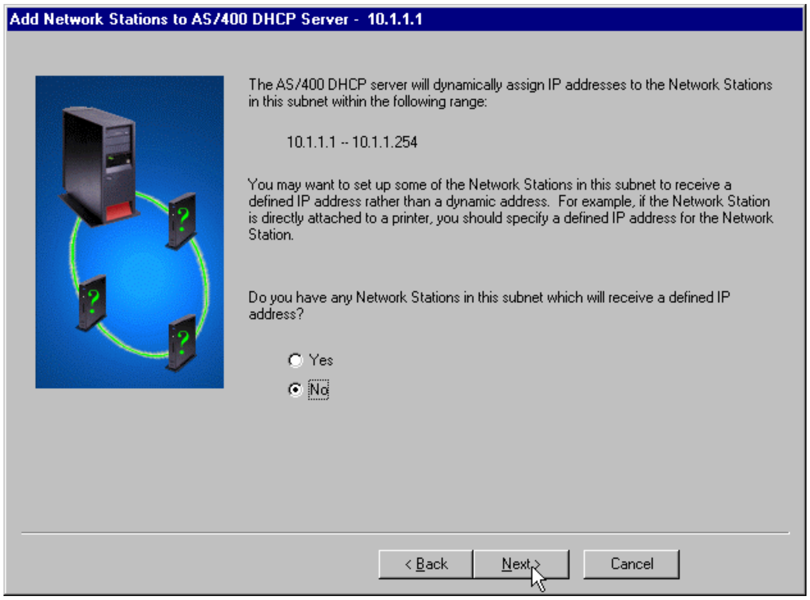
Are there any IP addresses in this subnet that you want to exclude from DHCP?

10.1.1.1
10.1.1.2
10.1.1.3

Figure 109. Excluding IP addresses from DHCP

12. From the provided range, the AS/400 DHCP dynamically assigns IP addresses to the Network Stations. If you need to assign a fixed IP address to some of your Network Stations, select **Yes**. Click **Next**.

    Since in our sample configuration, we do not need to assign fixed IP addresses to our Network Stations, we select **No**. Click **Next** as shown in Figure 110.



Add Network Stations to AS/400 DHCP Server - 10.1.1.1

The AS/400 DHCP server will dynamically assign IP addresses to the Network Stations in this subnet within the following range:

10.1.1.1 -- 10.1.1.254

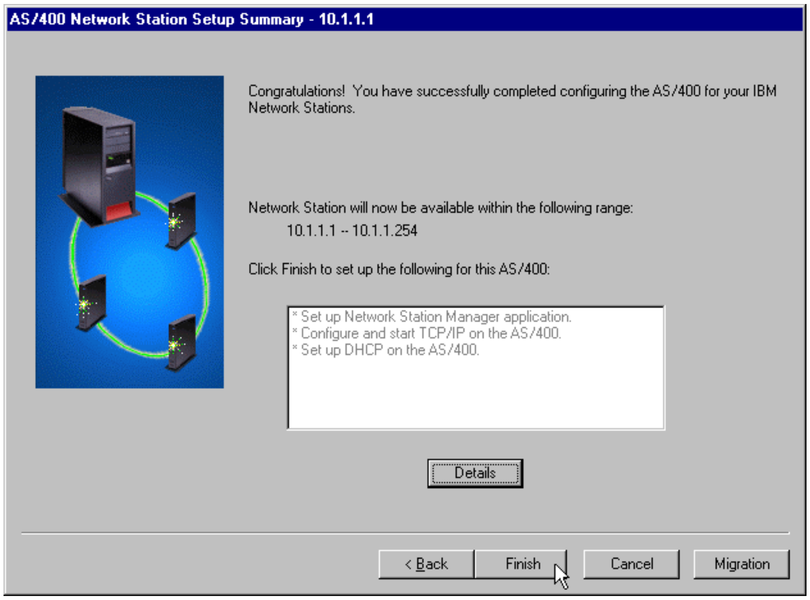
You may want to set up some of the Network Stations in this subnet to receive a defined IP address rather than a dynamic address. For example, if the Network Station is directly attached to a printer, you should specify a defined IP address for the Network Station.

Do you have any Network Stations in this subnet which will receive a defined IP address?

○ Yes
● No

Figure 110. Assigning a fixed IP address to the Network Stations

13. You finally reach the point where the AS/400 Network Station Setup Wizard has all the required information to perform a successful Network Station Manager setup. Clicking **Finish**, and the setup is performed as shown in Figure 111 on page 120.



Congratulations! You have successfully completed configuring the AS/400 for your IBM Network Stations.

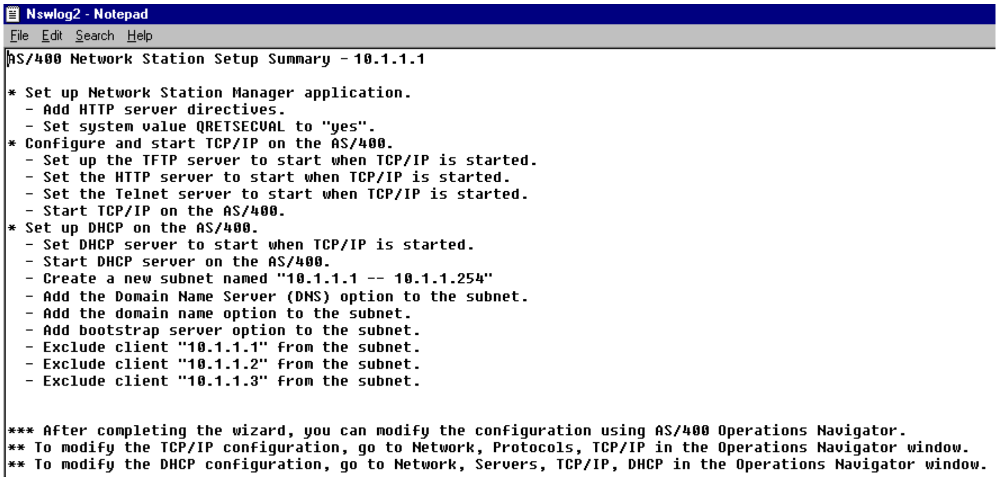
Network Station will now be available within the following range:
10.1.1.1 -- 10.1.1.254

Click Finish to set up the following for this AS/400:

* Set up Network Station Manager application.
* Configure and start TCP/IP on the AS/400.
* Set up DHCP on the AS/400.

Figure 111. AS/400 Network Station Setup Wizard Summary

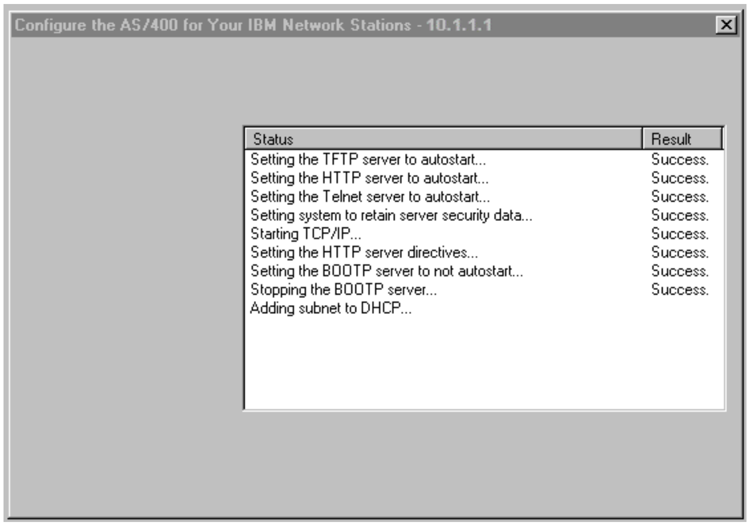
If you need to view details regarding the provided information and the tasks that the AS/400 Network Station Setup Wizard is going to perform on our AS/400 system, click **Details**. A NotePad window displays containing an AS/400 Network Station setup summary. Refer to Figure 112. To close the NotePad window, select **File->Exit** from the menu bar.



```
AS/400 Network Station Setup Summary - 10.1.1.1

* Set up Network Station Manager application.
  - Add HTTP server directives.
  - Set system value QRETSECVAL to "yes".
* Configure and start TCP/IP on the AS/400.
  - Set up the TFTP server to start when TCP/IP is started.
  - Set the HTTP server to start when TCP/IP is started.
  - Set the Telnet server to start when TCP/IP is started.
  - Start TCP/IP on the AS/400.
* Set up DHCP on the AS/400.
  - Set DHCP server to start when TCP/IP is started.
  - Start DHCP server on the AS/400.
  - Create a new subnet named "10.1.1.1 -- 10.1.1.254"
  - Add the Domain Name Server (DNS) option to the subnet.
  - Add the domain name option to the subnet.
  - Add bootstrap server option to the subnet.
  - Exclude client "10.1.1.1" from the subnet.
  - Exclude client "10.1.1.2" from the subnet.
  - Exclude client "10.1.1.3" from the subnet.


*** After completing the wizard, you can modify the configuration using AS/400 Operations Navigator.
** To modify the TCP/IP configuration, go to Network, Protocols, TCP/IP in the Operations Navigator window.
** To modify the DHCP configuration, go to Network, Servers, TCP/IP, DHCP in the Operations Navigator window.
```

Figure 112. Window containing the AS/400 Network Station Setup Summary

14. As shown in Figure 113, the AS/400 Network Station Setup Wizard is performing the IBM Network Station Manager setup on the AS/400 system. Once the setup is finished, the AS/400 system will be ready to address the network stations requests.


Configure the AS/400 for Your IBM Network Stations - 10.1.1.1

Status	Result
Setting the TFTP server to autostart...	Success.
Setting the HTTP server to autostart...	Success.
Setting the Telnet server to autostart...	Success.
Setting system to retain server security data...	Success.
Starting TCP/IP...	Success.
Setting the HTTP server directives...	Success.
Setting the BOOTP server to not autostart...	Success.
Stopping the BOOTP server...	Success.
Adding subnet to DHCP...	

Figure 113. IBM Network Station Manager setup on the AS/400 system

Chapter 5. Boot and login process

The process for booting a Network Station is explained in the 2.3, “The boot process architecture” on page 20. It looks closely at how individual servers are used and the design issues involved in setting them up.

This chapter takes the theoretical discussion further, by providing details on the configuration required, along with an example.

5.1 Network Station boot services

The working environment of a Network Station is provided by a number of different servers, or rather services or server functions, on the network. These services can all be installed onto one single server, which is common in small networks, or onto multiple separate servers with each server supporting one or more services. Many larger environments that distribute the Network Stations to remote branches use the concept of separating servers. This allows administrators to locate each server at the best place in the network in terms of performance, accessibility, and manageability.

The Network Station uses the following servers (services):

- A DHCP or BOOTP server to provide the Network Station with information such as its own IP address, the base-code server address, the address of the workstation configuration server, etc.
- A DNS server to provide information about mapping between the hostname of machines on a network and their IP addresses.
- An IBM Network Station Manager (NSM) server to configure user and workstation configuration settings.
- A base-code server or boot server to provide the Network Station with its operating system (boot file) and its local applications.
- A workstation or terminal configuration server to provide workstation configuration information.
- A user configuration server to provide user configuration information. The user configuration information is usually provided by the authentication server. It is possible to define a server other than the authentication server to serve user configuration information by using the nslduser.cfg file.
- An authentication and home directory server to provide user authentication and the site for the users’ home directory.
- An application server to provide the applications such as the emulator or browser functions. This function is currently implemented on the boot server.

5.2 What’s new in NSM V2R1

The Network Station Manager V2R1 provides the following new boot elements:

- New boot code for the Network Station Series 2800 and Series 2200 models (x86-based CPU)
- A new Network Station operating system that supports thread, preemptive multi-tasking and improves load time

- Design enhancements that reduce the number of files read and downloaded to the Network Station
- Separation of the user configuration service and authentication service

5.3 Boot flows and events

An overview of how the boot process occurs is shown in 2.3, “The boot process architecture” on page 20. Here, quickly summarize this process and then go into more detail.

The boot process is transparent to Network Station users. However, administrators have to configure the Network Station working environment before it can be accessed by users. This configuration is performed in two places:

- **DHCP (or BOOTP) server or NVRAM**

  The DHCP (or BOOTP) server allows the administrator to centrally define settings for the Network Stations, either individually for specific Network Stations or generically for all or a group of Network Stations. These settings determine where the Network Station servers are and the IP address for the Network Station itself.

  For test purposes or in small environments, the administrator can, instead, configure these settings in the Network Stations’ NVRAM setup utility.

- **Network Station Manager (NSM)**

  NSM allows the administrator to centrally define the workstation and user settings. To simplify this, NSM ships with a number of predefined configuration settings. Chapter 8, “Network Station Manager” on page 161, offers more information about the NSM configuration.

An overview of the boot process is shown in Figure 114.

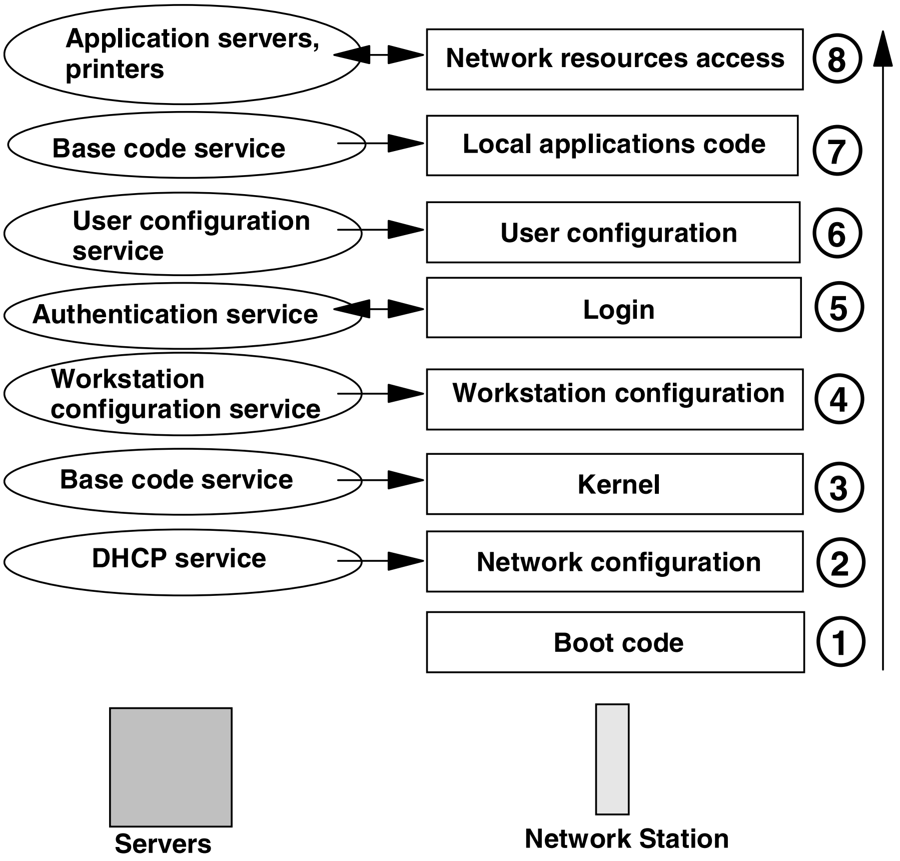


Figure 114. Boot flow overview

The boot flow is explained in the following sections.

Note: Each step corresponds to the numbers in Figure 114.

Step 1: Boot code

The boot code or boot monitor of a Network Station enables the machine to test its hardware and see that it is fully functional.

Step 2: Network configuration request

After the hardware test, the Network Station attempts to download its operating system. To do this, it needs to insert into the network with a TCP/IP address and request its operating system file from the boot server.

If this information was defined in NVRAM, the boot code uses the NVRAM information to locate its boot and workstation configuration server, etc., and download its operating system. The NVRAM setup utility is part of the boot code. If the Network Station is configured to request its own IP address and the IP addresses of the boot, workstation configuration server, etc. from a DHCP (or BOOTP) server, it does a DHCP broadcast to call for this information and attempts to download its operating system.

Step 3: Operating system download

Once the Network Station is assigned a valid TCP/IP address and knows where to find its operating system (provided by the base-code server), it accesses the base-code server and attempts to download the operating system kernel file.

The boot code uses the protocol (TFTP or NFS) as specified in DHCP or NVRAM to download the kernel. The kernel then always tries to mount its root file system via RFS first. On the AS/400 system, the mount succeeds, and the rest of the operating system files are accessed via RFS. On Windows NT and AIX, the RFS mount fails, so the kernel tries NFS next. That mount succeeds, and the rest of the operating system files are accessed via NFS.

The kernel file names and size for each Network Station model are shown in Table 17.

Table 17. Network Station kernel file names and sizes

Network Station model	Kernel file name	Kernel size (KB)
Series 300	kernel.300	Not yet available
Series 1000	kernel.1000	Not yet available
Series 2200	kernel.2200	1275
Series 2800	kernel.2800	1247

After downloading, the kernel executes three programs:

- **init**

  The init module establishes much of the initial operating environment for the kernel and its applications. This involves processing the $ProdBase/<x86|ppc>/etc/fstab file to establish any additional NFS or RFS mounts to systems on the network.

- **makedevices**

  The makedevices module mounts the particular devices necessary for applications and activates any additional device drivers, such as a file system for flash cards.

- **sh**

  The sh module reads the $ProdBase/<x86|ppc>/.profile shell script. This creates environment variables. It does not establish all environment variables, only the ones necessary to allow the kernel to load and execute other programs, such as X-windows support, the window manager, and the main login process. The shell script loads the NC Registry daemon that is populated using the boot information from the boot code.

Step 4: Workstation configuration download

The NC Registry daemon downloads and reads the following files from the server providing the workstation configuration service.

- `$UserBase/profiles/shipped.nsm`

  This file contains the IBM-shipped default settings. This is a static file and is never changed through NSM (though new releases of NSM may ship with new settings to support new features).

- `$UserBase/profiles/allncs.nsm`

  This file contains the workstation preferences defined at the system level in NSM.

- `$UserBase/profiles/ncs/hostname.nsm`
  `$UserBase/profiles/ncs/MACaddress.nsm`
  `$UserBase/profiles/ncs/IPaddress.nsm`

  These three files, if they exist (they won't initially), contain NC-specific preferences configured in NSM. Each Network Station can be configured individually. They are then identified either by their hostname, MAC address, or IP address.

Step 5: Login and user authentication
The login program, called ACTlogin, is loaded and the login dialog box is displayed. Once the login information is provided by the user, the Network Station contacts the authentication server to validate the user.

If an nslduser.cfg file exists on the authentication server and an entry exists for the Network Station, the user configuration profile is loaded from the user configuration server specified in the file. If a match is not found, the user configuration profile is loaded from the authentication server.

Using the nslduser.cfg file, it is possible to separate the user configuration files from the authentication or home directory server.

Step 6: User configuration download
The NC Registry daemon downloads the following files that are located on the server providing the user configuration service:

- `$UserBase/profiles/allusers.nsm`

  This file contains the system-level default settings.

- `$UserBase/profiles/groups/<group>.nsm`

  This file contains the group-specific settings made for the <group>.

- `$UserBase/profiles/users/<user>.nsm`

  This file contains the user-specific settings made for the <user>.

Step 7: Local applications downloaded on user demand
The desktop is built and displayed according to the settings in the configuration files. From their desktop, the user can launch local applications or emulators to access resources on the network. The local applications, such as the emulators, ICA client, Netscape Communicator, and so on, are downloaded from the base-code server on user demand.

Step 8: Network resources access
Once the user starts the local applications, they need, they can access the network resources that are available (application server, Web servers, print servers, file servers, and so on).

When the user logs off, the Network Station performs a cleanup and restarts from step 5. A new user can then login and get their personal desktop and preferences. The Network Station's kernel file, NC download profiles, and so on are only loaded at boot time. They are not re-read when a user logs out.

5.4 Network Station boot code

Each Network Station boot has code that is automatically invoked at power on. The boot code performs functions similar to the BIOS code available in PCs. It enables the Network Station to perform a self test, Power-On Self Test (POST), and verify its hardware is fully functional. Then, it attempts to download its operating system. The boot code is called *Boot Monitor* for PowerPC models and *NC Boot Code* for x86 models.

The boot code is responsible for the following tasks:

- **Power-On Self Test (POST)**: A basic hardware test performed before loading the operating system.
- **Basic hardware and TCP/IP configuration**: Through NVRAM or DHCP request.
- **Boot the operating system**: Through a network connection or from a local flash card into RAM, and run it.
- **Diagnostic tests**: Accessible from the setup utility for problem determination.
- **System firmware flash update**: Downloads a binary image that will be programmed into the Network Station's (EPROM) to update the boot code.
- **Adapter flash update**: Supports downloading and updating the flash image on the Token-Ring or Ethernet adapter on Network Stations.

5.4.1 PowerPC models (Series 300 and Series 1000)

The Boot Monitor used by the PowerPC models in NSM V2R1 has not changed since NSM V1R3. Therefore, the menus look the same as in earlier NSM releases.

The setup utility is accessible by pressing the Esc key when the `NSB11000 memory in megabytes ...` message is displayed after power-on.

The diagnostics utilities are accessible as a command line interface from the setup utility by pressing and holding down Left Ctrl+Left Alt+Left Shift+F1.

5.4.2 x86 models (Series 2200 and Series 2800)

The boot code used by the x86-based Network Stations has different menus compared to the PowerPC-based models, but offers the same functionality.

Attention

The earliest Series 2800 Network Stations may have a firmware version, such as H2033190, which must be updated by using a special procedure. When these early Network Stations are powered on for the first time, the user must quickly choose from the following operating systems:

- WSOD
- Other
- Auto

Choose option `2` (Other) quickly since option 3 is chosen by default after 10 seconds (you do not want option 3). As stated in Appendix C of *Using IBM Network Station Manager,* SC41-0690, if you choose the WSOD option in error, you must follow the steps given in Appendix D of the same manual, to return to the screen where you can select the correct option. If you choose Auto in error, restart the Network Station, and then select option `2`.

The setup utility is accessible by pressing the Esc key when the Network Station icon or the `NSB11000 memory in megabytes ...` message is displayed after power on. Please note that it may take several seconds for the current process to halt. The Network Station icon is displayed, when verbose messages are disabled and the `NSB11000 memory in megabytes ...` message is displayed (along with others) when verbose messages have been enabled (through the Setup Utility).

The diagnostics utilities on the x86-based models are menu driven, instead of command-line driven. They are accessible by selecting Service Aids in the setup utility. The menus integrate the necessary functions found in the PowerPC-based command line version.

5.5 Boot parameters configuration

After the Power-On Self Test, the Network Station boot code attempts to download the operating system (the kernel file). The boot code performs this operation based on the Network Station IP settings and some boot parameters. The boot parameters indicate from where and with which protocol to download the operating system and configuration files. The administrator has to configure the TCP/IP and boot parameters either locally with the setup utility menu screens or using DHCP (or BOOTP) servers.

5.5.1 NVRAM configuration

The following tables list the possible configuration options provided locally in the Network Station's setup utility (NVRAM) for both the PowerPC-based and x86-based Network Station models. The tables also include the default values that are set from the factory or set after a factory reset has been performed.

5.5.1.1 PowerPC models (Series 300 and Series 1000)

On the PowerPC-based Network Stations, the setup utility is accessible by pressing the Esc key when the `NSB11000 memory in megabytes...` message is displayed after power on. Table 18 shows the values that can be modified in the setup utility for the PowerPC models.

Table 18. PowerPC models setup utility

Labels and fields	Values	Default value
F2: View Hardware Configuration		
F3: Set Network Parameters		
IP Addressed from	Network NVRAM	Network
NS IP Address	x.x.x.x (IP address)	
Boot Host IP Address: First Host Second Host Third Host	 x.x.x.x x.x.x.x x.x.x.x	
Configuration Host IP Address: First Host Second Host	 x.x.x.x x.x.x.x	
Gateway IP Address	x.x.x.x	
Subnet Mask	x.x.x.x	
Broadcast IP Address	255.255.255.255	
F4: Set Boot Parameters		
Boot File		
TFTP Boot Directory		
NFS Boot Directory		
Boot Host Protocol: TFTP Order NFS Order Local Order	 Disabled/1/2/3 Disabled/1/2/3 Disabled/1/2/3	 TFTP: 1 NFS: 2 Local: Disabled
F5: Set Configuration Parameters		
Configuration File		
Configuration Directory: First Second		
Configuration Host Protocol: First Second	 Default, TFTP, NFS, RFS/400, Local Default, TFTP, NFS, RFS/400, Local	
F6: Set Monitors Parameters		

Labels and fields	Values	Default value
F2=Set Monitor Resolution	Automatic Detection (DDC) 640 by 480 at 60 Hz 640 by 480 at 72Hz 640 by 480 at 75Hz 640 by 480 at 85 Hz 800 by 600 at 72 Hz 800 by 600 at 75 Hz 800 by 600 at 85 Hz 1024 by 768 at 43 Hz 1024 by 768 at 60 Hz 1024 by 768 at 70 Hz 1024 by 768 at 75 Hz 1024 by 768 at 85 Hz 1280 by 1024 at 60 Hz 1280 by 1024 at 70 Hz 1280 by 1024 at 75 Hz 1600 by 1200 at 48 Hz	Automatic Detection (DDC)
F4=Monitor Power Management Disabled	Enabled / Disabled	Disabled
F7: Set Language Parameters		
F2: Select Keyboard Language	53 languages	13. US English
F3: Select Startup Language	6 languages	English
F10: Set Verbose Diagnostic Msg	Enabled / Disabled	Disabled

5.5.1.2 x86 models (Series 2200, Series 2800)

On the x86-based Network Stations, the setup utility is accessible by pressing the Esc key the Network Station icon or when the `NSB11000 memory in megabytes ...` message is displayed after power on. Table 19 shows the values that can be modified in the setup utility for the x86 models.

Table 19. x86 models setup utility

Labels and fields	Values	Default value
Change language settings		
	5 languages	English
Change keyboard settings		
	21 languages	English (US)
Change display settings		
Color palette	High color (16 bit) 256 colors (8 bit)	High color (16 bit)

Labels and fields	Values	Default value
Resolution and frequency	640 by 480 at 60 Hz 640 by 480 at 75Hz 640 by 480 at 85Hz 800 by 600 at 60 Hz 800 by 600 at 75 Hz 800 by 600 at 85Hz 1024 by 768 at 43 Hz 1024 by 768 at 60 Hz 1024 by 768 at 75 Hz 1024 by 768 at 85 Hz 1280 by 1024 at 60 Hz 1280 by 1024 at 75 Hz 1280 by 1024 at 85 Hz 1600 by 1200 at 48 Hz 1600 by 1200 at 60 Hz 1600 by 1200 at 75Hz 1600 by 1200 at 85Hz	
Power Management	Disabled Enabled	Disabled
Configure Network Settings		
Network priority: DHCP BOOTP Local (NVRAM)	 Disabled/first/second/third Disabled/first/second/third Disabled/first/second/third	 First Second Disabled
Boot file source	Network Flash	Network
Network Station IP address	x.x.x.x	
DNS IP address	x.x.x.x	
Gateway IP address	x.x.x.x	
Subnet mask	x.x.x.x	
TFTP subnet broadcast	Disabled Enabled	Disabled
Block size in bytes	512 to 8192	4096
Line speed automatic negotiation Line speed (if negotiation is disabled) Duplex (if negotiation is disabled)	Enabled/Disabled 10/100 (Ethernet), 4/16 (Token Ring) Half/Full	Enabled
Token Ring MTU size (only TR models)	256 to 16384	1492
Ethernet Standard (only Eth models)	Version 2 IEEE802.3	Version 2
Change boot file server settings		
Boot file server IP address: First Second Third	 x.x.x.x x.x.x.x x.x.x.x	

Labels and fields	Values	Default value
Boot file server directory and file name: First server Second server Third server **Note:** These reflect the use of a Series 2800. If a Series 2200 is being used then the kernel.2200 would be used instead of kernel.2800.	**NT**: /NetworkStationV2/prodbase/x86/kernel.2800 **AS400**: /QIBM/ProdData/NetworkStationV2/x86/kernel.2800 **AIX**: /usr/NetworkStationV2/prodbase/x86/kernel.2800 Customized entry	**First**: /usr/NetworkStationV2/prodbase/x86/kernel.2800 (AIX) **Second**: /QIBM/ProdData/NetworkStationV2/x86/kernel.2800 (AS400) **Third**: /usr/NetworkStationV2/prodbase/x86/kernel.2800 (AIX)
Boot file server protocol: TFTP NFS	 Disabled/first/second/third Disabled/first/second/third	 First Second
Change workstation configuration server settings		
Workstation configuration server IP address: First Second	 x.x.x.x x.x.x.x	
Workstation config. server directory: First Second	**NT**: /NetworkStationV2/userbase/profiles/ **AS400**: /QIBM/UserData/NetworkStationV2/profiles **AIX**: /usr/NetworkStationV2/userbase/profiles	**First**: /usr/NetworkStationV2/userbase/profiles (AIX) **Second**: /QIBM/UserData/NetworkStationV2/profiles (AS400)
Workstation configuration server protocol: First server Second server	 NFS/Boot file server/Flash/RFS NFS/Boot file server/Flash/RFS	 Boot file server Boot file server
Change authentication server settings		
Authentication server IP address: First Second	 x.x.x.x x.x.x.x	
Authentication server protocol First server Second server	 RAP RAP	
Display Hardware information		
Display boot log		
Change verbose diagnostic settings		
	Disabled Enabled	Disabled
Service aids		
Change firmware support	BIOS for Workspace On Demand NS Boot for Network Station Manager Automatic Selection	

Labels and fields	Values	Default value
Change local MAC address: Permanent MAC address Enable local MAC address Local MAC address	Disabled/Enabled	Disabled
Change fast boot settings	Disabled/Enabled	Disabled
Change retry settings: Boot file server retry count TFTP delay time between retries in sec Maximum TFTP retry count NFS delay time between retries in sec Maximum NFS retry count Network priority retry count	 10 6 10 6 10 1	
Change NS boot themes setting	Black background with white text White background with black text Steel blue background with light gray text Blue background with white text	Steel blue background with light gray text
Load factory defaults		

5.5.2 DHCP configuration

Section 3.4.2, “Obtaining an IP address” on page 49, gives an overview of how DHCP works and when you should use a DHCP server. As we learned in that section, any DHCP server can be used to provide network settings to Network Stations (for example, a Microsoft Windows NT 4.0 DHCP server or an IBM eNetwork On-Demand Server DHCP server). However, the standard DHCP configuration usually used with traditional client devices is not sufficient for Network Station devices. Since the Network Station needs to load its operating system and configuration information from servers on the network, it needs the DHCP server to pass that information to it. A PC that has a local hard disk does not need this information.

Therefore, to use Network Stations in a “PC DHCP environment”, some additional options must be configured in the DHCP server. If the DHCP server does not send this information to the Network Station, it rejects the DHCP offer and asks again, hoping to get an answer from another DHCP server.

5.5.2.1 DHCP options

Table 20 lists the possible DHCP options that can be used to configure Network Stations. Options that are marked with an asterisk (*) are required options.

Table 20. DHCP options for Network Station

Option	Example	Explanation
1*	255.255.255.0	Subnet mask.
3*	9.24.104.1 9.24.104.254	Router IP address (default gateway). Multiple IP addresses can be separated by a blank.
6*	9.24.104.108	Domain Name Server IP address.
15*	itso.ral.ibm.com	Domain name.
26	1492	MTU size.

Option	Example	Explanation
66*	9.24.104.173	Base code server IP address.
67*	/NetworkStationV2/prodbase/x86/kernel.2800	Boot file path. This example reflects booting a Series 2800 from an NT server. See Table 19 on page 131 for the file when booting from an AS/400 system or AIX.
98	rap://9.24.104.252 rap://9.24.106.118	Authentication server URL. Multiple URLs can be separated by a blank (rap is remote authentication protocol).
211*	nfs	Protocol to use for the base code server. Possible values are tftp, nfs or rfs/400.
212	9.24.104.253 9.24.104.119	Workstation configuration server IP address. Two IP addresses separated by a blank can be specified.
213	/NetworkStationV2/userbase/profiles /QIBM/Userdata/NetworkStationV2/profiles	Workstation configuration files path name for option 212. Two path names separated by a blank can be specified.
214	nfs rfs/400	Protocol to use for option 212. Possible values are nfs or rfs/400. Two protocol separated by a blank can be specified.
219	9.24.104.119	Secondary base code server IP address.

Notes:

- We found that options 67, 211, and 213 were case sensitive. If you have problems with your DHCP configuration, check that any options with a path name use the correct case.
- DHCP options 211, 212, 213, 214 and 219 are vendor-specific options. If you are already using these options for another purpose, you need to configure DHCP on a subnet or class basis to avoid conflicts.
- When two workstation configuration servers are specified, the first server is tried first. If that fails, then the second server is tried. If the second server is successful, then the second value in options 213 and 214 is used.

5.5.2.2 Network Station DHCP classes

The DHCP options have the flexibility to be applied on a network, subnet, or client basis. Some DHCP servers, such as the eNetwork On-Demand DHCP server shipped with NSM for Windows NT, offer the ability to apply the options on a class basis. This allows the DHCP server to determine which type of client is asking for an IP address and then to send the options that each type of client requires.

For example, a Token-Ring Series 1000 Network Station would have the specific class IBMNSM A.2.0 assigned. An Ethernet Series 1000 Network Station would have the class IBMNSM A.5.0 assigned. A DHCP server supporting classes could differentiate between these two types of machines. Settings defined on a class basis would then be applied depending on the class of the Network Station. A thorough discussion on classes and their use can be found in 3.4.2.3, “DHCP server: Which platform and product to use” on page 52.

To mix Network Stations running NSM V1R3 and NSM V2R1 and to mix different types of Network Stations, you need a DHCP server that can support classes. The DHCP Server can send the correct boot file names to each type of Network Station. The IBM eNetwork On-Demand DHCP server shipped with Network Station Manager for Windows NT can do that. The Microsoft Windows NT 4.0 DHCP server is not currently capable of handling classes.

The AS/400 DHCP server also has this class support. For an example of how to use the DHCP class support to aid in the administration of the Network Station boot administration, see 9.2.3, “Scenario 3: V1R3 clients using DHCP” on page 236, and 9.3.3, “Scenario 6: V1R3 and V2R1 clients using DHCP” on page 270.

5.5.3 A comparison of NVRAM versus DHCP

The NVRAM (static IP addresses) configuration is most suitable for testing purposes and in small environments. When you implement Network Stations for production in larger environments, using a DHCP server greatly simplifies the administrative tasks. It allows an administrator to centrally manage the Network Stations boot configurations. However, in certain environments, for example when you have locally attached devices such as printers or serial devices, using static IP addresses can simplify things since they can then be referred to with their IP addresses.

5.5.3.1 Boot parameters comparison

Table 21 shows how the configuration elements are mapped between an NVRAM and DHCP configuration. When using DHCP, some settings are picked up from NSM. The NS boot utility for x86-models is used for the comparison.

Table 21. NVRAM versus DHCP configuration

NVRAM	DHCP
Language settings	NSM: Environment->Language
Keyboard settings	NSM: Hardware->Workstation->Keyboard Settings->Keyboard mapping language
Display settings	
Color palette	NSM: Hardware->Workstation->Monitor settings->Color depth
Resolution & frequency	NSM: Hardware->Workstation->Monitor settings->Preferred monitor resolution
Power Management	Not available in DHCP or NSM.
Network settings	
Network priority: DHCP BOOTP Local (NVRAM)	Not applicable. DHCP is used.
Boot file source	DHCP option 66 and 219
Network Station IP address	DHCP IP address leasing
DNS IP address	DHCP option 6
Gateway IP address	DHCP option 3 (multiple servers can be specified)
Subnet mask	DHCP option 1
TFTP subnet broadcast	Not available in DHCP or NSM. Uses NVRAM default (=Disabled).
Block size in bytes	Not available in DHCP or NSM. Uses NVRAM default (=4096).
Line speed automatic negotiation Line speed Duplex	Not available in DHCP or NSM. Uses NVRAM default (=Enabled).

NVRAM	DHCP
Ethernet Standard	Not available in DHCP or NSM. Uses NVRAM default (=Version 2).
Boot file server settings	
Boot file server IP address: First Second Third	DHCP option 66 DHCP option 219
Boot file server directory and file name: First server Second server Third server	DHCP option 67
Boot file server protocol: TFTP NFS	DHCP option 211
Workstation configuration server settings	
Workstation configuration server IP address: First Second	DHCP option 212 DHCP option 212
Workstation configuration server directory: First Second	DHCP option 213 DHCP option 213
Workstation configuration server protocol: First server Second server	DHCP option 214 DHCP option 214
Authentication server settings	
Authentication server IP address: First Second	DHCP option 98 DHCP option 98
Authentication server protocol: First server Second server	DHCP option 98 DHCP option 98
Display hardware information	Not applicable
Display boot log	Not applicable
Verbose diagnostic settings	Not applicable
Service aids	Not applicable
Change NS boot themes setting	Not applicable
Load factory defaults	Not applicable

5.5.3.2 Multiple server roles configuration

Both NVRAM and DHCP configurations offer some ability to define multiple servers. Table 22 on page 138 shows the number of servers that can be defined by each service.

The implementation of multiple server roles in a Network Station environment provides a failover infrastructure.

Table 22. Multiple server roles

Services	NVRAM	DHCP
Base code server	3	2
Workstation configuration server	2	2
User configuration server (through nslduser.cfg file)	1	1
Authentication server	2	2

5.5.4 Defining a separate server for user configuration files

The nslduser.cfg file allows you to define a server other than the authentication server to serve user configuration profiles. If you want to take advantage of this capability, you must create the nslduser.cfg file yourself and place it on the authentication server.

Note

On Windows NT, the nslduser.cfg file must be created in the $ServBase/configs path.

In an AS/400 environment, the equivalent of an nslduser.cfg file is CONFIGSVR. The Work with Members Using PDM (`WRKMBRPDM FILE(QYTCV2/QYTCNSLD)`) command can be used to create the CONFIGSVR member. After pressing F6 to create a new member, be sure that CONFIGSVR is specified as the source member and TXT is specified as the source type.

After saving this member, the AS/400 Network Station Login daemon server must be stopped using the command:

```
CALL QYTCV2/QYTCUSVR ('ENDTCPSVR ')
```

Restart the server using:

```
CALL QYTCV2/QYTCUSVR ('STRTCPSVR ')
```

The format and contents of CONFIGSVR are identical to those of the Windows NT nslduser.cfg file.

The file has the following format:

```
nsm_userconfig_server = server1 x.x.x.x y.y.y.y
nsm_userconfig_server = server2 x.x.x.x y.y.y.y
...
nsm_userconfig_server = server3 x.x.x.x y.y.y.y
```

Note the following points for this format:

- *n* is less than or equal to 2048.
- *server* is the name of the server where the user configuration profiles are located.

- *x.x.x.x* is a subnet.
- *y.y.y.y* is the subnet mask for the subnet.

Depending on the authentication server type, the nslduser.cfg file or the CONFIGSVR member is read by the ACTlogin program at startup. When the user authenticates, ACTlogin looks for an IP address match between the IP address of the user's Network Station and the subnets defined in the nslduser.cfg file or CONFIGSVR member. If a match is found, the user configuration information is loaded from the server defined to serve the user configuration information for Network Stations in that particular subnet. If a match is not found, the user configuration information is loaded from the authentication server.

5.6 Example: Booting from a single boot server

To illustrate how the setup tasks are different for NVRAM boot and DHCP, we show a simple example. Figure 115 shows an environment where all the services required by the Network Station are installed onto a single server. This is the most simple implementation.

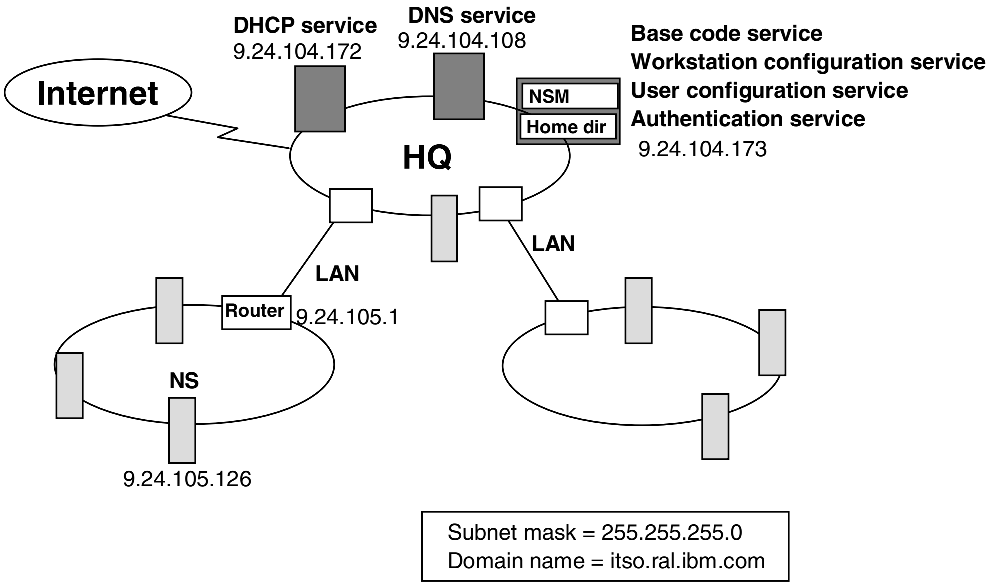


Figure 115. Single boot server implementation

In this example, the operating system, local applications, workstation, and user configuration files are all served by the central site server. The configuration files are maintained by the NSM installed on the central site server. The authentication service is also provided by this server.

Customers will use this implementation if a single server is enough to support the number of Network Stations installed and if the communication links between all Network Stations and the base code server has sufficient bandwidth.

The NVRAM and DHCP configuration parameters corresponding to the infrastructure in Figure 115 are shown in Table 23 and Table 24 for one of the Network Stations (9.24.105.126).

Table 23. NVRAM configuration parameters

Labels and fields	Values
Configure Network Settings	
Network priority DHCP BOOTP Local (NVRAM)	Disabled Disabled First
Network Station IP address	9.24.105.126
DNS IP address	9.24.104.108
Gateway IP address	9.24.105.1
Subnet mask	255.255.255.0
Change boot file server settings	
Boot file server IP address First	9.24.104.173
Boot file server directory and file name First **Note:** On the AS/400 system, the path is: /QIBM/ProdData/NetworkStationV2/x86/kernel.2800	/NetworkStationV2/prodbase/x86/kernel.2800
Boot file server protocol TFTP NFS **Note:** The Boot file server protocol shown is for NT; when booting from an AS/400 the TFTP protocol should be set to First and NFS Disabled.	Disabled First

Table 24. DHCP configuration parameters

Options	Values
IP addresses range definition	[....9.24.105.126...].
1 - Subnet mask	255.255.255.0
3 - Gateway	9.24.105.1
6 - DNS	9.24.104.108
15 - Domain Name	itso.ral.ibm.com
66 - Boot server	9.24.104.173
67 - Boot File **Note:** On the AS/400 system, the path is: /QIBM/ProdData/NetworkStationV2/x86/kernel.2800	/NetworkStationV2/prodbase/x86/kernel.2800

Options	Values
211 - Boot protocol **Note:** The boot protocol in an AS/400 environment would be TFTP.	nfs

Note: To use DHCP, you only need to configure the NVRAM Network priority setting for DHCP. The rest of the settings are not required and the defaults will be used.

Chapter 6. Flash card management

The flash memory booting solution is best employed in environments where booting to a local server is not available. A typical application is in a WAN where a few Network Stations are located in a remote site and it is not cost effective to provide a boot server.

It is also useful in situations where network traffic is already at a maximum. A network with multiple routers and bridges that is experiencing a huge hit from 30 or more Network Stations booting up at 8:00 a.m. on Monday, can reduce the amount of network traffic by deploying flash memory cards within key LAN segments or on the far side of WAN connections.

Each Network Station does not require its own flash memory card to be installed internally. One Network Station with a flash card installed can dispense files to many other units. The unit with the flash card installed is known as a flash-based Network Station. The units downloading files from the flash-based Network Station are known as Peer Stations.

How many Peer Stations can be supported by a single flash-based Network Station? The answer is “it depends”. Initially, the “conservative” thought was to recommend five or so Network Stations per flash card in a V2R1 peer boot or compact flash environment since the base code was larger. However, since the lab was able to peer boot about 30 Network Stations in an “isolated” NSM V1R3 test environment, they decided to do a similar test for V2R1. They were able to peer boot 31 S/2800s within six minutes on a dedicated 10 Mbps Ethernet LAN, and within 4.5 minutes on a dedicated 100 Mbps Ethernet LAN. Remember your actual experience will vary depending on network traffic, the amount of code or applications on the compact flash, and so on. The numbers provided here are not official, but are included to help you identify the best technical solution between cost and performance in your environment.

The configuration steps for *Peer Booting* are discussed in 6.5, “Network Station peer booting” on page 149. A good reference in regard to flash card management is the *IBM Network Station Advanced Information V2R1* publication. To view or print the latest update to this publication, go to:
`http://www.pc.ibm.com/us/networkstation/tech_library.html`

6.1 Prerequisites to building the flash image

Once the V2R1 Network Station Manager software has been installed on the boot server, the system administrator must perform the following steps. It is critical that each of these operations are performed before attempting to use the flash boot function. Not doing so results in failures when building flash images on the client or when booting from flash.

1. Apply the latest V2R1 update. It is a prudent step to ensure that you are working with the latest and greatest code before undertaking a new project.
2. Update the firmware. Flash boot will not work properly on Network Stations that do not have the most recent version of the firmware installed. The firmware date must be 8/20/99 or later. You must update the firmware for any client that will be booting from a flash. We strongly recommend that you update all clients with the latest firmware. Instructions for updating firmware

may be found in Chapter 3 of *Using IBM Network Station Manager V2R1*, SC41-0690, which is online at:

`http://www.pc.ibm.com/us/networkstation/tech_library.html`

Building flash cards for a remote site

The Flash Manager Tool in NSM assumes that you are building a card for the environment in which the NSM server exists. That's not true when you are building cards for a remote site or branch office.

Specifically, the /etc/hosts and /etc/resolv.conf files from the server where the Flash Manager is run are put onto the card image. If it is not edited on the server before the image is created or changed in the <userbase>/flash/Images<ImageName> directory after the image is created, these values will be incorrect. These files are copied onto every card, kiosk mode, or regular boot.

The /etc/resolv.conf file contains the domain name and DNS servers. If these are incorrect (that is, set to your local site values rather than the remote branch), the system will take a long time to boot (waiting for time-outs) and will not be able to connect to any hostnames, only IP addresses. As a solution, you can create a symlink (symbolic link) in the BOM file (/etc/resolv.conf->/tmp/resolv.conf). Then, the Network Station will build the resolv.conf file “on the fly” from the DNS specified via DHCP or NVRAM.

The /etc/hosts file should be edited to remove all of the local hostnames. You can substitute IP addresses or names for the remote systems. Simply leaving /etc/hosts with only the 127.0.0.1 (localhost) entry is probably the best approach.

6.2 Creating the flash image

Use the IBM Network Station Manager to create a flash image on the server. The Flash manager utility is a Java-based application so be sure you have Java enabled in your browser. Follow these steps:

1. Start the flash configuration utility. Click **Administration**, and then choose **Flash Manager** (Figure 116).

   Note: The flash configuration utility is only available at the System preference level.

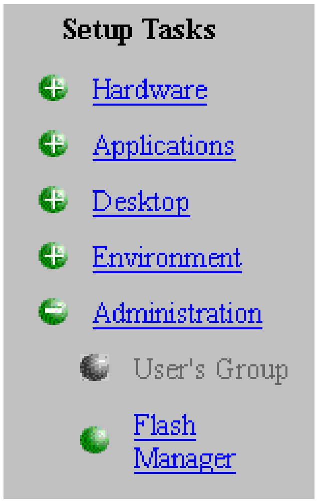
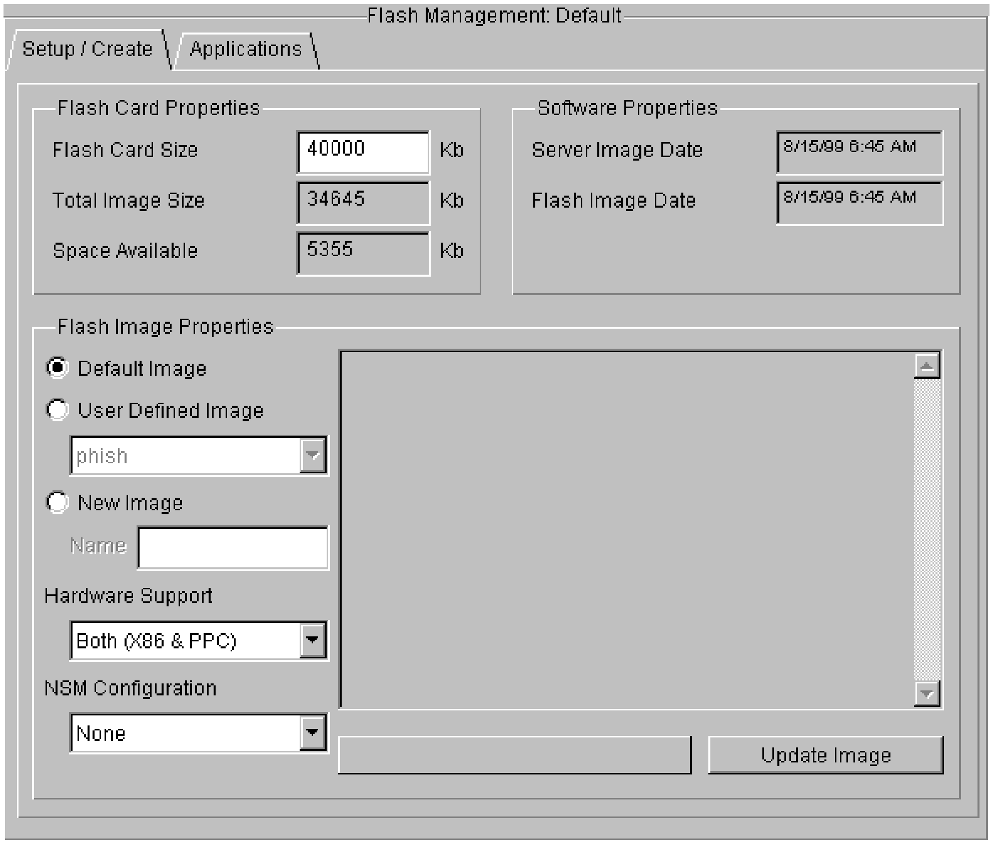


Figure 116. Selecting Flash Manager

The Flash Manager display should look like the example in Figure 117.



Flash Card Properties

Flash Card Size 40000 Kb

Total Image Size 34645 Kb

Space Available 5355 Kb

Software Properties

Server Image Date 8/15/99 6:45 AM

Flash Image Date 8/15/99 6:45 AM

Flash Image Properties

● Default Image

○ User Defined Image

phish

○ New Image

Name

Hardware Support: Both (X86 & PPC)

NSM Configuration: None

Figure 117. Initial Flash Manager display

2. Click the **Create/Setup** tab.

3. Select **Default Image** or **New Image** if you are creating an image for the first time. Selecting New Image allows for the naming and customization of the image to be created.

4. Select **User Defined Image** if previously created images are available and you want to further customize the image or place this particular image into the flash image directory.
5. Enter the size of your flash card (in K bytes) in the Flash Card Size field. Flash Card Properties does not prevent flash images from becoming too large, but helps you understand the size of the flash image.

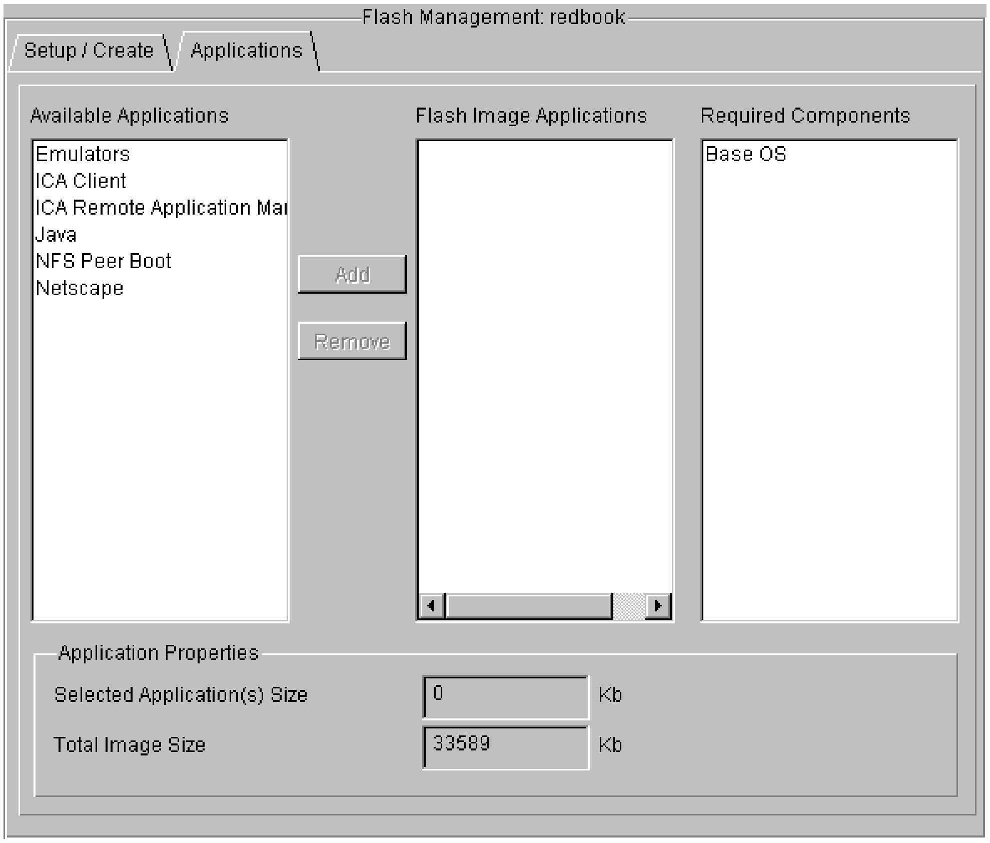
   The Flash Manager tool keeps track of the total image size and the space available on your flash card. As you add applications, the total image size increases and the space available on the flash card decreases. Table 25 shows the amount of space consumed for the different applications to give you an idea of the size of flash card you may need for your environment.

Table 25. The amount of space used for a flash image based on application

Applications on Series 2200 or 2800	Size in MB
Emulators (5250, 3270, VT)	6
ICA client	2
Java (JVM 1.1.8)	13
NFS Peer Boot	4
Netscape	20 (with built-in Java Virtual Machine)
Base OS (mandatory)	32

6. Select the Network Station platforms for which the new image is to be created. For example, click **Both** (X86 & PPC) under Hardware Support to specify both X86 and PPC client support. Select which IBM Network Station Manager configuration files to include in the flash image. For example, click **None** under NSM Configuration to specify that you are not configuring a flash image for a kiosk.
7. Click the **Applications** tab (Figure 118).
8. Select an application from the column on the left, and click **Add** to add an application to the flash image. Refer back to Flash Card Properties under the Create/Setup tab to monitor the Space Available on the flash card.

   Note: Space Available is not an exact representation of the size left on your flash card. Space Available is an approximation of the size of the applications minus the size of your flash card.



Available Applications

- Emulators
- ICA Client
- ICA Remote Application Mai
- Java
- NFS Peer Boot
- Netscape

Flash Image Applications

Required Components

- Base OS

Application Properties

Selected Application(s) Size: 0 Kb

Total Image Size: 33589 Kb

Figure 118. Flash Manager Applications display

9. Click the **Create/Setup** tab.
10. Click **Update** to save the flash image on the server.

6.3 Configuring the Network Station for a flash boot

The Network Stations with a flash memory card installed (otherwise known as flash-based Network Stations) must be configured to boot from flash first and over the network second. The following series of steps takes you through the configuration process:

1. Purchase and install a flash card in the IBM Network Station. See the manual that came with your Network Station for information on how to install the flash card.
2. If you have a type 8363 or 8364 (Series 2200 or 2800) Network Station, use the NS Boot utility to perform the following steps:
    a. On the Configure Network Settings menu, set Boot File Source to **Flash**. This field indicates if the Network Station should boot over the network or from a flash card. There are circumstances that can cause the Network Station to switch from flash boot to network boot even when the boot file source field is set to flash.
    b. On the Change Boot File Server Settings menu, set the second Boot file server IP address to the boot server on your network. The first boot file server IP address is ignored because the Network Station is booting from

flash. If you do not configure a boot server, the flash image cannot be created or updated. You can set the third boot file server IP address to a backup boot server.

c. On the Change Boot File Server Settings menu, set the first Boot file server directory and file name to `/kernel.<xxxx>` where `<xxxx>` is the appropriate series number for your Network Station (2200 or 2800). The second and third boot file server directory and file names should match the appropriate directory boot server specified in the Boot file server IP address field.

d. On the Change Boot File Server Settings menu, set the Boot file server protocol to the appropriate protocol for your boot servers. When booting from flash, this protocol is ignored.

e. On the Change Workstation Configuration Server Settings menu, set the Workstation configuration server IP address to the IP address of the server where the Network Station should obtain the workstation configuration information. If the flash image contains kiosk files, this field is ignored.

f. On the Change Workstation Configuration Server Settings menu, set the Workstation configuration server directory to the appropriate server directory for configuration files. If the flash image contains kiosk files, this field should be set to `/termbase/profiles/`.

g. On the Change Workstation Configuration Server Settings menu, set the Workstation configuration server protocol to the appropriate workstation server protocol. If the flash image contains kiosk files, set this field to **Flash**. *Do not* leave this field set to the default value (Boot file server).

h. On the Change Authentication Server Settings menu, set the Authentication server IP address to the IP address of the authentication server. You must specify an authentication server unless the flash image contains kiosk files.

6.4 Updating the flash card with the flash image

If the Network Station is configured to boot first from flash and second from the network, then the following events occur at power on:

1. The Network Station attempts to locate the kernel file (kernel.<xxxx>, where <xxxx> is 2800, 2200, 1000, or 300) on the flash card. If the kernel file is not found on the flash card, the Network Station attempts to boot over the network. If the kernel file is found on the flash card, the Network Station continues to boot from the flash card.
2. When the Network Station is booting from the flash card, the check for flash image updates (boot-flash-update) flag is tested on the secondary boot server. If the flag is set to yes, the flash image on the Network Station is compared to the flash image on the (secondary) boot server. If an update is required, the Network Station switches to boot from the network. This causes the Network Station to boot from the secondary boot server.
3. When the Network Station is booting from the network and a flash card is installed, the following actions apply:

   a. If the flash card is empty, the server flash image is written to the flash card. Then the Network Station automatically reboots from a flash.

b. If the flash card is not empty, the check for flash image updates (boot-flash-update) flag is tested on the secondary boot server. If the flag is set to yes, the flash image on the Network Station is compared to the flash image on the (secondary) boot server. If an update is required, the server flash image is written to the flash card. Then, the Network Station automatically reboots from flash.

If errors are encountered while attempting to create or update the flash image, the Network Station continues to boot from the network until the operation is completed successfully.

6.5 Network Station peer booting

A Network Station with a flash card installed and the flash image loaded properly can act as a boot server by performing the following steps:

1. Make sure that NFS Peer Boot was added to the flash-based Network Station's flash image in the IBM Network Station Manager flash configuration utility. The flash-based Network Station must have the NFS peer boot in the flash image. Flash-based Network Stations with an NFS peer boot installed automatically launch the NFS daemon when they boot.
2. Make sure that the flash-based Network Station is correctly configured. The flash-based Network Station must have a workstation configuration server specified unless the flash image contains kiosk files.
3. Configure the other Network Stations (Peer Stations) that are going to boot from the flash-based Network Station:

   a. Set the IP address of the flash-based Network Station as the boot server.

   b. Set the boot file name to `/kernel.<xxxx>`, where `<xxxx>` is 2800, 2200, 1000, or 300.

   c. Set the boot file server protocol to **NFS**.

6.6 Kiosk mode configuration for a flash boot

Kiosk mode is well suited for environments where only a single application is needed. See Chapter 16, “Kiosk mode” on page 527, for more detailed information.

The following steps allow the flash image to be created with the proper files for kiosk mode:

1. Follow the steps described in Chapter 16, “Kiosk mode” on page 527, for creating the kiosk files. When the flash image is being created, the Flash manager looks to the $UserBase/profiles/ncs/ directory and includes the configuration files contained within. If no kiosk files exist in this directory, the Flash manager creates a default kiosk image. When the Network Station loads this default kiosk flash image, the only application that is launched is Netscape. This is only useful if the administrator has created a home page from which other Network Station applications can be launched.
2. Access Network Station Manager using a Web browser like Netscape.

3. Follow the same steps outlined in 6.2, “Creating the flash image” on page 144, for configuring the Flash Manager’s Setup/Create display. In the section labeled NSM Configuration, select **Kiosk Files**.
4. Click the **Applications** tab.
5. Select from the Available Applications list the features needed for the kiosk mode and add them to the Flash Image Applications list.
   - If all end users will be running the same application, select only the application type needed to perform this function.
   - If there is a mix of applications being launched in kiosk mode, that is, if End User A runs only a 5250 session and End User B runs only the ICA client, both applications need to be selected from the list. The individual kiosk files in the $UserBase/profiles/ncs/ directory will determine which applications launched on each Network Station.
6. Click the **Setup/Create** tab.
7. Click **Update Image** to create the flash image on the server.
8. Follow the steps for updating the flash card with the flash image described 6.4, “Updating the flash card with the flash image” on page 148.
9. Once the flash image has been successfully mounted on the flash card, make the following changes to the Network Station configuration. These changes need to be applied to all Peer Stations booting off of a flash-based Network Station using the kiosk flash image:
   a. Set the IP address of the Network Station/Flash Server as the workstation configuration server.
   b. Set the workstation configuration server directory to `/termbase/profiles/`.
   c. Set the workstation configuration protocol to **Flash**.

6.7 Flash booting in a DHCP environment

If the network Stations receive their IP addresses from a DHCP server, you should make sure that the DHCP server is configured correctly for flash. Use Table 26 to verify your DHCP configuration.

Table 26. DHCP configuration options and their meaning

Option	Name	Description
3	Router IP	Specifies a list of IP addresses for routers on the client’s subnet.
66	Boot Server IP	Routers should be listed in order of preference.
67	Boot file name	This option is used to identify a boot file.

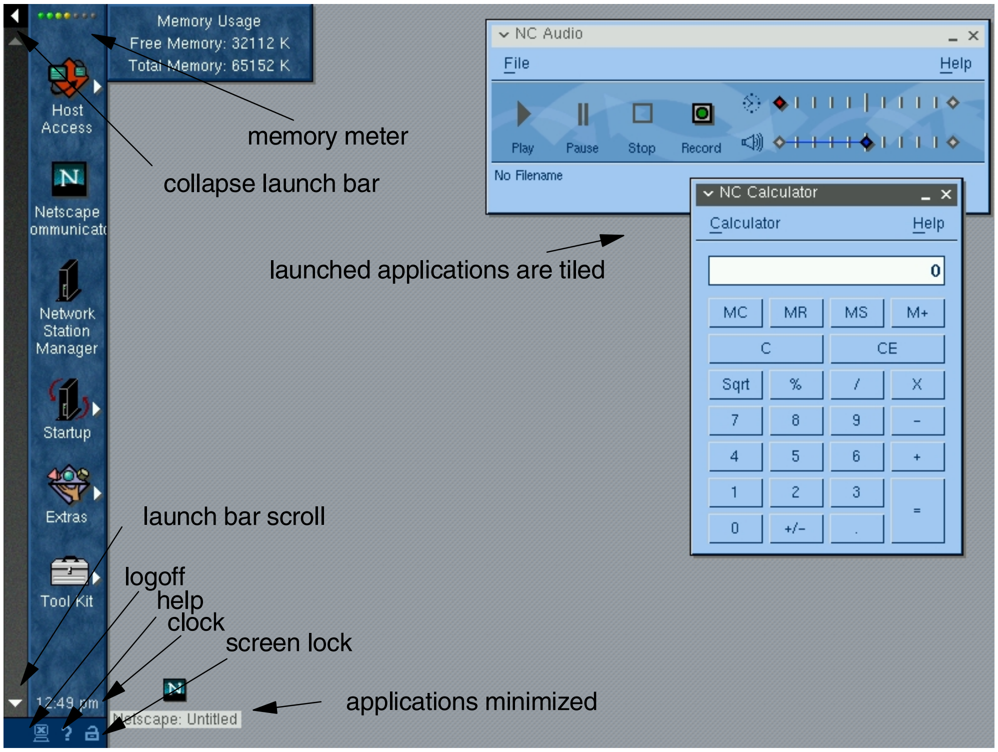
Option	Name	Description
98	Authentication Server	Important for flash-based clients in a DHCP environment. The default authentication server is the boot server. It is not possible to authenticate to a flash-based client. Therefore, a flash-based client must have an authentication server specified (unless the client will be running in kiosk mode). Specify `RAP://x.x.x.x`, where `x.x.x.x` is the IP address of the authentication server.
211	Base Code Server Protocol	Specifies the protocols used by the IBM Network Station when mounting the boot directory on the servers containing the boot file. Up to two protocols may be specified, separated by a blank. The first protocol is used with the server specified by option 66, and the second protocol is used with the server specified by option 219. If only one protocol is specified, it will be used with both servers (if both are specified). Specify **LOCAL** as the first value to indicate a network station client should boot from a flash.
212	Configuration Server IP	Specifies the IP addresses of the servers containing configuration data for the IBM Network Station.
213	Configuration Path	Specifies the directories containing the configuration data for the IBM Network Station.
214	Configuration Protocol	Specifies the protocols to use when mounting the directories on the servers specified in option 212.
219	Second Boot Host IP	Specifies the IP address of a backup boot server.

Chapter 7. NC desktop

NSM V2R1 introduces a new graphical desktop with a task bar and helper applications. This chapter takes a quick look at the new Network Station V2R1 desktop and shows how it is configured with the Network Station Manager. This chapter does not go deep into these matters, because both subjects are covered in *Using IBM Network Station Manager,* SC41-0690.

7.1 The NC desktop

The new look of the NC Desktop is shown in Figure 119.



Memory Usage
Free Memory: 32112 K
Total Memory: 65152 K

Figure 119. The NC desktop

To the left is the Launch Bar that the users use to start their applications. The Launch Bar can be hidden and shown by clicking the minimized arrow in the upper left corner of the screen. When minimized, only the arrow is shown. The location of the Launch Bar is fixed, always vertically at the left of the screen.

At the top of the Launch Bar is the memory meter. When not expanded, it shows the amount of memory used with colored dots. Green indicates that there is a lot of memory left. Orange indicates that there is medium memory usage. Red indicates that the memory is getting full. If the Memory meter is clicked, it expands and shows the total and available amount of RAM. This can be useful to monitor the amount of RAM required when loading certain applications.

The Launch Bar has two kinds of icons on it. The icons with arrows to the right indicate folders that can be expanded and have more icons in them. The icons without arrows are application icons and launch the corresponding application when clicked.

The default folders and applications provided in the IBM-shipped default settings are:

- **Host Access**: Initially this folder includes a 3270 emulator, 5250 emulator, VTxxx emulator, and the ICA remote application manager.
- **Netscape Communicator**: This icon starts Netscape Communicator 4.5.
- **Network Station Manager**: This icon starts a Netscape Communicator 4.5 session and initializes the location to the Network Station Manager URL.
- **Startup**: Applications placed in this folder will start automatically when the user logs on (autostart). This folder is initially empty.
- **Extras**: This folder initially includes the following add-on applications:
  - NC Audio Player
  - Calendar
  - Calculator
  - File manager
  - Paint program
  - Real player
  - Text editor
  - NC Video Player
- **Tool kit**: This folder includes an Advanced Diagnostics command prompt for problem determination and the print monitor for monitoring print jobs on this Network Station.

At the very bottom of the Launch Bar is a digital clock and icons for logoff, online Help, and screen lock.

Applications that are minimized show up as minimized icons on the desktop. The location of the icons can be changed in NSM.

Tips

- You can take a screen capture of the desktop by pressing the keys Alt+Shift+Print Screen simultaneously. To capture only the application in focus, press the Alt+Shift+Scroll Lock keys instead. The images are saved as bitmap files (.bmp extension) in the /registry/documents folder in the user's home directory.
- Pressing Ctrl+Alt+I displays network information.
- Pressing Ctrl+Alt+V displays version information.
- Pressing Ctrl+Alt+L displays the name of the logged on user.
- For more keyboard shortcuts, see Appendix E, “Keyboard shortcuts” on page 623.

The desktop pop-up menu

The *desktop pop-up menu* is a window that appears in the Network Station workspace when a user clicks either mouse button in the workspace (Figure 120). You can perform several tasks from the desktop pop-up menu.

The pop-up menu is enabled and disabled via Network Station Manager (the default is Yes, meaning you have access to the desktop pop-up menu).

When you make a change by using the pop-up menu, the changes take place immediately. The administrator can also configure some of these settings from Network Station Manager (see 7.2.1, “Desktop display options” on page 156).

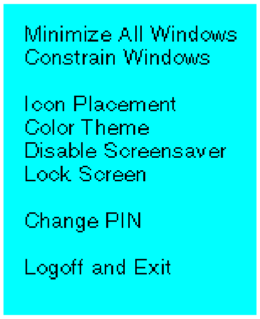


Figure 120. Menu for mouse button click on the desktop

Using these options, you can:

- **Minimize All Windows**: This option is grayed out until you have one or more windows open in the desktop workspace.
- **Constrain Windows**: When this is enabled, you cannot move a window outside the desktop workspace. If this option is disabled, you may accidentally lose a window outside the normal working area.
- **Icon Placement**: This option is also grayed out until you have minimized a session in the desktop workspace. Using this option, you can select how the NC Desktop should arrange the minimized icons. The default is at the bottom of the screen, from left to right.
- **Select color themes**: There are several IBM-supplied color themes that can change the look of the desktop. Changing the desktop theme may change the colors in the Launch Bar, the desktop background (either a solid color or a bitmap picture), the colors used for the applications windows, and so on.
- **Disable Screen Saver**: If the screen saver is configured to start after certain period of mouse and keyboard inactivity, using this option turns the screen saver timer off.
- **Lock Screen**: A password protects the screen. To unlock the screen, you use the same password as entered during the Network Station logon.
- **Logoff and exit**: Does the same thing as clicking the Logoff icon in the Launch Bar.

Tip

The Ctrl+Alt+Backspace key combination is a shortcut for logging off.

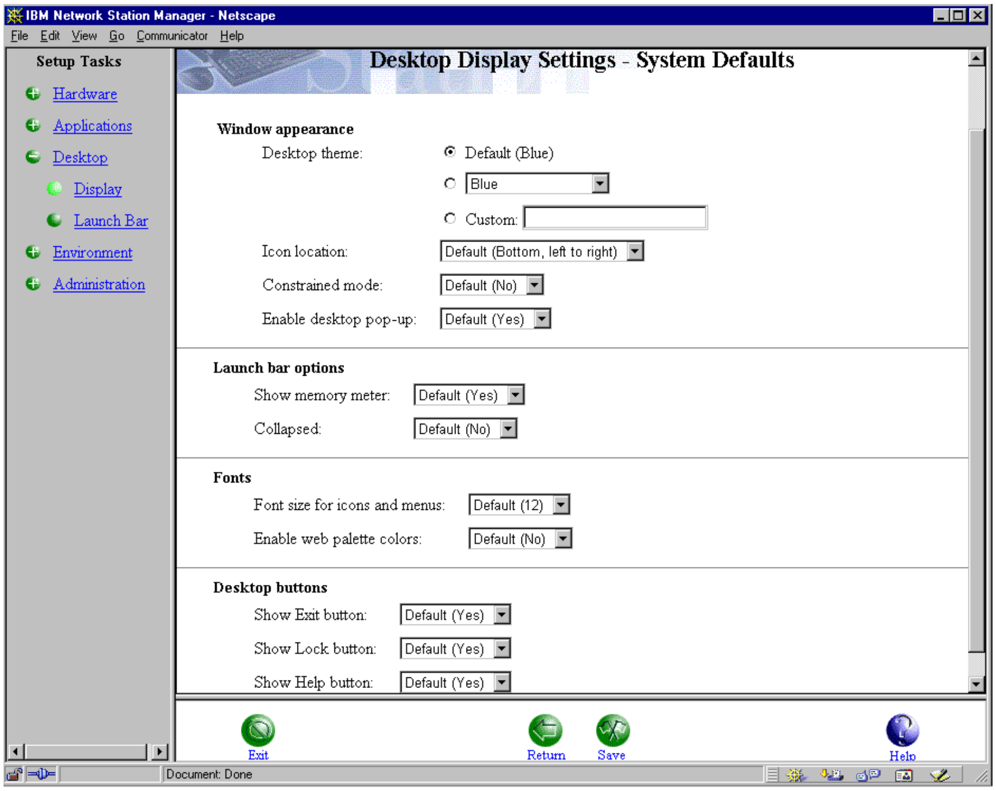
7.2 Managing the NC desktop with Network Station Manager

The Network Station Manager program is used to manage the general configuration properties of the NC desktop and the properties of the Launch Bar.

The desktop settings are defined by selecting **Desktop->Display** and **Launch Bar** options.

7.2.1 Desktop display options

Desktop options can be customized with NSM at the system, group, or user level. Using NSM, select the **Desktop** option under the Display category. On this screen, shown in Figure 121, the administrator can specify Desktop display characteristics including the window appearance, Launch Bar options, fonts, and desktop buttons.



Desktop Display Settings - System Defaults

Window appearance

Desktop theme: ● Default (Blue) ○ Blue ○ Custom:

Icon location: Default (Bottom, left to right)

Constrained mode: Default (No)

Enable desktop pop-up: Default (Yes)

Launch bar options

Show memory meter: Default (Yes)

Collapsed: Default (No)

Fonts

Font size for icons and menus: Default (12)

Enable web palette colors: Default (No)

Desktop buttons

Show Exit button: Default (Yes)

Show Lock button: Default (Yes)

Show Help button: Default (Yes)

Figure 121. Network Station Manager: Desktop Display Settings

The fields are explained in the following list:

- **Desktop theme**: Desktop themes are different colors or graphics that make up the Network Station's desktop color presentation for all areas of the desktop. The default is a blue color theme from the almost 20 color themes that are supplied with the Network Station Manager.

  You can select a predefined color theme from the list, or you can specify a custom file to be used for your color theme. For creating custom desktop themes, see *IBM Network Station Advanced Information V2R1*, for more information. To view or print the latest update, visit the Web site at:

  `http://www.pc.ibm.com/us/networkstation/tech_library.html`

  Desktop themes change the color relationships between the different pieces of the desktop. These pieces include (but are not limited to) the active work area, the Launch Bar area, and the area where the logoff, help, and lock icons are located.

There is also a relationship between desktop themes and desktop background settings found under Monitor settings in the Workstation Hardware Setup Task. The default setting for Desktop background is to use the default value for Desktop theme, which is specified here.

If a change is made to the background, foreground, or a custom file is specified for the background, that change takes precedence over the Desktop theme value.

When creating a desktop theme of your own, you must place the file in the $ProdData/<x86|ppc>/usr/local/nc/registry/desktop/temes directory for it to be picked up by Network Station Manager.

- **Icon location**: Specifies the location where minimized applications (represented by an icon) will appear on the Network Station desktop. Individual users can change the icon location by placing the mouse pointer in their workspace and clicking the mouse. Click **Icon Placement**, and select a new value.
- **Constrained mode**: Constrained mode means that you cannot move any portion of a window out of view on the Network Station desktop. Constrained mode prevents users from losing active windows by inadvertently moving the window out of view.
- **Show memory meter**: The memory meter appears at the top of the Launch Bar on the Network Station desktop. It is used to indicate the amount of memory being used as you open and close applications. It is a series of colored lights starting with green and progressing to yellow and finally red. Green indicates low memory usage, while red indicates you are approaching a point where all available memory is in use.
- **Collapse Launch bar**: You can collapse (hide) the entire Launch Bar on the Network Station. The Launch Bar can be shown again by clicking the small white triangle in the upper-left corner of the NC Desktop.
- **Font size for icons and menus**: You can make the text of the icons and menus larger or smaller by selecting one of the available values (8, 10, 12, 14, 18, and 24 point).
- **Enable Web palette colors**: Enabling this field provides full color palette support for applications. The default is Yes, which means full color palette support is active.

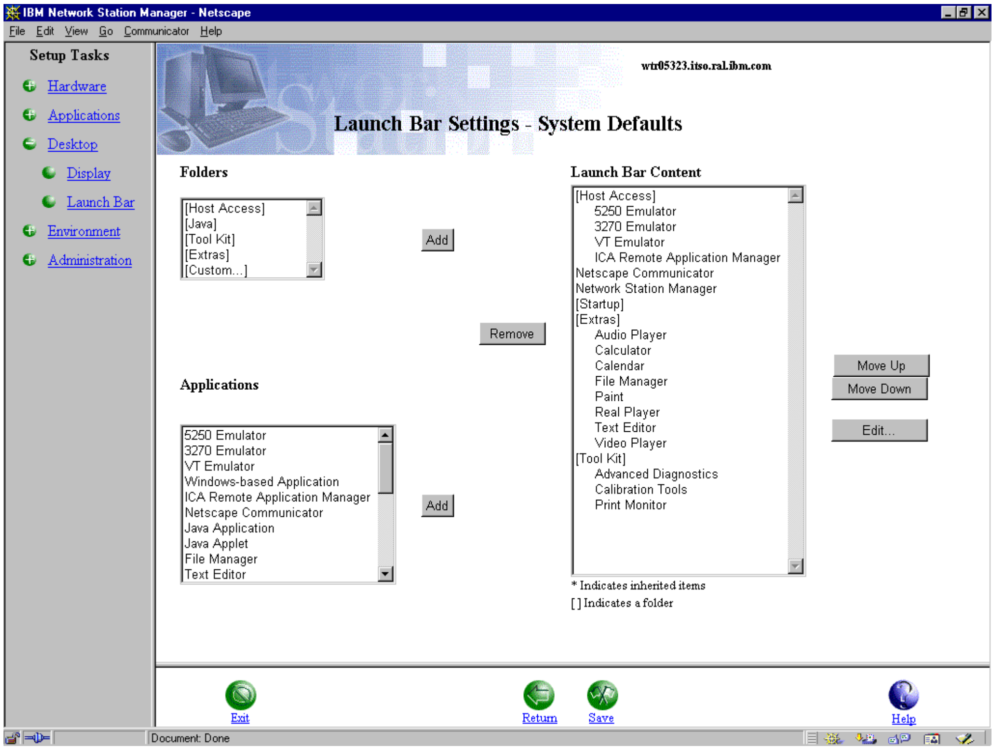
Note

If you are using 8-bit color support or your workstation only supports 8-bit color, enabling a full color palette can produce a conflict with customized color maps used by other applications such as emulators. Enabling may result in an unexpected color appearing in your emulator or other application.

- **Desktop buttons**: Controls whether the exit, lock, and help buttons appear on the desktop. The default is Yes for all these options.

7.2.2 Desktop: Launch Bar

The administrator may modify the contents of the Launch Bar with the Network Station Manager program. The Launch Bar Settings page is shown in Figure 122 on page 158. We do not go into detail on this subject, because it is well covered in *Using IBM Network Station Manager*, SC41-0690.



Folders

[Host Access]
[Java]
[Tool Kit]
[Extras]
[Custom...]

Applications

5250 Emulator
3270 Emulator
VT Emulator
Windows-based Application
ICA Remote Application Manager
Netscape Communicator
Java Application
Java Applet
File Manager
Text Editor

Launch Bar Content

[Host Access]
    5250 Emulator
    3270 Emulator
    VT Emulator
    ICA Remote Application Manager
Netscape Communicator
Network Station Manager
[Startup]
[Extras]
    Audio Player
    Calculator
    Calendar
    File Manager
    Paint
    Real Player
    Text Editor
    Video Player
[Tool Kit]
    Advanced Diagnostics
    Calibration Tools
    Print Monitor

* Indicates inherited items
[ ] Indicates a folder

Figure 122. Launch Bar Settings display in Network Station Manager

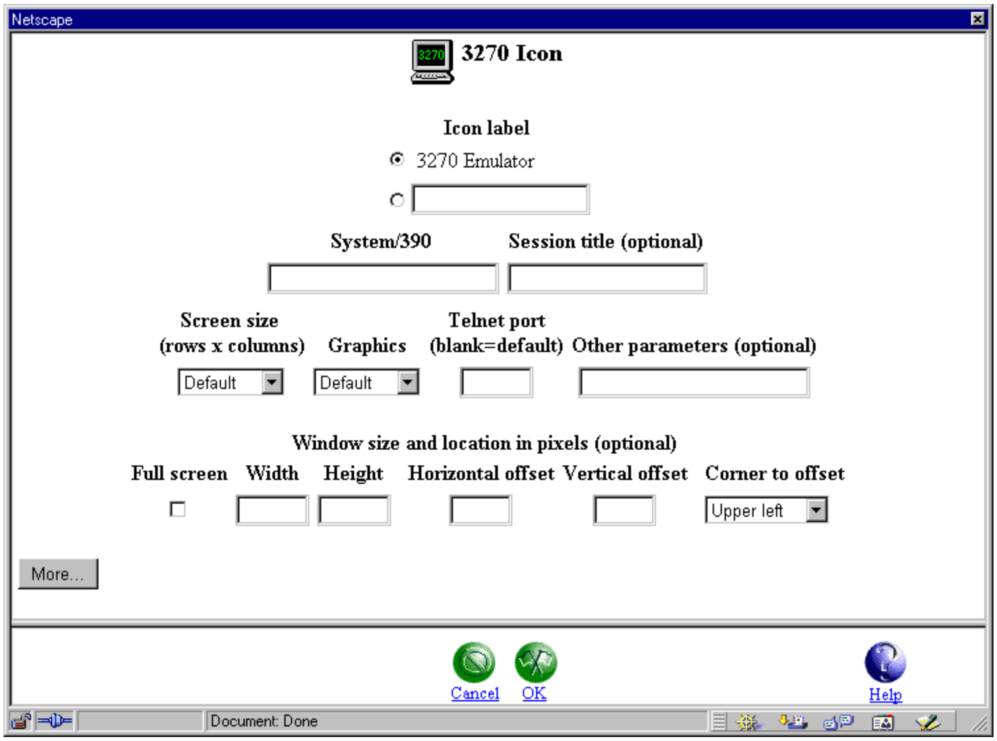
On the page shown in Figure 122, there are three fields:

- Folders list
- Applications list
- Launch Bar Content

The Folders and Applications lists each have an Add button to add items to the launch bar. For example, if you want to add a customized folder, select **Custom...** from the Folders list, and click **Add**. A pop-up window opens asking you to specify a name for the folder. The new folder is added to the last row on the Launch Bar Content list, unless an item in the launch bar list has been selected. If an item in the list is highlighted when you click Add, the item will follow the highlighted item. If you want to change its place (or the order of folders and applications in the list in general), select an item from the Launch Bar Content list and use the Move Up and Move Down buttons.

Applications are added in a similar fashion.

If you want to remove something from the Launch Bar Content list, select the item from the list and click **Remove**. Selecting an item from the Launch Bar Content list and then clicking the Edit button opens a pop-up window in which the administrator can change some options. Figure 123 shows the editable options for the 3270 emulator.



3270 Icon

Icon label

● 3270 Emulator

○

System/390

Session title (optional)

Screen size (rows x columns): Default

Graphics: Default

Telnet port (blank=default)

Other parameters (optional)

Window size and location in pixels (optional)

Full screen □ Width Height Horizontal offset Vertical offset Corner to offset: Upper left

Figure 123. The editable options for 3270 emulator in Launch Bar settings

Note

There is one special folder in the Launch Bar, the Startup folder. It does not have editable options, and the administrator cannot remove the folder from the Launch Bar Contents list. Applications placed in this folder are auto-started when a Network Station user logs on.

Depending of the target level (group or user), some of the items listed in the Launch Bar Content list may have an asterisk (*) after the item name. The asterisk indicates that the item is inherited. For example, if you are modifying the launch bar and select the group preference level, you will see all system applications listed with an asterisk (*).

If an item is inherited from a higher preference level, you cannot modify or remove it. To make changes, you have to return to the main menu and select the preference level (for example, system) where the application was added.

Chapter 8. Network Station Manager

This chapter explains what the Network Station Manager is and how it works. We do not describe all settings available in it, since that is covered in the Network Station Manager publications. Instead, we help you understand what is happening behind the scenes. Plus, we introduce you to some of the tools and tricks that you can use to customize your Network Station installation to suit your particular needs.

8.1 Introduction to Network Station Manager

Network Station Manager (NSM) is the software that works closely together with the Network Station hardware to provide its functionality. NSM includes *all* the software the Network Station needs to be operable. This includes the Network Station’s operating system, fonts and other support files, and local applications such as:

- 3270 emulator
- 5250 emulator
- VT emulator
- ICA client
- Netscape Communicator 4.5 browser
- JDK 1.1.8 environment
- Audio and video player, RealPlayer
- PDF viewer
- Additional utility applications

In addition to providing the Network Station with the necessary software, NSM also includes an administration tool. The administration tool is used for configuring both the Network Station hardware and its applications and to give the Network Station users access to the Network Station applications they need. Since the Network Station is a thin client, it does not contain very much hardware to manage. Therefore, NSM is really targeted at administering and configuring the Network Station software.

For ease of use and intuition, the NSM user interface is browser-based. To make any changes, the administrator or end-user launches a Web browser and connects to the server where NSM is installed. Using panels and dialogs displayed in the browser, the administrator or end-user interacts with NSM and performs the necessary changes. The beauty of having a browser-based user interface is that the administrator can manage the Network Stations from *any platform, anywhere*. It is not necessary to sit at the server console or to install special management software, a browser is all that is needed. And today, a browser is part of every administrators desktop and almost all users’ desktops as well.

8.1.1 Technical overview

To understand what happens behind the scenes when an administrator performs a change and how the Network Station and its user retrieves these settings, see Figure 124 on page 162.

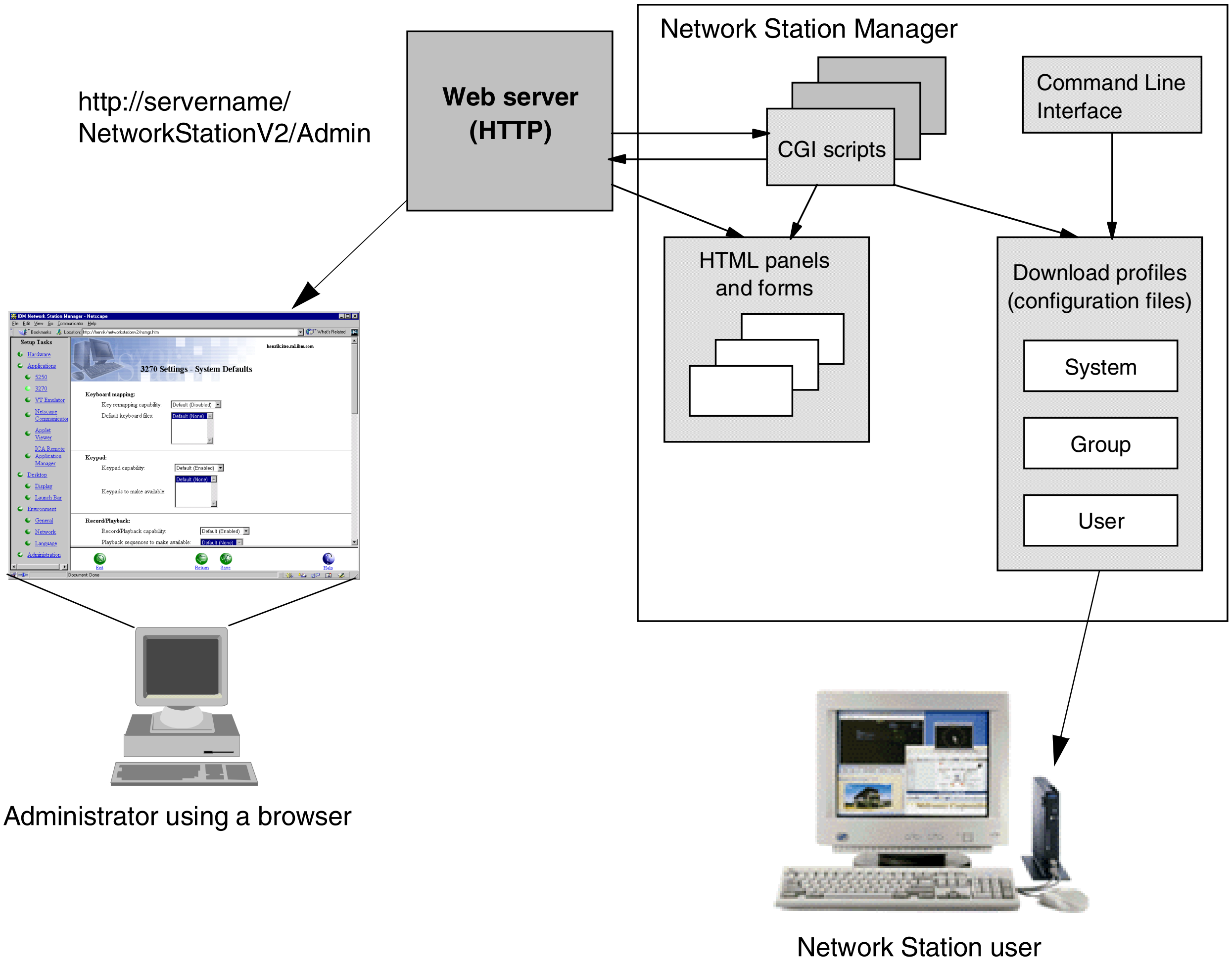


Figure 124. Network Station Manager technical overview

As mentioned earlier, NSM is built using Web technology. When an administrator makes a change, they launch their Web browser and connect to the NSM Web server using the URL `http://servername/NetworkStationV2/Admin`. After an authentication process, the Web server presents the administrator with an interactive Web page with dialogs, input fields, buttons, and so on. This Web page is built from pre-defined HTML panels and forms stored on the Web server. After the administrator makes a change, a number of CGI scripts executing behind the Web server interpret the data sent back to the Web server and retrieve the necessary information. The information is then converted into a format readable by the Network Station and the CGI scripts create (or update) a number of configuration files (download profiles) on the NSM server. When a Network Station user powers on their Network Station, the Network Station reads these configuration files and retrieves the settings from them.

A new feature in NSM V2R1 is the ability to make changes to NSM by using a Command Line Interface (NSMCL) instead of using browser-based GUI. Using the Command Line Interface, changes to NSM configuration files can easily be scripted. It can also be used to make changes to NSM that are not available in the browser-based GUI. This is usually advanced configuration parameters and are not required by the end users.

This overview, except for the Command Line Interface, is true for all versions of Network Station Manager so far.

8.1.2 NC Registry

The NC Registry is a new function included in NSM V2R1. This is a Network Station internal database (or rather information keeper, registry) that holds *all* the configuration settings and preferences during a work session. It has been developed to improve Network Station performance by reducing the number of configuration files that need to be downloaded during boot and login time. NC Registry also makes it easier for local Network Station applications to retrieve their settings by providing a standardized interface for that purpose. The information in the NC Registry is not saved to disk, and the administrators do not need to care about this registry at all. It is purely a Network Station internal function.

The NC Registry runs as a daemon in the Network Station and is responsible for accessing all the download profiles created by NSM. It is also the *only* client code that directly accesses the download profiles. When an application needs to retrieve its settings, it does that from the NC Registry, so an application never directly retrieves settings from NSM.

8.2 Network Station Manager settings

To launch NSM, start your Web browser and connect to:

```
http://servername/NetworkStationV2/Admin
```

The browser presents you with a login dialog. Depending on the group your ID belongs to, you may either have NSM administrator or NSM user authority. Groups are described later in this chapter.

The AS/400 administrator

In an AS/400 environment, a user is considered an administrator if their user profile has the *ALLOBJ and *SECADM special authorities. Since these authorities are very powerful, most AS/400 customers tend to have few user “administrator” level user profiles.

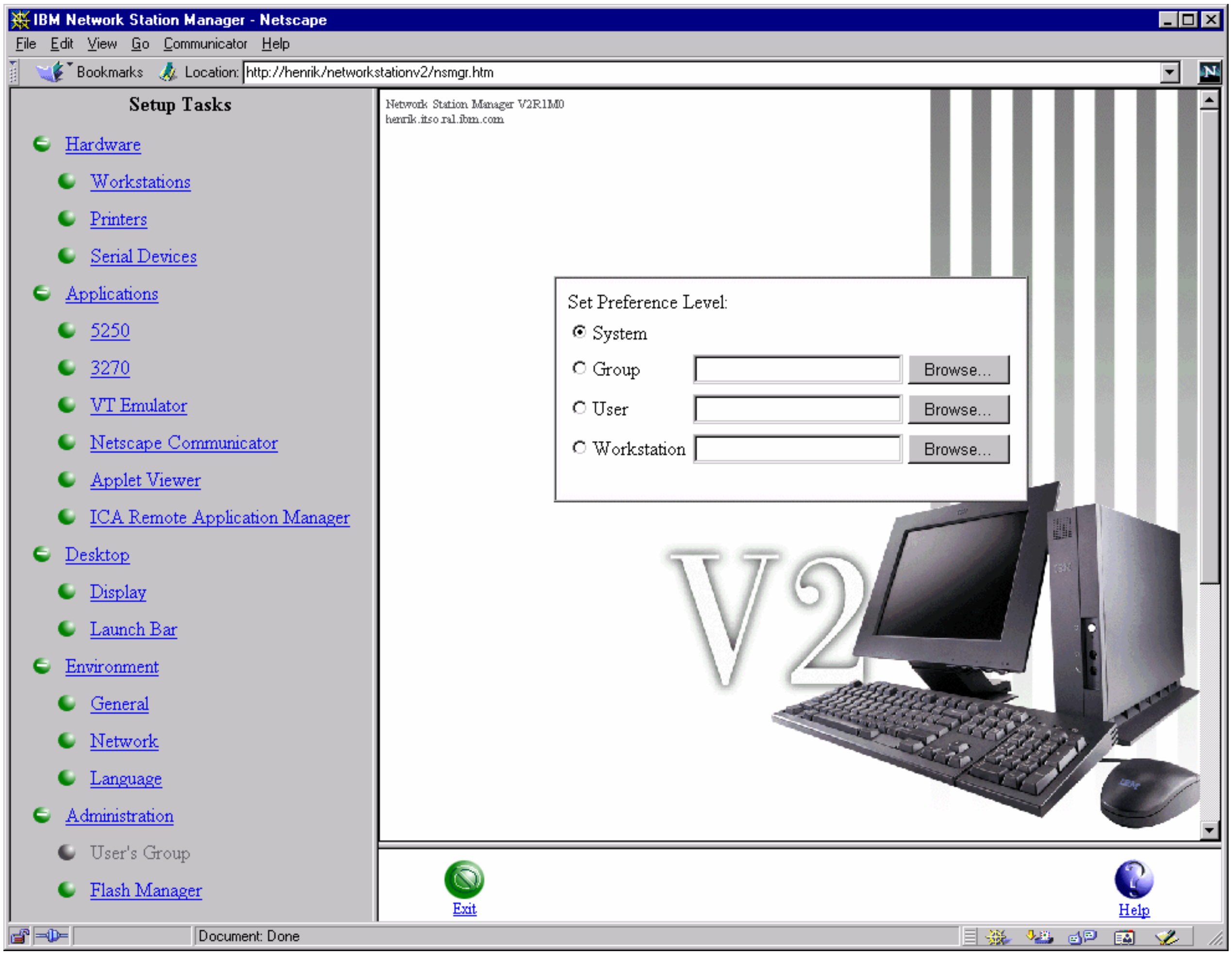
8.2.1 Different levels of settings

Configuration settings in NSM can be made at four different levels:

1. **System**: Settings that are made at the System level affect *all* Network Stations and *all* users.
2. **Group**: Settings that are made for a specific group only affect users that are members of that specific group and have it defined as their main group in NSM.
3. **User**: Settings made for a specific user only affect that particular user.
4. **Workstation**: Changes that need to be made for a specific Network Station (workstation) can be made at the workstation level. At this level, *only* hardware-related settings can be made, no user-related or application-related

settings are made here, since they are not tied to a specific (physical) Network Station.

These levels are shown as they appear on the display in Figure 125.



Set Preference Level:

- ● System
- ○ Group [ ] Browse...
- ○ User [ ] Browse...
- ○ Workstation [ ] Browse...

Figure 125. Network Station Manager: Select a level

These four levels all contain settings that can be modified. When Network Station Manager is installed for the first time, it also contains a number of default settings called the *Shipped Defaults*. These settings are overridden by the settings made at the four preference levels (Figure 126). The Shipped Defaults are provided to give the administrators a smooth start and not to have a completely empty NSM.

Note

To easily identify which settings can be modified at the Workstation, System, Group and User levels, NSM V2R1 now grays out those settings that do not apply to the selected level. For example, if you select the Workstation level, you cannot modify Netscape Communicator settings. These settings are not tied to one particular workstation, but rather to all users (System), a group, or a specific user. And if, for example, you select a group, you cannot make changes to Serial Devices, since these are tied to one particular workstation and not a group. This visual appearance is a new feature of V2R1.

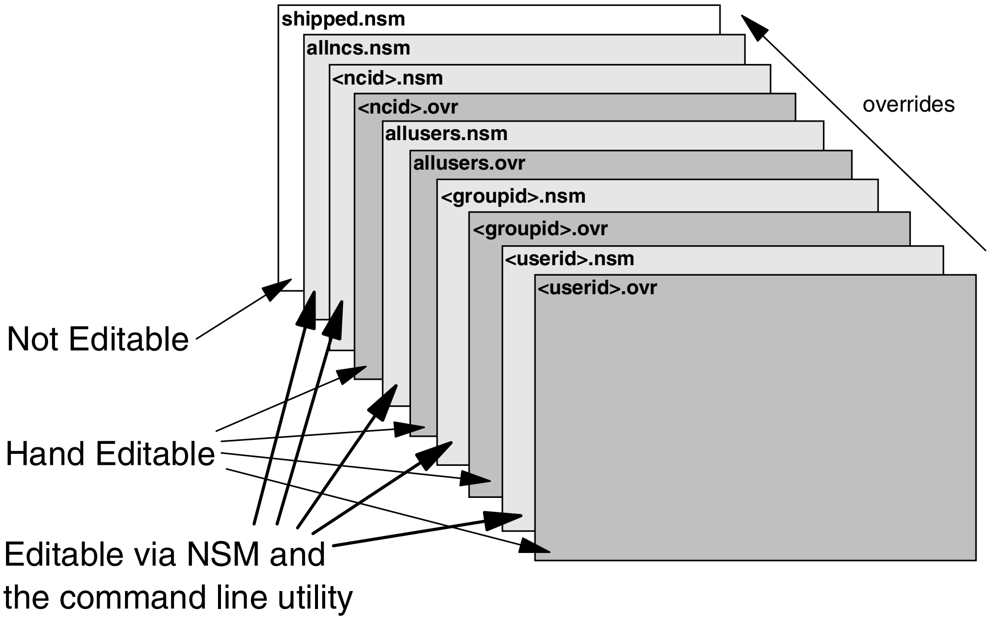


Figure 126. NSM settings override path

When a user logs on to a Network Station, they receive settings from all four configurable levels and the Shipped Defaults level.

Some of these settings are additive, meaning the user receives the sum of all settings. Other settings are mutually exclusive, meaning the user receives the setting configured at the highest level.

For example, the Shipped Defaults level may contain an icon for Netscape Communicator (and that icon has not been removed). In addition, the administrator may have given all users (System level) an icon for a 3270 emulator, an icon for a particular Java application to the group to which a user belongs, and an icon for a particular Java application to the user. In this case, the net result would be that the user would get all four icons on their Launch Bar. Therefore, icons are additive.

In contrast, the Shipped Defaults may have defined the background color to be gray. The administrator may have defined the background color for all users (System level) to be red, and at the group level to be green. Plus, the user may have set the background color to blue. In this case, the background color does not become a mix of all the colors, but rather the user’s own choice. Therefore, the background color is not additive, but mutually exclusive and then the setting made at the highest level (in this case, the user level) is what becomes active.

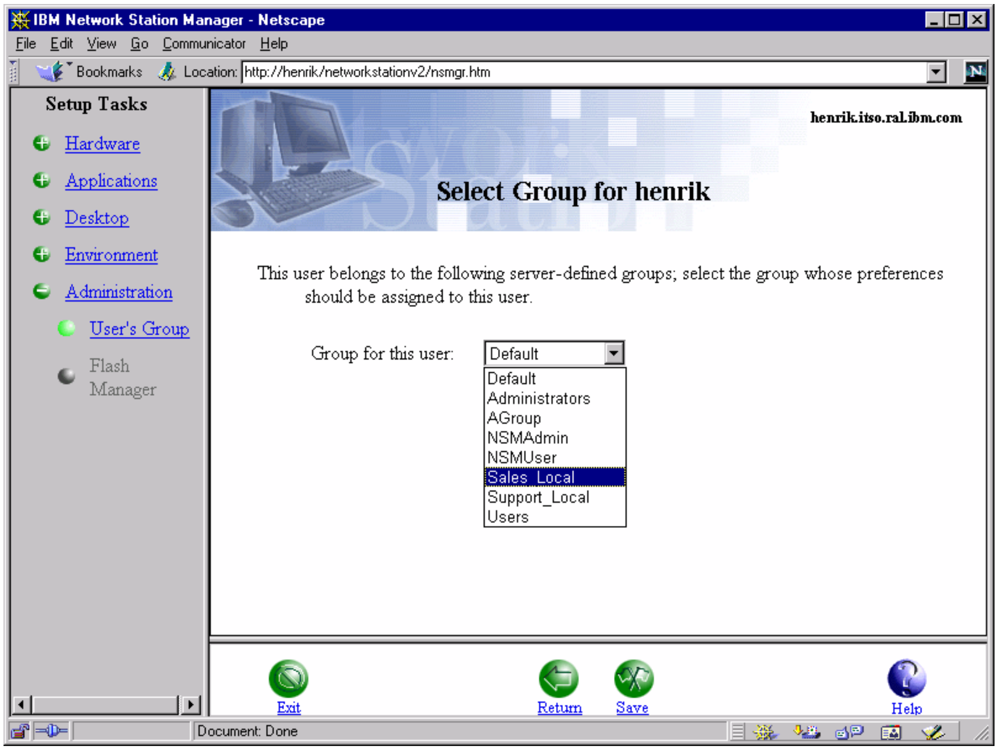
8.2.2 NSM groups and users, main group

The groups and users available to NSM are retrieved from the operating system on which NSM is installed. For example, if NSM is installed on a Windows NT server, Windows NT groups and users are made available to NSM.

Even if a user happens to be a member of multiple groups in the operating system on which NSM is installed (which is very common), they can only receive settings from *one* of these groups in NSM. Now you probably wonder why? While at the first glance this doesn’t really make sense, think a little bit further. Let’s say a user is a member of both the Secretaries group and the Sales group in the underlying operating system (Windows NT for example). Then, let’s say that, in NSM, the administrator has configured the Secretaries group to use a left-handed mouse and the Sales group to use a right-handed mouse. This may not be the best example, but it at least demonstrates the concept. Now, the secretaries for the sales persons are all members of both the Secretaries and the Sales groups. Which setting should these users be given? Left-handed or right-handed?

To avoid running into problems like this, the approach taken by NSM is that a user can only receive settings from *one* group in the operating system. This group is called the user’s *main group*. To define the main group for a user, select a user. Then, go to the **Administration->User’s Group** panel in NSM and select group. The user will now pick up settings from the selected group (but no other *groups*) in addition to the system and user level settings.

Note that users must always be a member of the NSMUser group to authenticate when logging on. In addition, the users can be members of other groups. The main group where the user will pick up group settings can be an NSMUser or any other group of which the user is a member. Figure 127 shows the page for selecting a user’s main group.



Select Group for henrik

This user belongs to the following server-defined groups; select the group whose preferences should be assigned to this user.

Group for this user: Default

- Default
- Administrators
- AGroup
- NSMAdmin
- NSMUser
- Sales_Local
- Support_Local
- Users

Figure 127. Selecting a user's main group

If you do not define the main group for a user, it is retrieved from the operating system on which NSM is installed. This group is usually called the *primary group* in the operating system if the operating system supports the concept of a primary group.

Windows NT servers

Windows NT does have a term called primary group. There is a “type” of primary group when a user accesses a NT server from a Macintosh or POSIX platform, but it is not what NSM considers a true primary group. Therefore, in NSM on Windows NT, the default main group is NSMUser.

8.2.3 User versus administrator configurable setting

In NSM, users are divided into two categories: *users* and *administrators*. When you logon to the NSM administration tool (the browser-based interface), you are validated with a user ID and a password. If you are a member of the NSM administrators group (on Windows NT) or your user profile has *ALLOBJ and *SECADM authority (on an AS/400 system), you are allowed to make changes to all Network Stations and all users. If you are only a member of the NSM users group then you can only make a limited number of changes that affect only yourself.

The outline in Appendix D, “User verses administrator configurable settings” on page 617, lists all settings the administrators and end-users can choose, respectively.

8.3 NSM on Windows NT and in Windows NT domains

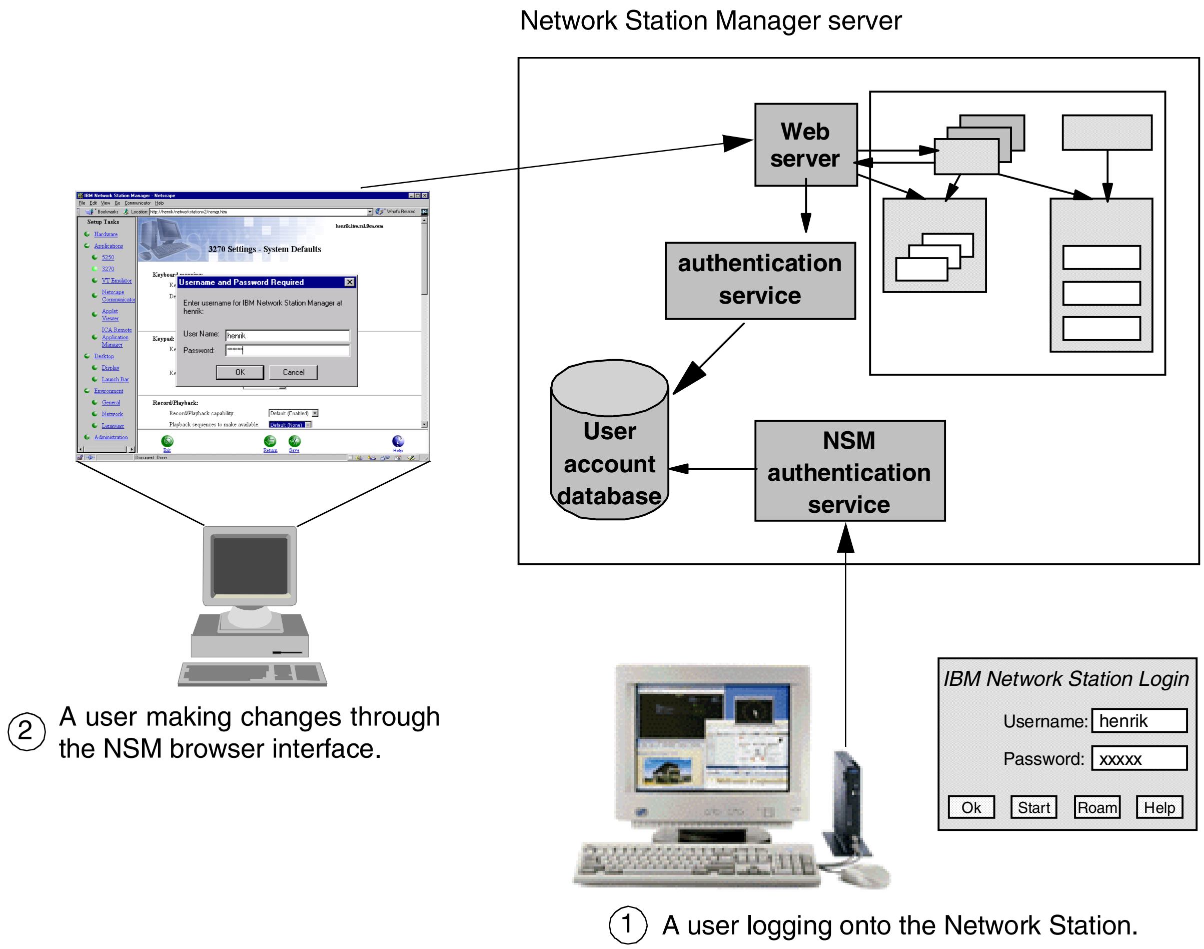
Figure 128 describes the two logon procedures with which a user may contact NSM.

Windows 2000 and NSM

At the time this redbook was written, Microsoft Windows 2000 was not yet a supported platform for NSM V1R3 or V2R1.

Windows NT product information

A readme file that contains some helpful information can be found on the Windows NT installation CD in the directory as /ntnsm/en/Readme.txt. You can also look on the Internet at: `http://techsupport.services.ibm.com/nc/`


Network Station Manager server
Web server
authentication service
User account database
NSM authentication service
3270 Settings - System Defaults
IBM Network Station Login
Ok
Start
Roam
Help
2 A user making changes through the NSM browser interface.
1 A user logging onto the Network Station.

Username and Password Required

Enter username for IBM Network Station Manager at henrik:

User Name: henrik

Password: ******

OK Cancel

Username: henrik

Password: xxxxx

Figure 128. NSM users and groups

The first scenario (1 in Figure 128) is when a user powers on their Network Station and is presented with the IBM Network Station Login panel. They enter their user ID and password and are then authenticated by the NSM authentication service and granted or denied access to work at their Network Station. When they logon, they receive settings from the different levels described earlier: the IBM-shipped defaults, the System level settings, settings made for their main group (the *one* group they are configured to pick up settings from), and from settings done on a user-level basis (for their user ID).

The second scenario (2 in Figure 128) is when a user launches a Web browser (from the Network Station, a PC, a UNIX workstation, etc.) and connects to the NSM browser-based interface for customizing some settings. The browser presents a logon dialog. When the user ID and password have been entered, the Web server verifies if the user is to be granted or denied access and if they are to be granted NSM administrator privileges or NSM user privileges. The authentication process for the NSM Web application varies among platforms. Windows NT and AIX use the Web server basic authentication. The AS/400 server does the authentication as a part of the CGI. All platforms check for user authority versus administrative authority in their CGI.

When NSM is installed on a Windows NT server, two *local* groups are created on the server: NSMAdmin and NSMUser. These two groups correspond to the NSM administrators and NSM users. All users that are made members of the NSMUser group are allowed to logon to the Network Station (1) and *also* to logon to the NSM browser-based interface (2). When they logon to the browser-based interface, they are allowed to modify a limited number of settings that only affect themselves. If a user is also made a member of the NSMAdmin group, when they logon to the NSM browser-based interface (2), they are allowed to make changes to all Network Stations and all users. If a user is *only* a member of the NSMAdmin group and not the NSMUser group, they are allowed to logon to the NSM browser-based interface (2), but *not* to a physical Network Station (1). To logon to a physical Network Station, a user *must* be a member of the NSMUser group.

8.3.1 NSM on a standalone Windows NT server

NSM running on a Windows NT server can only locate those users and groups that are *locally* defined on the Windows NT server (Figure 129).

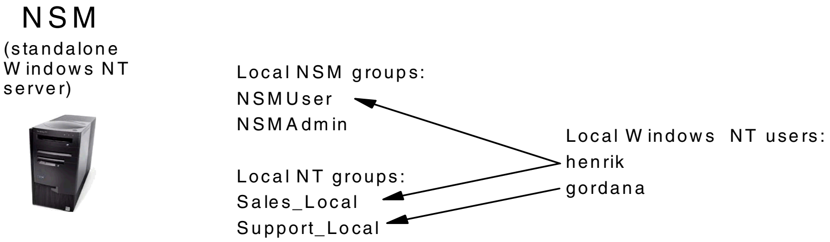
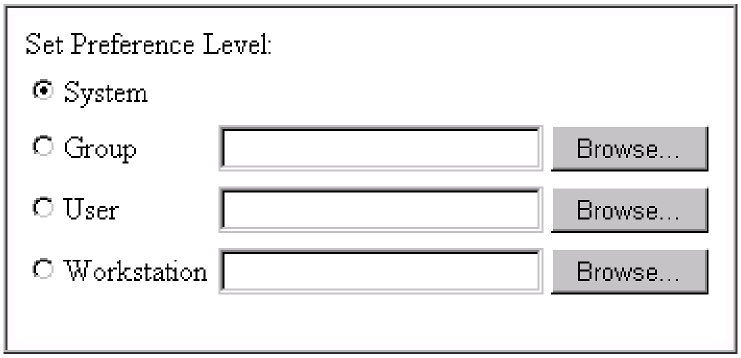


Figure 129. NSM groups and users on a standalone Windows NT server

To allow the users locally defined on a standalone Windows NT NSM server to logon to the Network Station (1 in Figure 128), they must be made members of the local NSMUser group. In the above example, only henrik is made a member of this group. Therefore, he is the only one able to logon to the Network Station. Those users that should have NSM administrative privileges when logging on to the browser-based interface (2 in Figure 128) should also be made members of the local NSMAdmin group (none have been given NSM administrative privileges in the above example).



Set Preference Level:

● System

○ Group

○ User

○ Workstation

Figure 130. NSM Browse Group button

To configure settings for all users belonging to a specific Windows NT group, click the **Group** radio button, and then click **Browse...** in the NSM browser-based interface to list all groups known to NSM (Figure 130). NSM then lists all *local* groups on the Windows NT NSM server (it filters out the Backup Operators and Power Users groups). A group can then be selected from the list and changes made to this specific group. All users that are members of this group in Windows NT and have it defined as their main group in NSM will receive these settings.

After an NSM installation, all users that are made members of the NSMUser group are also assigned the NSMUser group as their main group in NSM. That means that in the previous example, if henrik was not assigned the Sales_Local group as his main group, he would not receive any settings made for the Sales_Local group, even though he is a member of that group in Windows NT. At the group-level, he would only receive settings made for the NSMUser group.

To configure settings for a specific Windows NT user, click **User** radio button, and then click **Browse...** in the NSM browser-based interface to list all configurable users. NSM then lists all users that are members of the local NSMUser group but no others. It doesn’t make sense to list non-NSMUser members since they cannot logon and work with the Network Station anyway.

8.3.2 NSM on a standalone server in a Windows NT domain

When NSM is installed on a standalone server that is part of a Windows NT domain, NSM can use global groups and users defined in the domain (Figure 131). However, just as in the case where NSM was installed on a standalone Windows NT server, it only allows users that are members of the local NSMUser group to logon to the Network Station.

Any users defined in the domain are not automatically added to the local NSMUser group. That has to be done manually. This can be done in three different ways, all of which have their advantages and disadvantages.

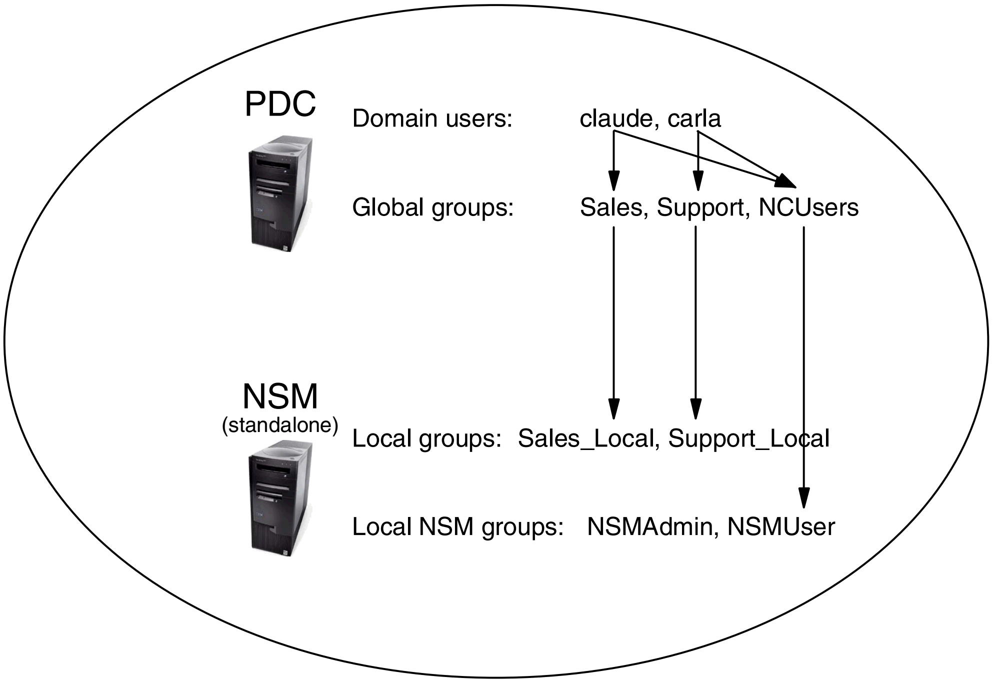

PDC
Domain users: claude, carla
Global groups: Sales, Support, NCUsers
NSM
(standalone)
Local groups: Sales_Local, Support_Local
Local NSM groups: NSMAdmin, NSMUser

Figure 131. Using global groups and users from a Windows NT domain

For example, in Figure 131 there is a primary domain controller (PDC) with three groups defined. We need to allow the users, claude and carla, to logon to Network Stations authenticated by the NSM server. We assume claude and carla are already members of global Windows NT groups to get their Windows NT privileges and permissions:

- All users in the domain can simply be directly added to the local NSMUser group. If claude and carla were added to the local NSMUser group, they would be allowed to logon to the Network Stations. While this is a quick and easy way to let the domain users logon to the Network Stations, it does not allow an NSM administrator to make changes to the respective groups they belong to (Sales and Support). Remember, NSM only locates and allows settings to local groups. This method is not shown in Figure 131.
- A new global group, for example, NCUsers, could be created in the domain, and the domain users could be added to this group. Then this single group could be added to the local NSMUser group. This would also let the domain users (now also members of the NCUsers group) logon to the Network Station, but it would still not allow an NSM administrator to make changes to the respective groups to which the users belong. However, it would make it easier to make new domain users able to logon to the Network Station, by just adding them to the NCUsers group. This method is not shown in Figure 131.
- The most flexible alternative is to create local groups (Sales_Local and Support_Local) on the NSM server for each global domain group (Sales and Support). Then each global domain group could be added to the respective local group. To allow the domain users to logon to the Network Stations, a new global group, NCUsers, could then be created in the domain, the domain users added to it and finally this group added to the local NSMUser group. This is the method shown in Figure 131.

This would allow the domain users belonging to the NCUsers group to logon to the Network Station. It would also allow an NSM administrator to assign settings to each group in the domain, by making the changes to the local groups (Sales_Local and Support_Local).

However, to have the users in the global Sales group pick up settings made to the local Sales_Local group, they would have to be assigned the Local_Sales group as their *main* group. If this is not done, they will only use settings from their default main group, which is NSMUser.

If there are many domain user accounts, this would best be done via a script using the NSM Command Line Interface. A list of users in each global domain group could be extracted and a script with NSM Command Line Interface commands could be created to perform this operation. See 8.5, "NSM Command Line Interface" on page 180, for an example of this.

8.3.3 NSM on a standalone server in a trusted Windows NT domain

Consider the example where you have a separate account domain where you keep all your users and groups and a separate resource domain where you keep all your resources (such as file servers, print servers, and so on) and the NSM server is a member of the resource domain. In this case, you need to set up a trust between your account domain and the resource domain (but you probably already have this). Once the trust relationship is established, the above technique with local groups (Sales_Local and Support_Local) and a global group (NCUsers) could be used to add the groups and users from the account domain to the NSM server in the resource domain. This is demonstrated in Figure 132.

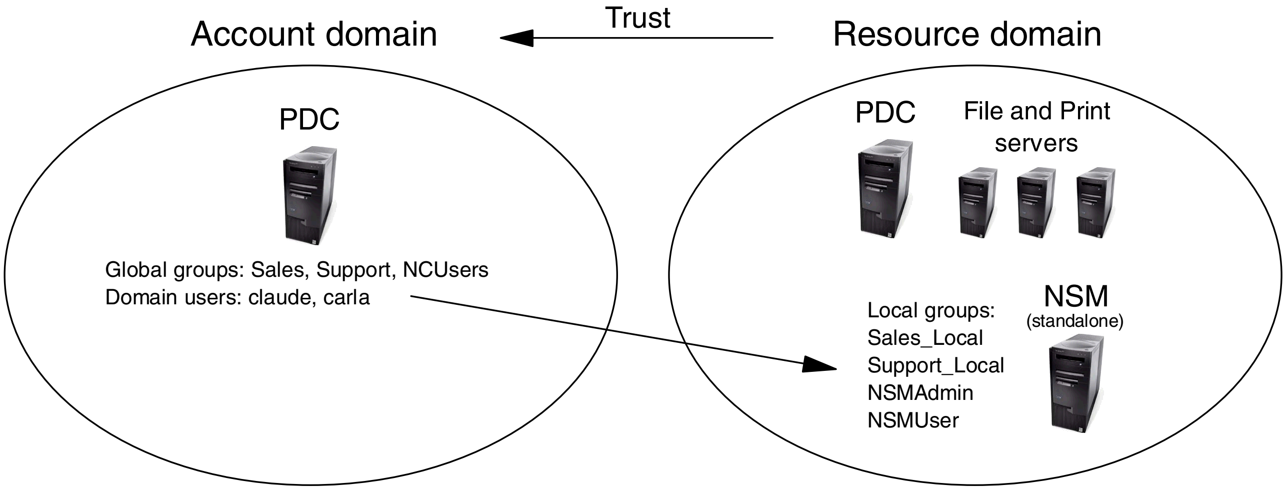


Figure 132. Using global groups and users from a trusted Windows NT domain

> **Note**
>
> When a user logs on to the Network Station, the user ID and password is sent to the NSM authentication service. The authentication service first checks if the user ID is *locally* available on the server. If it is, the password is verified and the user is either granted or denied access. If the user ID is not locally available on the server, the authentication service looks for the user ID in the *domain* (or trusted domain) and verifies the password there. If the user ID is locally available but the password is incorrect, the authentication service does *not* look for the user ID in the domain.
>
> If you logon with a user ID that is available both locally and in the domain (for example Administrator), you must enter the password for the local (Administrator) account.

8.4 Download profiles

All changes made to NSM are stored in *download profiles*. This is a new term introduced by NSM V2R1. The download profiles serve exactly the same purpose as the *configuration files* used in previous NSM releases.

However, to improve performance, the number of configuration files (download profiles) the Network Station must read at power up and user logon have been reduced. The information is now consolidated into these few, well-defined files called the download profiles.

In previous releases, the information in the configuration files were also stored in many different file formats. This has now been reduced to only one format, so all download profiles are now stored as XML with UTF-8 encoding.

The download profiles are managed by NSM. The enduser or administrator must not directly modify them by themselves. Figure 133 shows a look at one of the files.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCREGISTRY SYSTEM "registry.dtd" >
<NCREGISTRY VERSION="1.0">
<OBJECT NAME="/config">
<CATEGORY NAME="WORKSTATION">
<PROPERTY NAME="xserver-keyboard-type">5</PROPERTY>
<PROPERTY NAME="pref-screensaver-enable">true</PROPERTY>
<PROPERTY NAME="pref-screensaver-time">60</PROPERTY>
</CATEGORY>
</OBJECT>
</NCREGISTRY>
```

Figure 133. Sample download profile in XML format

As you can see, the download profiles in the XML format look similar to the HTML format, just with different tags. The XML definition used by Network Station Manager is specifically tailored to handle the information that is stored in the download profiles.

XML and UTF-8 Mini FAQ

What is XML?
XML is the Extensible Markup Language, designed to enable the use of SGML on the World Wide Web. It is not a single, predefined markup language. It's a metalanguage, a language for describing other languages, which lets you design your own markup. A predefined markup language like HTML defines a way to describe information in one specific class of documents. XML lets you define your own customized markup languages for different classes of documents.

What is SGML?
SGML is the Standard Generalized Markup Language (ISO 8879), the international standard for defining descriptions of the structure and content of different types of electronic documents.

What is HTML?
HTML is the HyperText Markup Language (RFC 1866), a specific application of SGML used on the World Wide Web.

Aren't XML, SGML, and HTML all the same thing?
Not quite. SGML is the "mother tongue", used for describing thousands of different document types in many fields of human activity. HTML is just one of these document types, the one most frequently used in the Web. It defines a simple, fixed type of document with markup designed for a common class of office or technical report, with headings, paragraphs, lists, illustrations, etc., and some provision for hypertext and multimedia.

XML is an abbreviated version of SGML, to make it easier for you to define your own document types, and to make it easier for programmers to write programs to handle them. It omits the more complex and less-used parts of SGML in return for the benefits of being easier to write applications for, easier to understand, and more suited to delivery and interoperability over the Web. But it is still SGML, and XML files may still be parsed and validated the same as any other SGML file.

What is UTF-8?
UTF-8 is an efficient encoding of Unicode character strings that recognizes the fact that the majority of text-based communications are in ASCII. Therefore, it optimizes the encoding of these characters.

What is Unicode?
Unicode is a character encoding standard, aimed to consolidate the alphabets and ideographs of the world's languages into a single, international character set. It is not concerned about the languages themselves, but rather focuses on the characters used. Most Western character sets are 7-bit (for example, US ASCII) or 8-bit (Latin-1), limiting them, respectively, to 128 or 256 characters. To support other character sets (for example for Chinese, Korean, Japanese), the Unicode character set is 16-bit (2 bytes), allowing 65,536 different characters.

Note

The industry now has the three basic functions necessary for true network computing:

- The platform independent communications protocol TCP/IP
- The platform independent programming language Java
- The platform independent file formats SGML and XML

NSM V2R1 uses two different types of download profiles (Figure 134):

- **NC profiles**: The NC profiles contain information that is needed to initialize the Network Station hardware, its operating system, and initial application environment. The NC profiles are downloaded to the NC Registry in the Network Station during its boot process. The information lasts until the Network Station is rebooted.
- **Session profiles**: The Session profiles contain information that is needed to tailor the environment that was established by the NC profiles to an individual user's requirements. The Session profiles contain information that applies to all users, the group a user belongs to, and to the specific user. Session profiles are downloaded to the NC Registry in the Network Station after the user has been authenticated (using the ACTlogin process). The information lasts until the user logs off.

The NC profiles contain the Network Station configuration information, while the Session profiles contain the user-related configuration information.

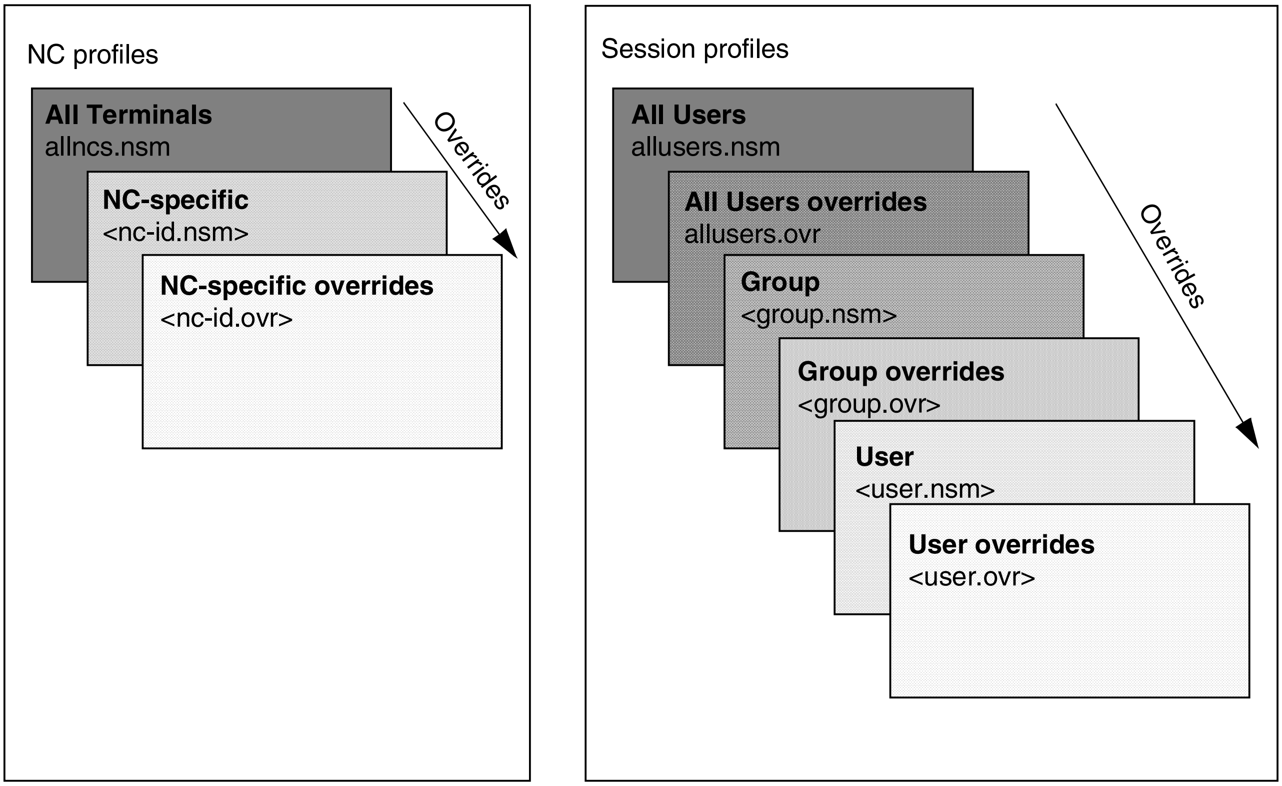


Figure 134. NSM download profiles

In addition to these download profiles, there is also a file called *shipped.nsm,* which is also read by the Network Station during the boot process. This file contains all IBM-shipped default settings that apply to both Network Stations and the users. This file never changes after installation. All changes made through NSM are stored in one of the other files, which override the values in the shipped.nsm file.

The two groups of download profiles can be broken down further:

- NC profiles include these profiles:
  - **All NCs profile**: The All NCs profile contains settings and preferences that apply to *all* Network Stations. Only *one* All NCs profile exists per NSM server and is valid for all Network Stations downloading the NC profiles from that NSM server. The file containing this information is called *allncs.nsm*. This file does not exist directly after NSM installation, but is created by NSM whenever changes that should be stored in it have been made.
  - **NC-specific profile**: The NC-specific profile contains configuration information that applies only to a specific Network Station. If a configuration is made on a per-Network Station basis, NSM creates one NC-specific profile per Network Station being customized. The file containing this information is called *<nc-id>.nsm*, where <nc-id> is either the Network Station's IP address, its hostname, or its MAC address.
  - **NC-specific override profile**: The NC-specific override profile contains override preferences for a specific Network Station. The information in this profile overrides any settings made in either the All NCs profile or an NC-specific profile. The NC-specific override profile is not created, modified, or otherwise managed by NSM, but is to be created and managed by the NSM administrator manually. There can exist only one NC-specific override profile per Network Station. The file is called *<nc-id>.ovr*, where <nc-id> is either the Network Station's IP address, its hostname, or its MAC address.
- Session profiles include:
  - **All Users profile**: The All Users profile contains settings and preferences that apply to *all* Network Station users. Only *one* All Users profile can exist per NSM server. The file containing the information is called *allusers.nsm*. During NSM installation, this file is populated with IBM-shipped default settings such as Launch Bar icons and so on.
  - **All Users override profile**: The All Users override profile contains settings that override settings made for all users. The All Users override profile is not created, modified, or otherwise managed by NSM, but is to be created and managed by the NSM administrator manually. There can exist only one All Users override profile per NSM server. The file is called *<allusers>.ovr*.
  - **Group profile**: The Group profile contains all settings for a specific group. If configuration is done on a per-group basis, NSM creates one Group profile for each group being customized. The file is called *<group>.nsm*, where <group> is the name of the group being customized.
  - **Group override profile**: The Group override profile contains settings that override settings made for a specific group. The Group override profile is not created, modified, or otherwise managed by NSM, but is to be created and managed by the NSM administrator manually. There can exist only one

Group override profile per group. The file is called *<group>.ovr,* where <group> is the name of the group whose settings are being overridden.

– **User profile**: The User profile contains all settings for a specific user. If a configuration is made on a per-user basis, NSM creates one User profile for each user being customized. The file is called *<user>.nsm*, where <user> is the name of the user being customized.

– **User override profile**: The User override profile contains settings that override settings made for a specific user. The User override profile is not created, modified, or otherwise managed by NSM, but is to be created and managed by the NSM administrator manually. There can exist only one User override profile per user. The file is called *<user>.ovr*, where <user> is the name of the user whose settings are being overridden.

Figure 135 shows where the download profiles are located.

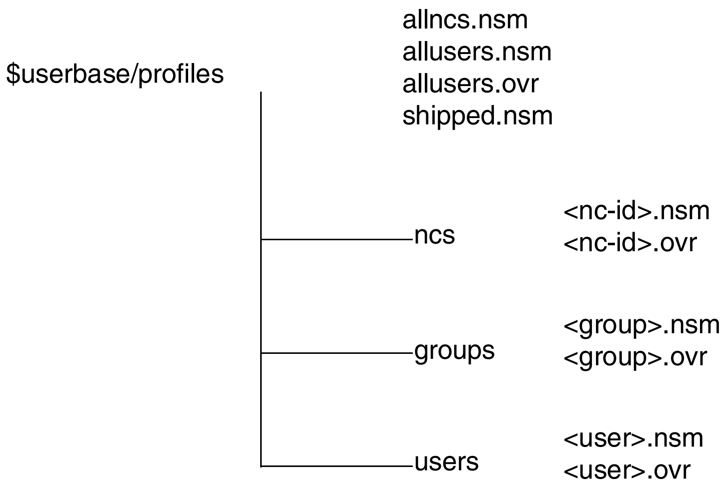


Figure 135. Download profiles directory structure

The override profiles serve the same purpose as the *backdoor files* in NSM V1R3. They configure settings that are not available in the NSM browser-based interface.

A note on the <nc-id> format

- If the IP address is used, the format should be a dotted decimal TCP/IP address, for example, 9.24.104.192.
- If the hostname is used, it should be the hostname that the Network Station receives when it performs a reverse name lookup to get its hostname from its IP address. If the DNS (or hosts file) returns a fully qualified hostname (like hondo1.itso.ral.ibm.com), a fully qualified host name should be used. If the DNS (or hosts file) returns only the hostname part and not the domain name part (like hondo1) the host name should be used. Use nslookup *ipaddress* to see what your DNS returns.
- If the MAC address is used, it should be a full 12-character MAC address without colons and with single-digit fields padded with a leading zero. For example, if a Network Station has a MAC address of 0:6:29:F5:D7:3, the valid MAC address would be 000629F5D703.
- If changes have been made for a Network Station using more than one <nc-id> identifier (for example, both on MACaddress and IPaddress level), they are read in the following order:

  1. *Hostname*.nsm
  2. *MACaddress*.nsm
  3. *IPaddress*.nsm

  This means that the settings in the IPaddress.nsm file override the settings made in the hostname.nsm and MACaddress.nsm files.

  The override files, if used, are read after the .nsm files and in the same order as above. This means that the *IPaddress*.ovr file has the highest priority of all NC-specific download profiles.

Important note on override profiles

Even though NSM V2R1 has this override capability and we have described it here, it is *not* enabled by default. The reason for it being disabled is that the preferred way of adding settings that are not available from the browser-based GUI is to use the NSM Command Line Interface (NSMCL). The NSMCL really makes the override profiles unnecessary, so they are disabled. If you are using the NSMCL, you do not have to worry about the correct XML syntax, because NSMCL takes care of that for you (which is a major advantage).

However, should you want to enable the override profiles support anyway, the NSM_ALLOW_OVERRIDES value in the NC Registry must be set to ENABLE. This is done easily by using the NSMCL and issuing the following command:

```
INSERT IBMNSM/SYSTEM/DEFAULT/RULES/NSM_ALLOW_OVERRIDES/ ENABLE
```

Remember that if you enable the override support, NSM will not create and manage the override profiles for you. It’s your responsibility to create the override profiles files with the correct XML syntax. We strongly recommend that you use the NSMCL instead of the override profiles. By not using the override profiles, you actually benefit from somewhat improved performance, since the NC Registry does not have to look for the download profiles.

Tip

If you need to restore the IBM-shipped default profiles, shipped.nsm and allusers.nsm, there are backup copies in the $servbase/defaults directory. Copy these files to the $UserBase/profiles directory to restore the default values. You should also delete the allncs.nsm file, since it contains settings you've made in NSM.

Improving startup performance by skipping download profiles

By default, when the Network Station is powered-on and a user logs on, the NC Registry looks for download profiles at the system, group, user, and workstation levels. This allows an administrator to configure settings in each of these levels.

However, if certain levels do not contain any settings, the NC Registry can be told not to look for settings at these levels, which improves performance when the Network Station is powered on and when the user logs on.

Table 27 lists the configuration parameters that control the behavior of the NC Registry and the possible values they can have.

Table 27. Performance tuning: Values for controlling download profiles in NC Registry

Key	Explanation
NSM_ACCESS_NC_CONFIG	This setting determines if the NC Registry should look for NC-specific download profiles, for example, the <nc-id>.nsm files. If set to ENABLE, it looks for them. If set to DISABLE, it skips them. The default value is ENABLE.
NSM_ACCESS_GROUP_CONFIG	This setting determines if the NC Registry should look for group-level download profiles, for example, the <group>.nsm files. If set to ENABLE, it looks for them. If set to DISABLE, it skips them. The default value is ENABLE.
NSM_ACCESS_USER_CONFIG	This setting determines if the NC Registry should look for user level download profiles, for example, the <user>.nsm files. If set to ENABLE, it looks for them. If set to DISABLE, it skips them. The default value is ENABLE.
NSM_NC_NAME_TYPE	If the NSM_ACCESS_NC_CONFIG setting is set to ENABLE, this setting determines which files are searched, for example, what is used for the <nc-id> identifier in the <nc-id>.nsm filename. Valid values are HOST_NAME, MAC_ADDRESS, IP_ADDRESS, or ANY. If set to HOST_NAME, MAC_ADDRESS or IP_ADDRESS, the NC Registry looks for the hostname.nsm, macaddress.nsm, and ipaddress.nsm files respectively. If set to ANY, the NC Registry looks for all three possible filenames. The default value is ANY.

Key	Explanation
NSM_ALLOW_OVERRIDES	This setting determines if the NC Registry should look for the override profiles, for example, the filename.ovr files. If set to ENABLE the NC Registry looks for the download profiles. If set to DISABLE, it skips them. The default value is DISABLE.

These values are most easily modified by using the NSM Command Line Interface (NSMCL), which is described in the next section. In the following examples, we use NSMCL to modify the values:

- To make the NC Registry skip any group-level download profiles, use the following NSMCL command:

  ```
  INSERT IBMNSM/SYSTEM/DEFAULT/RULES/NSM_ACCESS_GROUP_CONFIG/ DISABLE
  ```

- To make the NC Registry only look for TCP/IP addresses in the NC-specific download profiles (<nc-id>.nsm), use the following NSMCL command:

  ```
  INSERT IBMNSM/SYSTEM/DEFAULT/RULES/NSM_NC_NAME_TYPE/ IP_ADDRESS
  ```

  This causes the NC Registry to only look for download profiles named 9.24.104.192.nsm, 9.24.104.199.nsm, and so on.

- To make the NC Registry only look for MAC addresses in the NC-specific download profiles (<nc-id>.nsm) use the following NSMCL command:

  ```
  INSERT IBMNSM/SYSTEM/DEFAULT/RULES/NSM_NC_NAME_TYPE/ MAC_ADDRESS
  ```

  This causes the NC Registry to only look for download profiles named 0020355f47d4.nsm, 000629670506.nsm, and so on.

8.5 NSM Command Line Interface

The NSM Command Line Interface (NSMCL) is a utility shipped with NSM V2R1 that allows an administrator to make settings to NSM that are not available in the NSM browser-based GUI. The changes made with NSMCL are usually advanced configuration settings, typically the same settings that were put in the defaults.dft configuration file NSM V1R3. Using NSMCL, changes can also be run in batch scripts, which simplifies the task when changing a large number of settings for a user or settings for a large number of users.

NSMCL is written in Java. Therefore, it requires JVM 1.1.6 (or later) installed on the operating system where it is used. The NSMCL utility can be run in three different modes:

- **SGCL command**: This starts NSMCL with a command as the input parameter. The command is executed.
- **SGCL scriptfile**: This starts NSMCL with the name of a script file that includes commands that should be executed.
- **NSM_CL**: This starts NSMCL and runs it in graphical mode. This is useful for debugging commands and developing the script files.

These commands are actually part of Java classes shipped with NSM. You will not find these commands by looking in the directory structure. They are included in the Java JAR files shipped with NSM in the $ServBase/tools directory and require a proper Java environment to execute.

The NSMCL is well documented in the *IBM Network Station Advanced Information*, September 1999, that can be downloaded from the Web at:

```
http://www.pc.ibm.com/us/networkstation/tech_library.html
```

This documentation covers all of the commands that the NSMCL can perform and the syntax for each individual command. It also explains how to start NSMCL and how to customize the SGCL.INI file that is used to configure NSMCL.

Also, a readme file is shipped with the product and can be found in the product directory <PRODBASE>\nsm\tools\readme_cl.txt.

8.5.1 Command syntax

The syntax for most (but not all) of the NSMCL commands is:

```
command ibmnsm/level/name/category/configname/ configvalue
```

Note

- The forward slash (/) is used as a delimiter. Please also note that there is a trailing slash after the `configname`. This slash is required. The space between the trailing slash and the configvalue is optional.
- User names, file/path names (except Windows NT file/path names), configuration names, and configuration values are case sensitive. Other parameters are not.

The command is one of the following supported NSMCL commands (not case sensitive):

Update Changes existing configuration values.

Insert Creates new (or changes if they already exist) configuration values.

Delete Deletes existing configuration values.

Select Returns existing configuration values.

Copy Copies configuration values.

Call Runs script files.

Commit Writes all pending (since last commit) changes to disk.

Rollback Discards all pending (since last commit) changes.

Set Temporarily sets any value in the SGCL.INI file.

Exec Runs a native operating system command in the operating system.

Note on committing changes

When you use NSMCL in any of the three modes, all commands are buffered. Their result is not automatically written to the download profiles. To write the result of one or more commands you issued to the download profiles, you *must* issue the `commit` command. Until the changes are committed, they can be undone by issuing the `rollback` command.

The ibmnsm means that changes should be made to IBM Network Station Manager. The `ibmnsm` parameter is the only one supported by NSMCL today, and it is a required parameter.

The level specifies at which level the changes should be made. There are four possible levels: system, workstation, usergroup, and user.

The name is one of the following four values (names and filenames are case sensitive):

name Any valid name. For a workstation, it would be an IP address, a MAC address, or a fully qualified hostname. For a group, it would be the name of the group, and for a user, it would be the name of a user.

all Denotes all workstations, groups, or users.

all like xxx Denotes all workstations, groups, or users that match the regular expression pattern `xxx`. The syntax to be used when creating regular expression patterns is documented in the *Network Station Manager Advanced Information V2R1* publication. We do not reproduce it here. It is important to note that the `all like xxx` construct in the name field only *selects* the set of *existing* NSM names (user, workstation or group) that match the xxx expression from existing name.nsm files. It never creates new names and corresponding files.

list filename Denotes all workstations, groups or users that are listed in the specified file.

A note on addressing Network Stations

The syntax of the *name* and the names in a *list* filename are the same as the ones the NC Registry looks for when it searches for NC-specific download profiles:

- If the IP address is used, the format should be a dotted decimal TCP/IP address, for example, 9.24.104.192.
- If the hostname is used, it should be the hostname that the Network Station receives when it performs a reverse name lookup to get its hostname from its IP address. If the DNS (or hosts file) returns a fully qualified hostname (like hondo1.itso.ral.ibm.com), the fully qualified host name should be used. If the DNS (or hosts file) returns only the hostname part and not the domain name part (like hondo1), the host name should be used.
- If the MAC address is used, it should be a full 12-character MAC address without colons and with single-digit fields padded with a leading zero. For example, if a Network Station has a MAC address of 0:6:29:F5:D7:3, the valid MAC address would be 000629F5D703.

A *category* is a group of related configuration parameters. The category can have one of the following values (not case sensitive):

WORKSTATION Denotes workstation settings such as keyboard repeat rate, color depth, and so on. These settings correspond to those found in the Hardware->Workstation panel in the NSM Web interface.

EXTERNAL Denotes workstation settings such as 1st, 2nd, and 3rd boot server, boot protocol, and so on. Some of these settings are found in the Hardware->Workstation panel in the NSM Web interface. Many are not available from the Web interface.

DEVICE Denotes printer and serial device settings. These settings are found in the Hardware->Printers and Hardware->Serial Devices panels in the NSM Web interface.

DESKTOP Denotes NC Desktop settings such as icon placement, logout button, etc. Some of these are settings are found in the Desktop->Display panel in the NSM Web interface. Many are not available from the Web interface.

NS5250 Denotes 5250 emulator settings such as keyboard remapping enabled/disabled, menus enabled/disabled, and so on. These settings correspond to those found in the Applications->5250 panel in the NSM Web interface.

NS3270 Denotes 3270 emulator settings such as keyboard remapping enabled/disabled, menus enabled/disabled, and so on. These settings correspond to those found in the Applications->3270 panel in the NSM Web interface.

NSTERM Denotes VT emulator settings such as keyboard remapping enabled/disabled, menus enabled/disabled, and so on. These settings correspond to those found in the Applications->VT Emulator panel in the NSM Web interface.

NETSCAPE Denotes Netscape Communicator browser settings such as Java applets enabled/disabled, memory cache, and so on. These settings correspond to those found in the Applications->Netscape Communicator panel in the NSM Web interface.

APPLETVIEWER The appletviewer category allows one property setting only, the startup command for the appletviewer.

ENVVARS Denotes environment variables settings. These settings correspond to those found in the General->Environment panel in the NSM Web interface.

ICA Denotes ICA client settings.

INTERNET Denotes Internet-related settings such as the user’s e-mail, home page, etc. These settings correspond to those found in the General->Network panel in the NSM Web interface.

LANGUAGE Denotes language-related settings such as the language to use for menus, date and time format, and so on. These settings correspond to those found in the General->Environment panel in the NSM Web interface.

HLOGIN Denotes login-related settings such as NumLock key on/off. These settings correspond to those found in the Hardware->Workstation panel in the NSM Web interface.

USERGROUP Denotes which main group should be assigned to a user. This setting (only one) corresponds to the Administration->User’s group panel in the NSM Web interface.

RULES Denotes settings that control how the download profiles should be processed. Using these settings, the download override profiles can be enabled/disabled and so on. These settings are note available from the NSM Web interface.

The configname is the name of the setting that should be modified. This name is case sensitive. The configvalue is the value for the configuration. The value is also case sensitive. We do not list all possible settings and values because they are covered in detail in the *IBM Network Station Advanced Information V2R1* document.

Note

The NSMCL supports all settings available from the NSM browser-based GUI except settings for the Launch Bar. That means, in order to add or modify icons on the Launch Bar for users, you need to use the NSM browser-based GUI.

8.5.2 Initializing the SGCL.ini file

Before using the NSM command line interface, you need to update the initialization file, SGCL.ini, in the $ServBase/tools directory. The parameters in the file are commented and are self-explanatory. We found two parameters that we wanted to update.

The PATH_TO_SCRIPTS statement contains the directory where you will keep scripts. For simplicity, we chose to keep our scripts in the $ServBase/tools directory (d:\NetworkStationV2\servbase\tools for Windows NT). To do this, we simply blanked out the path so it defaulted to the current directory:

```
PATH_TO_SCRIPTS=
```

We also updated the PATH_TO_PROFILES statement with the directory where our NSM V2R1 files were installed. Our statement in the SGCL.INI file looked like this example:

```
PATH_TO_PROFILES=d:\NetworkStationV2\Userbase\
```

8.5.3 NSMCL command line interface

As mentioned before, you need the proper Java environment (Java 1.1.6 or later) to run the command line interface. This includes setting up the correct classpath for the Java classes.

To make this easier, we created a BAT file to run the NSMCL in command mode. We called the BAT file SGCL.BAT (lines are split for easier reading here) and put it in the $ServBase/tools directory. Our example is shown in Figure 136.

```
@java -classpath d:\jdk1.1.8\bin;d:\jdk1.1.8\;d:\jdk1.1.8\lib\classes.zip;
.;d:\networkstationv2\servbase\tools\ibmnsmcl.jar;
d:\networkstationv2\servbase\tools\jt400.jar;
d:\networkstationv2\servbase\tools\ibmxml.jar com.ibm.nsm.cl.SGCL %1 %2 %3 %4 %5 %6 %7 %8 %9
@type sgcl_log.txt
```

Figure 136. BAT file for running NSMCL in command mode

The bat file allows you to enter SGCL.bat followed by the command. To run the command line interface using SGCL, switch to the $ServBase/tools directory and execute the bat file. See the example in Figure 137.

```
d:\networkstationv2\servbase\tools\sgcl.bat update ibmnsm/user/sadtler/
workstation/pref-mouse-arrangement/left-handed
```

Figure 137. Example of running 'left-handed' bat file

8.5.4 NSMCL graphical user interface

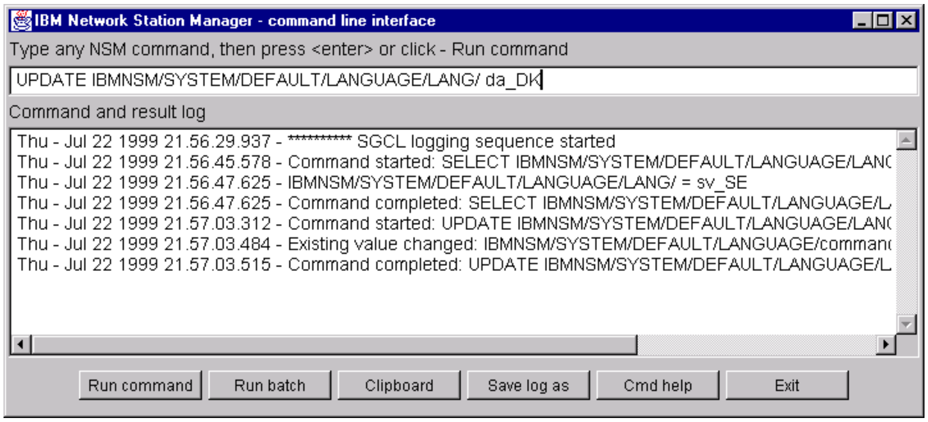
The graphical version of NSMCL also uses the SGCL.ini file for initializing the environment. Once again, you must have the proper Java environment to run the interface, including the correct classpath.

To make it easier to start also the graphical interface, we created a small BAT file for invoking it. We called the BAT file nsm_cl.bat and put it in the $ServBase/tools directory (lines are split for easier reading). Our example is shown in Figure 138.

```
java -classpath d:\jdk1.1.8\bin;d:\jdk1.1.8\;d:\jdk1.1.8\lib\classes.zip;
.;d:\networkstationv2\servbase\tools\ibmnsmcl.jar;
d:\networkstationv2\servbase\tools\jt400.jar;
d:\networkstationv2\servbase\tools\ibmxml.jar com.ibm.nsm.cl.NSM_CL
```

Figure 138. BAT file for running NSMCL in graphical mode

To run the bat file just created, switch to the $ServBase/tools directory (d:\NetworkStationV2\servbase\tools for Windows NT) and enter `nsmcl.bat`. Using this script, we could then launch the graphical version of NSMCL (Figure 139).



Type any NSM command, then press <enter> or click - Run command

UPDATE IBMNSM/SYSTEM/DEFAULT/LANGUAGE/LANG/ da_DK

Command and result log

```
Thu - Jul 22 1999 21.56.29.937 - ********** SGCL logging sequence started
Thu - Jul 22 1999 21.56.45.578 - Command started: SELECT IBMNSM/SYSTEM/DEFAULT/LANGUAGE/LAN(
Thu - Jul 22 1999 21.56.47.625 - IBMNSM/SYSTEM/DEFAULT/LANGUAGE/LANG/ = sv_SE
Thu - Jul 22 1999 21.56.47.625 - Command completed: SELECT IBMNSM/SYSTEM/DEFAULT/LANGUAGE/L
Thu - Jul 22 1999 21.57.03.312 - Command started: UPDATE IBMNSM/SYSTEM/DEFAULT/LANGUAGE/LAN(
Thu - Jul 22 1999 21.57.03.484 - Existing value changed: IBMNSM/SYSTEM/DEFAULT/LANGUAGE/comman(
Thu - Jul 22 1999 21.57.03.515 - Command completed: UPDATE IBMNSM/SYSTEM/DEFAULT/LANGUAGE/L
```

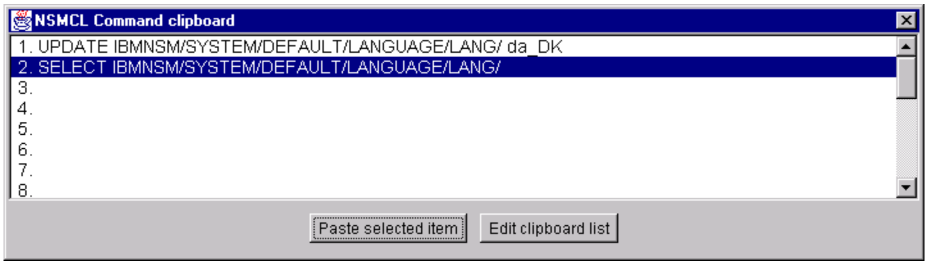
Figure 139. NSMCL graphical user interface

The graphical version does much the same as the command line versions. However, in the graphical version, you have the ability to copy and paste commands, thereby reusing them, and you can view the log file instantly.

You type the commands into the command field and then press Enter. Click **Run Command**. You can scroll through your 20 most recently used commands by pressing the Up and Down keys on the keyboard.

If you click the **Run Batch** button, you can load a script file and execute the commands in it.

If you click the **Clipboard** button, you see a list of your 20 most recently used commands (Figure 140).



1. UPDATE IBMNSM/SYSTEM/DEFAULT/LANGUAGE/LANG/ da_DK
2. SELECT IBMNSM/SYSTEM/DEFAULT/LANGUAGE/LANG/
3.
4.
5.
6.
7.
8.

Figure 140. The NSM_CL graphical clipboard

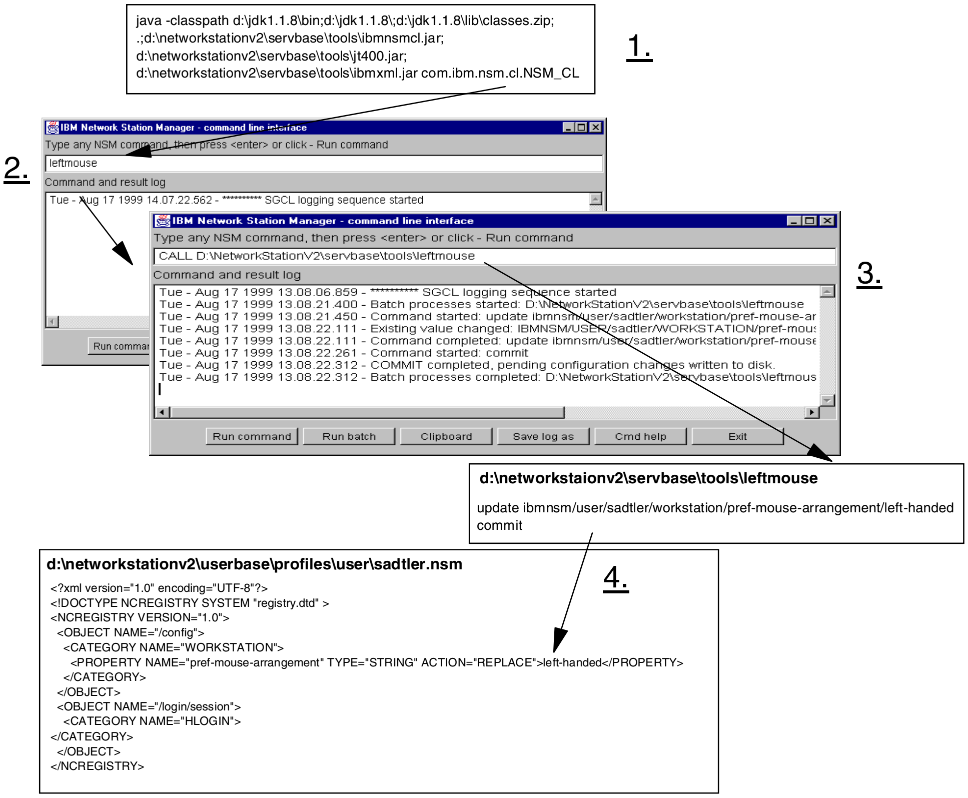
To recall a previous command, select it. Then, click **Paste selected item**. If you want, click **Edit clipboard list** and save the clipboard to a file or load a file you've previously saved. This can be useful if you have commands you need to carry out frequently.

8.5.5 NSMCL process overview

There are several important points to remember about running the NSM command line process:.

- You must have the proper Java environment. Problems running the command usually start here. If you have problems, check the following items:
  - You need to make sure Java 1.1.6 or later is installed.
  - The proper classpath is either set up permanently or entered as part of the command.
  - The path containing the SGCL.ini file is accessible from where you are running the command. It is easiest to switch into the $ServBase/tools directory to execute the command line interface.
- Remember to commit the changes

For a quick overview of how the commands work, see Figure 141.



```
java -classpath d:\jdk1.1.8\bin;d:\jdk1.1.8\;d:\jdk1.1.8\lib\classes.zip;
.;d:\networkstationv2\servbase\tools\ibmnsmcl.jar;
d:\networkstationv2\servbase\tools\jt400.jar;
d:\networkstationv2\servbase\tools\ibmxml.jar com.ibm.nsm.cl.NSM_CL
```

Type any NSM command, then press <enter> or click - Run command

```
leftmouse
```

Command and result log

```
Tue - Aug 17 1999 14.07.22.562 - ********** SGCL logging sequence started
```

Type any NSM command, then press <enter> or click - Run command

```
CALL D:\NetworkStationV2\servbase\tools\leftmouse
```

Command and result log

```
Tue - Aug 17 1999 13.08.06.859 - ********** SGCL logging sequence started
Tue - Aug 17 1999 13.08.21.400 - Batch processes started: D:\NetworkStationV2\servbase\tools\leftmouse
Tue - Aug 17 1999 13.08.21.450 - Command started: update ibmnsm/user/sadtler/workstation/pref-mouse-ar
Tue - Aug 17 1999 13.08.22.111 - Existing value changed: IBMNSM/USER/sadtler/WORKSTATION/pref-mous
Tue - Aug 17 1999 13.08.22.111 - Command completed: update ibmnsm/user/sadtler/workstation/pref-mouse
Tue - Aug 17 1999 13.08.22.261 - Command started: commit
Tue - Aug 17 1999 13.08.22.312 - COMMIT completed, pending configuration changes written to disk.
Tue - Aug 17 1999 13.08.22.312 - Batch processes completed: D:\NetworkStationV2\servbase\tools\leftmous
```

d:\networkstaionv2\servbase\tools\leftmouse

```
update ibmnsm/user/sadtler/workstation/pref-mouse-arrangement/left-handed
commit
```

d:\networkstationv2\userbase\profiles\user\sadtler.nsm

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCREGISTRY SYSTEM "registry.dtd" >
<NCREGISTRY VERSION="1.0">
  <OBJECT NAME="/config">
    <CATEGORY NAME="WORKSTATION">
      <PROPERTY NAME="pref-mouse-arrangement" TYPE="STRING" ACTION="REPLACE">left-handed</PROPERTY>
    </CATEGORY>
  </OBJECT>
  <OBJECT NAME="/login/session">
    <CATEGORY NAME="HLOGIN">
</CATEGORY>
  </OBJECT>
</NCREGISTRY>
```

Figure 141. NSM_CL Example

The process flow shown in Figure 141 is explained here:

1. The administrator enters the Java command to invoke the graphical interface, either by entering the entire command, or by creating a .bat file and executing it.
2. The graphical interface allows you to enter commands directly or to execute batch files. In this example, a batch file was created with the update command and commit command. The administrator enters the file name on the command line and clicks a Run batch.
3. The batch file is read and the commands are executed. The output messages appear on the console. The update command is stored in a buffer. No changes have actually been made. At this point, the command should either be committed, rolled back (erased), or more commands entered.
4. The commit command causes the actual change to be made. In this case, the change was specific to a user and was stored in the users profile.

8.5.6 NSMCL examples

This section provides some examples of how the NSMCL could be used. If you use the SGCL.bat file created in the previous section, add `SGCL.bat` in front of the commands. If using the graphical interface, type them in as shown. Remember to run the `commit` command after each sequence of commands. Otherwise, the changes will not be written to disk.

8.5.6.1 Changing the IP address of a particular Network Station

If not using DHCP, it may sometimes be necessary to change the IP address of a particular Network Station (for example, if the network topology has changed). The setting that controls this is EXTERNAL/ip-address-at-next-boot. To change the IP address of a Network Station from 9.24.104.192 to 9.24.105.6 without physically visiting it, the following command can be used (the lines split here for easier reading):

```
INSERT IBMNSM/WORKSTATION/9.24.104.192/EXTERNAL/
ip-address-at-next-boot/ 9.24.105.6
COMMIT
```

For this change to take effect, the Network Station must be rebooted twice. On the first reboot, it reads the download profile where the “update your IP address” command is stored (\userbase\profiles\ncs\9.24.104.192.nsm) and writes it into NVRAM. Then, on the second reboot, it reads its new IP address from NVRAM and uses this new IP address to insert into the network.

8.5.6.2 Adding a new boot server

Again, assuming we don’t use DHCP, let’s say that the number of Network Stations in one of our remote branch offices has grown substantially so we decided to add a new boot server. Since our new boot server (which is given the IP address 9.24.104.13) is more powerful than our existing one (which has IP address 9.24.104.2), we want to use the new one as the primary boot server and keep the old one as a backup server. The subnet for the remote branch office is 9.24.104.0 and is a C-class subnet. We want to make this change to all our Network Stations in this subnet. The settings that control the primary and secondary boot servers are EXTERNAL/boot-tcpip-desired-server and EXTERNAL/boot-tcpip-second-server.

First, we have to create a list of all our Network Stations in the 9.24.104.0 subnet (let’s say beginning with IP address 9.24.104.20 and ending with IP address 9.24.104.250):

```
9.24.104.20
9.24.104.21
9.24.104.22
9.24.104.23
..
..
9.24.104.250
```

If we save this list in a file called gothenburg.txt (because that is where the remote branch is), we can use the following two commands to perform the change (lines are split here for easier reading):

```
INSERT IBMNSM/WORKSTATION/list gothenburg.txt/EXTERNAL/
boot-tcpip-desired-server/ 9.24.104.13
INSERT IBMNSM/WORKSTATION/list gothenburg.txt/EXTERNAL/
boot-tcpip-second-server/ 9.24.104.2
COMMIT
```

The first command tells all Network Stations listed in the gothenburg.txt file to use the 9.24.104.13 boot server as their primary server. The second command tells the same Network Stations to use the 9.24.104.2 boot server as their secondary server.

As with the previous example, the Network Stations needs to be rebooted twice in order for them to use the new boot server.

8.5.6.3 Defining the main group for a group of users

To make settings for a specific group of users in NSM, the users must have that group defined as their main group in NSM. Let's say we want the user claude to be assigned the Sales_Local group as his main group. We can use the following command:

```
INSERT IBMNSM/SYSTEM/DEFAULT/USERGROUP/claude/ Sales_Local
COMMIT
```

If we want to make the same association for a large number of users, we can create a script for it. To create the input for the script, we can use any tool that can extract the users from a particular group (for example, the Sales_Local group) in the operating system. Let's say we extract the following list of users:

- carla
- claude
- gordana
- henrik

Then, we can use the following script to assign all these users the Sales_Local group as their main group:

```
INSERT IBMNSM/SYSTEM/DEFAULT/USERGROUP/carla/ Sales_Local
INSERT IBMNSM/SYSTEM/DEFAULT/USERGROUP/claude/ Sales_Local
INSERT IBMNSM/SYSTEM/DEFAULT/USERGROUP/gordana/ Sales_Local
INSERT IBMNSM/SYSTEM/DEFAULT/USERGROUP/henrik/ Sales_Local
COMMIT
```

8.5.6.4 Remapping the Alt+Tab, Alt+F4, Ctrl+Alt+Del keys

When the ICA client is used on the Network Station, some keys do not behave as many Windows users are accustomed to. For example, when the Alt-Tab keys are pressed on the Network Station, it circles through the local Network Station applications that are active (3270, 5250, ICA client, and so on). When the same keys are pressed on a Windows PC, it circles between the Windows applications started. The reason for this different behavior is that the Network Station's Window Manager steals the Alt+F4 key sequence and does not pass it into the ICA client. To circumvent this problem, the Alt+F4 key sequence can be remapped to something else, for example Ctrl+Tab. To do that, we use the following NSMCL command:

```
INSERT IBMNSM/SYSTEM/DEFAULT/DESKTOP/key_window_switch/~Shift Ctrl<Key>Tab
INSERT IBMNSM/SYSTEM/DEFAULT/DESKTOP/key_window_switch_back/Shift Ctrl<Key>Tab
COMMIT
```

The same problem appears with the Alt+F4 key. When pressed on a Windows PC, it terminates the Windows application in focus, but when pressed on the Network Station, it terminates the whole ICA client. To remap the Alt+F4 key to Shift+Ctrl+F4, for example, we use the following command:

```
INSERT IBMNSM/SYSTEM/DEFAULT/DESKTOP/key_window_close/Shift Ctrl<Key>F4
COMMIT
```

To unmap the Alt+F4 completely, we use the following command:

```
INSERT IBMNSM/SYSTEM/DEFAULT/DESKTOP/key_window_close/ nil
COMMIT
```

We had to put something after the trailing slash and a space was not enough (it was stripped by NSMCL). We chose an invalid key combination that would never appear (no user can press the keys n, i and l simultaneously).

When the key combination Ctrl+Alt+Del is pressed on the Network Station, it means the Window Manager should stop the local application in focus immediately. Some Windows users use this key combination to quickly bring up the dialog where they can lock their computer, logoff, shutdown, etc. To unmap this combination so the Ctrl+Alt+Del sequence is passed onto the ICA client, we use the following command:

```
INSERT IBMNSM/SYSTEM/DEFAULT/DESKTOP/key_window_kill/ nil
COMMIT
```

Now we can press Ctrl+Alt+Del when the ICA client is in focus to quickly logoff from our Metaframe servers for example.

For reference purposes, we have included a list of the possible key combinations and their default values (Table 28).

Table 28. The Window Manager's key combinations

Default values	Key combinations
key_toggle_keys	Shift Ctrl Alt<Key>F11
key_print_window	Alt<Key>PrtSc
key_print_screen	~Alt<Key>PrtSc
key_information	Ctrl Alt<Key>I
key_login_name	Ctrl Alt<Key>L
key_window_kill	Ctrl Alt<Key>Delete
key_logoff	Ctrl Alt<Key>BackSpace
key_version	Ctrl Alt<Key>V
key_window_switch_back	Shift Alt<Key>Tab
key_window_switch	~Shift Alt<Key>Tab
key_window_menu_alt	Alt<Key>minus
key_window_menu	Alt<Key>space
key_root_menu	Alt<Key>F10
key_window_close	Alt<Key>F4

8.6 NSM V2R1 directory structure

NSM V2R1 includes a completely new underlying operating system, which has a different directory structure from V1R3. We describe the directory structure used by V2R1. This information is merely for the anyone interested in digging really deep into the heart of the Network Station. It's definitely not necessary to understand where the files are and what they do to install, use, and administer Network Stations. Also, since NSM V2R1 includes more than 8,000 files in 700 directories, we don't cover them all, but rather the ones we found interesting and worth knowing about while investigating V2R1.

Important note

If you manually modify any of the configuration files in any of the directories, you must make sure that you do not accidentally convert them from their original UNIX file formats into, for example, DOS/Windows file formats. A text file on a DOS or Windows PC uses CR/LF (Carriage Return and Line Feed, ASCII code 13 and 10, respectively) as the end-of-line marker. A text file in UNIX only uses LF. This means you must not use, for example, Notepad to modify these files, since it's not aware of the UNIX end-of-line marker. If you do, you may accidentally save the file in an unusable DOS/Windows format.

We recommend that you use the free Programmer's Facility Editor (PFE) if you want to look at and modify the files. PFE can be downloaded from its author's site at: `http://www.lancs.ac.uk/people/cpaap/pfe`

The directory structure for the three server platforms, AIX, Windows NT, and AS/400, are similar but not exactly the same. The higher levels of the path structure vary slightly. To make this discussion generic, we use variables to denote the initial path structure. Table 29 lists these variables.

Table 29. Substitution variables used for V2R1 Network Station directories

Substitution variables	Value
$ProdBase (AS/400)	/QIBM/ProdData/NetworkStationV2
$HttpBase (AS/400)	/QIBM/ProdData/HTTP/Protect/NetworkStationV2
$ServBase (AS/400)	/QIBM/ProdData/NetworkStationV2/NSM
$UserBase (AS/400)	/QIBM/UserData/NetworkStationV2/
$ProdBase (RS/6000)	/usr/NetworkStationV2/prodbase
$ServBase (RS/6000)	/usr/NetworkStationV2/servbase
$UserBase (RS/6000)	/usr/NetworkStationV2/userbase
$ProdBase (Windows NT)	<float>\NetworkStationV2\prodbase
$ServBase (Windows NT)	<float>\NetworkStationV2\servbase
$UserBase (Windows NT)	<float>\NetworkStationV2\userbase

The NetworkStationV2 directory includes three major subdirectories which are shown in Figure 142 on page 192.

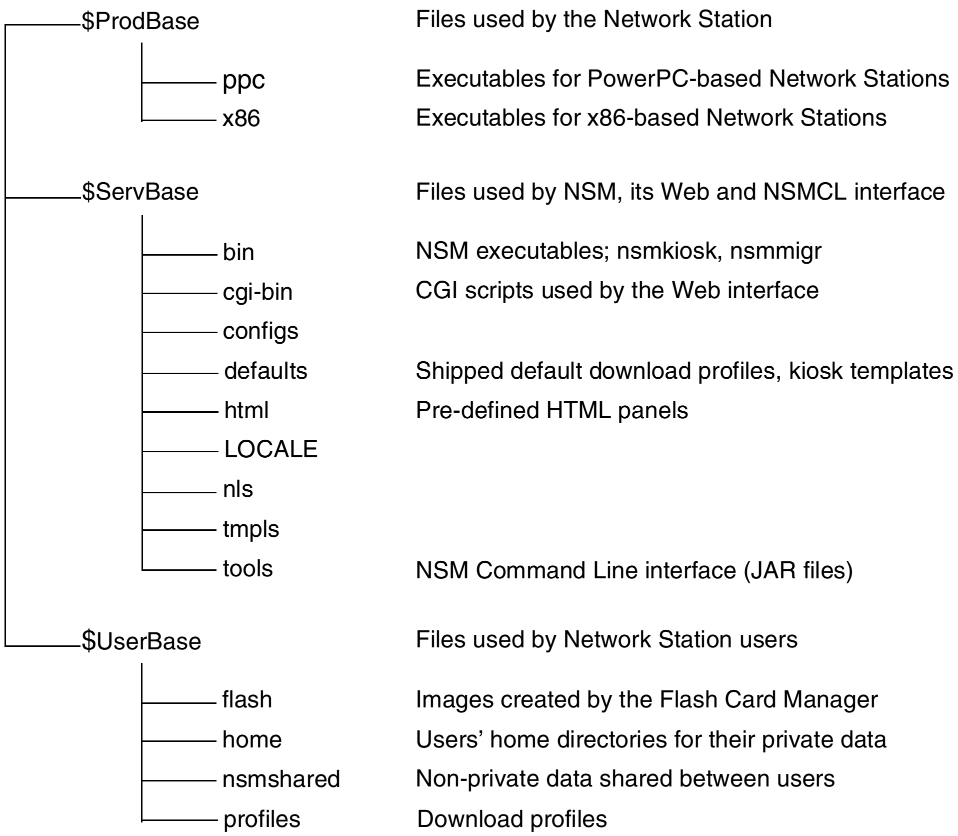

$ProdBase
Files used by the Network Station
ppc
Executables for PowerPC-based Network Stations
x86
Executables for x86-based Network Stations
$ServBase
Files used by NSM, its Web and NSMCL interface
bin
NSM executables; nsmkiosk, nsmmigr
cgi-bin
CGI scripts used by the Web interface
configs
defaults
Shipped default download profiles, kiosk templates
html
Pre-defined HTML panels
LOCALE
nls
tmpls
tools
NSM Command Line interface (JAR files)
$UserBase
Files used by Network Station users
flash
Images created by the Flash Card Manager
home
Users' home directories for their private data
nsmshared
Non-private data shared between users
profiles
Download profiles

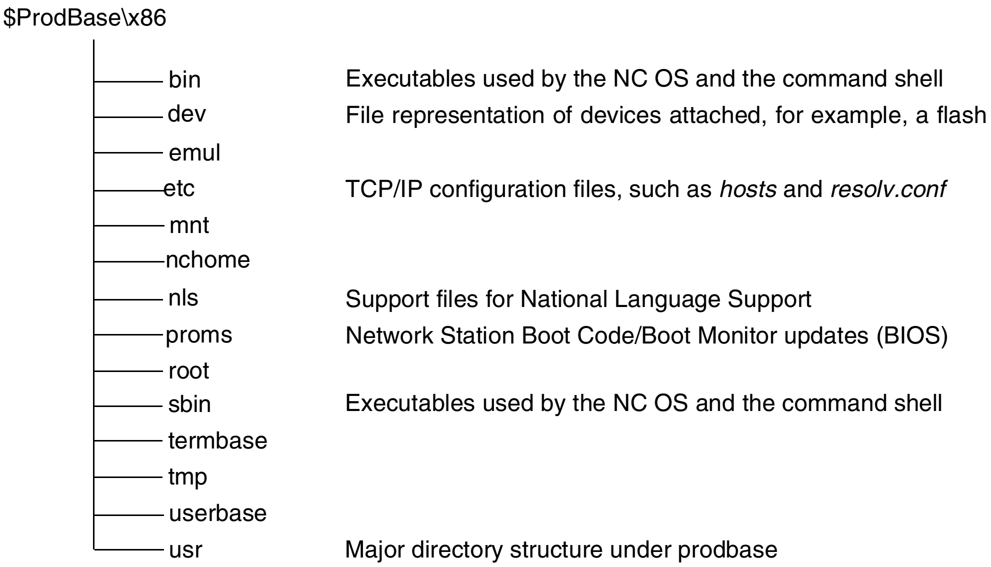
Figure 142. NSM V2R1 directory structure

8.6.1 Prodbase

The prodbase directory holds the Network Station executables (Figure 143). The Network Station only *reads* from this directory. It never writes. The prodbase directory has one subdirectory for each type of Network Station CPU architecture: ppc for PowerPC-based Network Stations (Series 300, Series 1000) and x86 for x86-based Network Stations (Series 2200, Series 2800).

In the prodbase root directory, there are several files with .BOM extensions. These are the so called *Bill Of Materials* files used by the Flash Manager when building flash card images.

The prodbase directory is exported read-only as $ProdBase with both the NFS and TFTP protocols.



$ProdBase\x86

bin	Executables used by the NC OS and the command shell
dev	File representation of devices attached, for example, a flash
emul	
etc	TCP/IP configuration files, such as *hosts* and *resolv.conf*
mnt	
nchome	
nls	Support files for National Language Support
proms	Network Station Boot Code/Boot Monitor updates (BIOS)
root	
sbin	Executables used by the NC OS and the command shell
termbase	
tmp	
userbase	
usr	Major directory structure under prodbase

Figure 143. NSM V2R1 prodbase directory structure

The **bin** and **sbin** directories include executables and scripts that are used by the Network Station's operating system. Some of them may also be useful for an administrator when doing, for example, problem determination.

The **dev** directory is used for file representation of any devices attached to the Network Station. UNIX knows nothing about CON:, LPT1:, and COM1, for example, but uses /dev/tty, /dev/lpt1, and so on instead.

The **etc** directory holds some important configuration files:

- **hosts**
  The hosts file defines the list of IP address and hostname pairs that are used if a DNS server is not available or does not have the information. If the servers you need to access are not in your DNS servers, you can add them here. Since the information in this file is used before a DNS lookup occurs, you can also override DNS entries by adding them here. You do not need to reboot or logoff the Network Station for your changes to this file to become active. During the NSM installation, this file is populated with the corresponding information from the server on which NSM is installed. Here is an example of a valid hosts file:

  ```
  127.0.0.1 localhost
  9.24.104.252 henrik henrik.itso.ral.ibm.com
  9.24.104.253 nsmv2r1 nsmv2r1.itso.ral.ibm.com
  9.24.105.22 mail.itso.ral.ibm.com
  ```

  If you edit the file, you must make sure that you do not accidentally remove the `127.0.0.1 localhost` line.

- **resolv.conf**
  This file is used to define the DNS configuration. During the NSM installation, this file is populated with the corresponding information from the server on which NSM is installed. It can also be updated by selecting **NSM->[System]->Hardware->Domain Name Server: Update Network Station Manager DNS file** option in NSM. A valid resolv.conf file is shown in the following example:

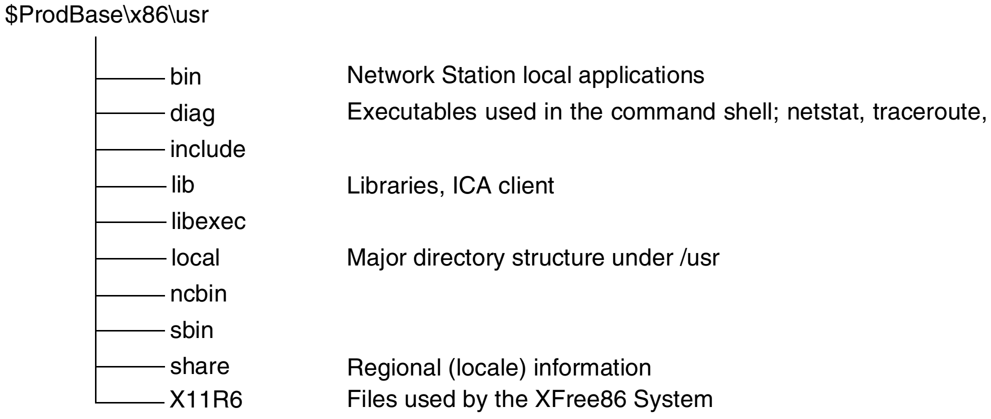
```
domain itso.ral.ibm.com
nameserver 9.24.104.108
nameserver 9.52.37.134
lookup file bind
```

The **proms** directory holds the Network Station Boot Code (Boot Monitor) update images. These files are used to update the firmware (BIOS) in the Network Stations. This is done by selecting **NSM->[System]->Hardware->Workstations->[Boot Parameters]** and setting the Update to boot code installed on the boot server parameter to `Update`.

The **usr** directory is a major directory structure under the prodbase directory.

8.6.1.1 prodbase\..\usr

Figure 144 shows the prodbase\..\usr directory structure.



$ProdBase\x86\usr
bin
Network Station local applications
diag
Executables used in the command shell; netstat, traceroute,
include
lib
Libraries, ICA client
libexec
local
Major directory structure under /usr
ncbin
sbin
share
Regional (locale) information
X11R6
Files used by the XFree86 System

Figure 144. NSM V2R1 directory prodbase/x86/usr structure

The **bin** directory includes most, but not all, of the Network Stations local (native) applications, such as the 3270, 5250, VT emulators and the Java environment. In addition to these well-known applications there are many of the support files the Network Station needs, such as actlogin, lpr, and so on.

The **lib** directory includes libraries. Also, to maintain full compatibility with the Citrix ICA client for UNIX, the ICA client is installed in its original directories, which is /usr/lib/ICAClient. In the /usr/lib/ICAClient/config directory, there are the appsrv.ini, module.ini, and wfclient.ini files that NSM uses to customize the ICA client.

The **share** directory includes regional (locale) definitions, two SNMP MIB definitions, and so on.

The **X11R6** directory includes all of the support files for the XFree86 system, including fonts (about 13 MB), NLS files, etc. XFree86 is a freely redistributable implementation of the X Window System that runs on UNIX and UNIX-like operating systems (and OS/2). More information on XFree86 can be found on the Web at: `http://www.xfree86.org`

The **local** directory is a major directory structure under /usr.

8.6.1.2 prodbase\..\usr\local

Figure 145 shows the directory structure for prodbase\..\usr\local.

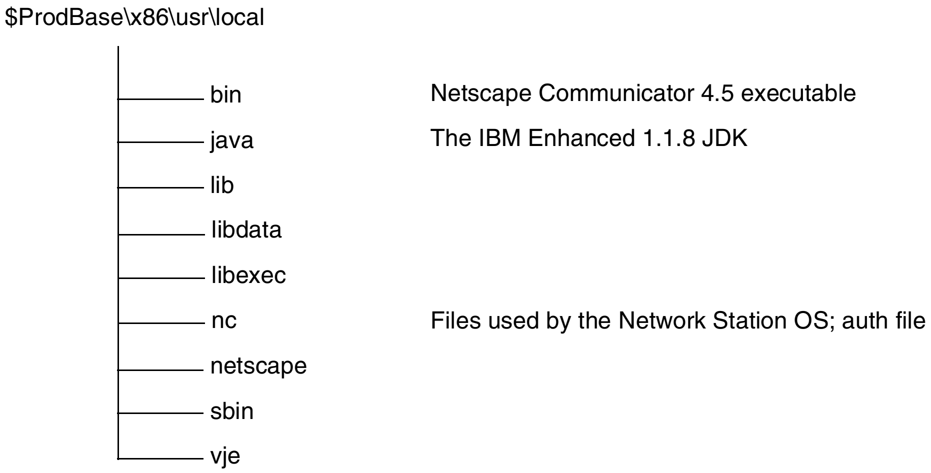

$ProdBase\x86\usr\local
bin
Netscape Communicator 4.5 executable
java
The IBM Enhanced 1.1.8 JDK
lib
libdata
libexec
nc
Files used by the Network Station OS; auth file
netscape
sbin
vje

Figure 145. NSM V2R1 directory structure, NetworkStationV2\prodbase\x86\usr\local

The **bin** directory stores the Netscape Communicator 4.5 executables.

The **java** directory has a **J118** subdirectory that holds all the files used by the IBM enhanced 1.1.8 JVM.

The **nc** directory holds support files used by the Network Station operating system. The only really interesting file here is the **auth** file in the usr/local/nc/boot/login directory. This file specifies which user ID user IDs are allowed to remotely login to the Network Station. See the 18.6, “Remote Shell Program command” on page 598, for more details on this.

The **netscape** directory includes support files used by Netscape Communicator 4.5, such as its Java classes, help files, and so on. The netscape.cfg file contains the default settings for Netscape Communicator 4.5.

8.6.2 Servbase

The servbase directory (Figure 146 on page 196) is used by the Network Station Manager and its Web and NSMCL interface.

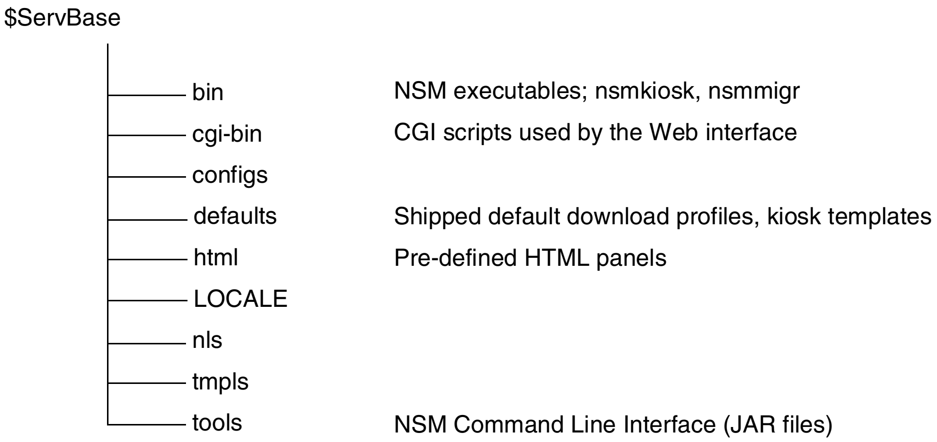

$ServBase
bin
NSM executables; nsmkiosk, nsmmigr
cgi-bin
CGI scripts used by the Web interface
configs
defaults
Shipped default download profiles, kiosk templates
html
Pre-defined HTML panels
LOCALE
nls
tmpls
tools
NSM Command Line Interface (JAR files)

Figure 146. NSM V2R1 directory structure for NetworkStationV2\servbase

The **bin** directory stores some utility programs included in NSM. For example, the nsmkiosk is used when creating kiosk files for suppressed login. The nsmmigr is used when migrating from an earlier version of NSM to NSM V2R1. The ntnsmver utility can be used to dump all necessary information from the NSM server to an HTML file, which can be essential for troubleshooting. See 18.7, “NSM Service Tool for Windows NT” on page 598, for more details.

The **cgi-bin** directory includes all of the CGI scripts that make up the intelligence of NSM. The scripts interpret the data sent from the NSM HTML pages and writes it to the download profiles.

The **defaults** directory stores backup files for NSM settings that can be used if it’s necessary to restore the IBM-shipped default values. The kiosk (.ksk) files, which are used as templates when setting up the Network Station in kiosk mode, are also in the defaults.

The **tools** directory includes the files used by the NSMCL utility.

8.6.3 Userbase

The userbase directory (Figure 147) is mostly used for storing download profiles, users’ preferences, and the users’ home directory.

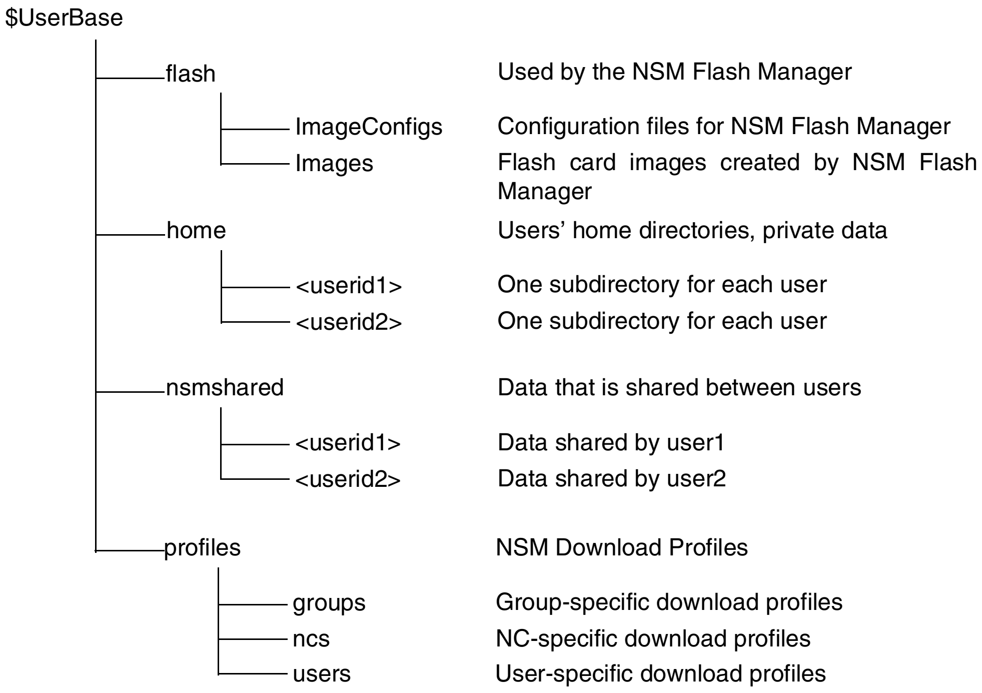

$UserBase
flash
Used by the NSM Flash Manager
ImageConfigs
Configuration files for NSM Flash Manager
Images
Flash card images created by NSM Flash Manager
home
Users’ home directories, private data
<userid1>
One subdirectory for each user
<userid2>
One subdirectory for each user
nsmshared
Data that is shared between users
<userid1>
Data shared by user1
<userid2>
Data shared by user2
profiles
NSM Download Profiles
groups
Group-specific download profiles
ncs
NC-specific download profiles
users
User-specific download profiles

Figure 147. NSM V2R1 directory structure for NetworkStationV2/userbase

The **flash** directory is used by the NSM Flash Manager utility. Each flash card image created by the utility is stored in a separate subdirectory in the Images directory.

The **home** directory is where each users’ private data is stored.

The **nsmshared** directory stores data that is not private to a user but is to be shared between many users.

The **profiles** directory stores the download profiles for all levels (IBM-shipped defaults, system, group, user, and workstation level).

8.6.4 Userbase\nsmshared: Users’ shared data

Figure 148 on page 198 shows the userbase\nsmshared directory structure.

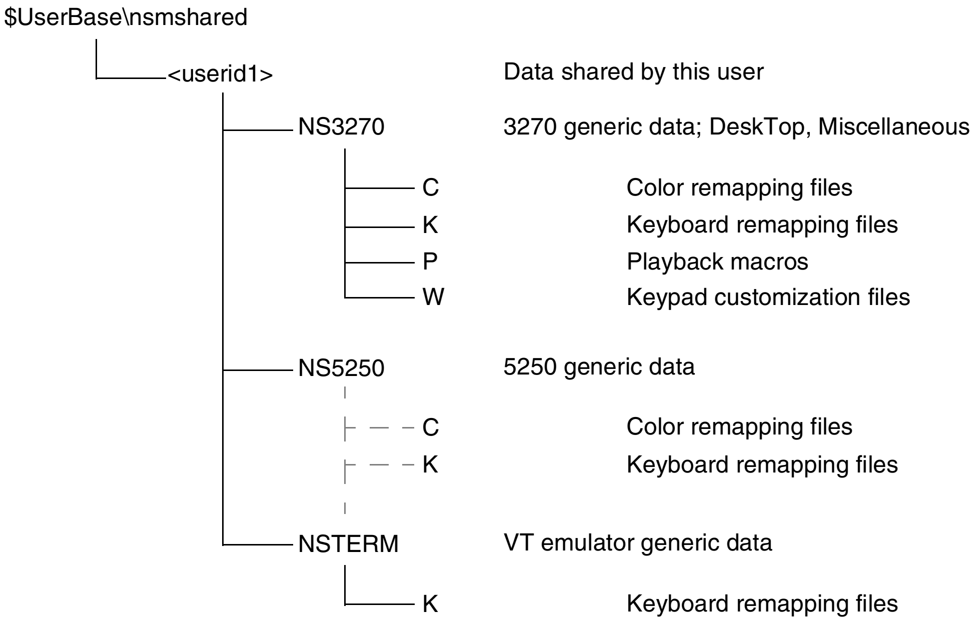


Figure 148. NSM V2R1 directory structure for NetworkStationV2/userbase/nsmshared

Each application that needs to share data among users (for example, when an administrator creates a 3270 keyboard remap they want all their users to use) creates its own subdirectory in each users' subdirectory in nsmshared. Let's take the 3270 emulator as an example. It creates up to four subdirectories in the NS3270 directory to hold data that is shared by this user. The C directory is for storing color mapping files, the K directory is for storing keyboard remapping files, the P directory is for storing playback macro files, and the W directory is for storing keypad customization files.

In addition to the information stored in the C, K, P, and W subdirectories, the 3270 emulator also stores such information as the DeskTop and Miscellaneous files in its NS3270 directory. The DeskTop file stores the size and position of the window so it can be retrieved the next time the emulator starts. The Miscellaneous file stores miscellaneous settings made in the emulator.

8.6.4.1 Userbase\home: Users' home directory

Each user logging on to the Network Station is also given a home directory, which is used for storing user-private data. Each application (for example, Netscape Communicator, ICA client, and so on) that needs to store user-private data creates its own directory in each users' home directory. Information in the user's home directory is not accessible by anyone but the user. The information stored varies from application to application. For example, Netscape Communicator stores the user's bookmarks, cookies, history file, and so on.

In the user's home directory, there is also a directory called public_html. This appears to the user as the "My Web Site" folder when the user views it in some applications' "File Open" dialogs. Most applications do not support this special directory. This directory is actually a symbolic link pointing to the public_html directory in the user's home directory ($HOME/public_html). This is the place where common Web servers, such as Apache, look for documents to be made available publicly.

There is also a directory called registry with three subdirectories: desktop, documents, and tmp (temporary). The desktop directory saves information on the user's current desktop look-and-feel so it can be retrieved the next time the user logs on. The documents directory is the default directory to store documents. The tmp directory is the user's temporary directory, which applications use to temporarily store files.

8.7 Mount points

The directories that need to be accessed by the Network Station need to be *mounted* from the Network Station. This is done automatically when the Network Station is powered on and when the user logs on. For those interested in digging into the heart of the Network Station, it is good to know the so called *mount points* being used. These points are explained in Table 30.

Table 30. Mount points used by the Network Station

Server export	Client path	Description
$ProdBase/ppc or $ProdBase/x86	/	Provides read-only access to the architecture-specific root file system. It is exported through RFS and TFTP or NFS and TFTP. This mount point lasts for the life of the machine session.
$UserBase/profiles	/termbase/profiles	Provides read-only access to terminal specific configuration data. It is exported through RFS or NFS. This is a transient mount point for reading terminal profiles and is only established during the boot sequence.
$UserBase/profiles	/userbase/profiles	Provides read-only access to user and group-specific configuration data. It is exported through RFS or NFS. The directories within this export must have appropriate permissions set to allow or limit client access as needed. This mount point lasts for the life of the user session.
$UserBase/home	/userbase/home	Provides read-write access to the user's home directory on the authentication server. It is exported through RFS or NFS. The directories within this export must have appropriate permissions set to allow or limit client access as needed. This mount point lasts for the life of the user session.

Server export	Client path	Description
$UserBase/nsmshared	/userbase/nsmshared	Provides read-write access to the user's shared directory. It is exported through RFS or NFS. The directories within this export must have appropriate permissions set to allow or limit client access as needed. This is a transient mount point that is only established as needed by client applications.

Tip

The mount points used can be viewed with the `mount` command from the Advanced Diagnostics shell.

For other UNIX commands that you can run from the Advanced Diagnostic Window, see Appendix C, "UNIX commands" on page 613.

8.8 eNetwork On-Demand server

The IBM Network Station Manager program on Windows NT ships with a set of TCP/IP support programs called the IBM eNetwork On-Demand Server. These are used by the Network Station Manager to support the Network Stations so they can receive their IP addresses, access files on different servers, and so on.

The administration GUIs for these applications (where applicable) are written in Java, so the look-and-feel of them may not be what a Windows NT administrator would expect. Despite their look-and-feel, they have capabilities that go well beyond the corresponding TCP/IP services included in the Windows NT 4.0 operating system. Do not judge them from just looking at them. The only corresponding TCP/IP service found in the Microsoft Windows NT 4.0 TCP/IP stack is really the DHCP server. All others are not standard in the Windows NT 4.0 TCP/IP stack.

8.8.1 TCP/IP services

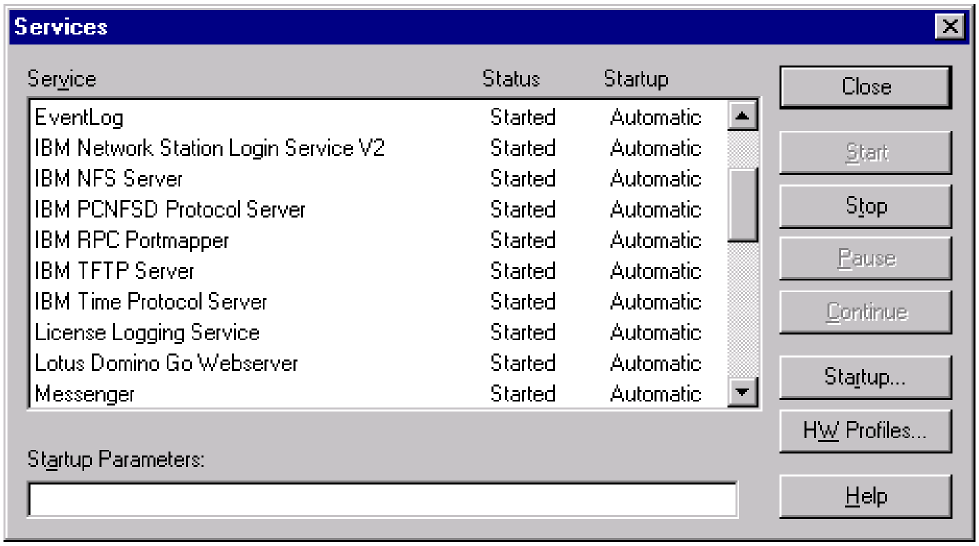
The following TCP/IP services are included in eNetwork On-Demand:

- **DHCP server**: The DHCP server is capable of supporting both unlisted and listed clients (Windows NT 4.0 DHCP server calls this *client reservations*). In addition to this, it also supports the additional DHCP options required by the Network Stations (66, 67, 211, and so on), as do the Windows NT 4.0 DHCP server. What is not supported by the Windows NT 4.0 DHCP server, however, but by eNetwork On-Demand is the useful *DHCP Classes* feature. This allows the DHCP server to send different DHCP options to different types of clients—Windows 98 PCs, Windows NT 4.0 PCs, Network Station S300, S1000, etc.—and with different values. This can be useful if you mix PCs and Network Stations or different models of Network Stations on the same subnet.
- **DDNS server**: The DDNS server is a Dynamic Domain Name Server. This means it can receive commands from the eNetwork On-Demand DHCP server and update its DNS table with the IP address for a given hostname. This can be used to allow a Network Station (which cannot be given a hostname in its

Boot Monitor setup utility) a fixed hostname, even though its IP address varies from day to day. This can be very useful if you have local printers or serial devices attached to Network Stations and you want to access them using meaningful hostnames, instead of just IP addresses. When the Network Station accepts an IP address from the DHCP server, the DHCP server sends an update command to the DDNS server asking it to update the hostname associated with the Network Stations MAC address with its new IP address. When setting up the DDNS, a table must be created with the Network Stations' MAC addresses and their hostnames.

- **NFS server**: The Network File System (NFS) is the protocol the Network Station uses to access the files on different servers. The NFS protocol can be used both for downloading the kernel file and the support files and also for accessing the user's home directory. The NFS server maintains the NFS security bits in the file system so one user cannot access private data in another user's home directory.
- **TFTP server**: The Trivial File Transfer Protocol (TFTP) is similar to the NFS server, but instead of being a full-featured file system, it's more of a file transfer protocol. The T in TFTP stands for Trivial, and the TFTP protocol only supports a very limited set of commands (a subset of the commands in the FTP protocol) like `get`, `put`, etc. This makes it suitable for downloading the Network Station's kernel and some support files, but not for accessing, for example, the user's home directory, where NFS is a must.
- **RPC Portmapper**: The RPC Portmapper is used by the NFS server to map incoming NFS requests to the correct TCP/IP port number used by the NFS server.
- **TIME server**: Since the Network Station does not have a battery backed-up clock, it needs to retrieve the current time from a time server when it is powered on. The eNetwork On-Demand TIME server provides this capability.
- **Network Station Login server**: A user powers on their Network Station and enters their user ID and password. This information is sent to the Network Station Login server. This service validates the user ID and password to the Windows NT account database (SAM) and replies with an OK or not OK answer.

These functions run as Windows NT services and can be seen in the Control Panel->Services dialog. The DHCP and DDNS servers were not installed on the server where the display in Figure 149 on page 202 was created.



Service	Status	Startup
EventLog	Started	Automatic
IBM Network Station Login Service V2	Started	Automatic
IBM NFS Server	Started	Automatic
IBM PCNFSD Protocol Server	Started	Automatic
IBM RPC Portmapper	Started	Automatic
IBM TFTP Server	Started	Automatic
IBM Time Protocol Server	Started	Automatic
License Logging Service	Started	Automatic
Lotus Domino Go Webserver	Started	Automatic
Messenger	Started	Automatic

Figure 149. eNetwork On-Demand TCP/IP services

As you can see, all these services are automatically started whenever the NSM server is powered on. If you should experience any problems with booting a Network Station or logging on to it, verify that the corresponding Windows NT service is alive.

Also, there is one service called *IBM PCNFSD Protocol Server*. This one works together with the RPC Portmapper to provide services for the NFS server.

These functions do not need to be managed by an administrator. Since the NFS server is capable of exporting other directories than the ones determined by NSM, it can be used to add additional exports. You can find documentation on this by selecting **Start->Programs->eNetwork On-Demand Server**, and clicking the **Documentation** icon from the Windows NT desktop.

8.8.2 Performance tuning the NFS server on Windows NT

The default values used for the NFS server usually provide a good compromise between performance, server CPU load and level of security. However, should you in some cases want to tune the NFS server's values, you can do that by changing a number of values in the Windows NT registry.

These values are located under the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NFSD\Security.

Table 31. NFS server parameters

Value	Explanation
DebugSecurityCache	If set to non-zero, the NFS server operates in verbose logging mode and *many* debug statements are sent to the Windows NT event logger. This impacts the performance of the NFS server. In a production environment, this value should be set to zero, which is the default value.
FileCacheSize	Maximum number of entries in the file information cache. Range is 17 to 997, and the default value is 199. Prime values are recommended.

Value	Explanation
FileInfoMaxCacheAge	Maximum number of seconds before cached file security information is treated as too old to be reliable. Range is 5 to 600, and the default value is 60.
UserCacheSize	Maximum number of entries in the user information cache. Range is 17 to 997, and the default value is 17. Prime values are recommended. This should be set to a value larger than the number of different users expected to access the server during any given short period of time.
UserInfoMaxCacheAge	Maximum number of seconds before cached user security information is treated as too old to be reliable. Range is 5 to 600 seconds, and the default value is 60.

All these values are of REG_DWORD type.

To improve performance and somewhat reduce server CPU load, these values can be increased. This means a larger cache will be used for file and user information. The values in the cache will be valid for a longer period of time. This means the NFS server less often needs to contact the Windows NT security database (SAM) to validate the user's permissions for a requested file or directory.

8.9 Windows NT, NTFS, and NFS security

Note about this chapter

In this chapter, we explain how the Network Station accesses different files and the levels of security involved when doing so. You do not need to understand to install and maintain a network of Network Stations. We also strongly recommend that you *do not* modify any of the securities mechanisms involved, since this may render your Network Station unusable. Also, keep in mind that this applies to the current implementation and is subject to change.

When NSM is installed on a Windows NT server, there are three levels of security involved when a Network Station (or its user) accesses files on the NSM server:

- The first level is the NFS export itself. The directories can be exported either as read-only or as read-write.
- The second level is the UNIX permission bits in the NFS file system. These are grouped into user, group and other permissions as defined in the NFS standard. Since these do not map directly to Windows NT NTFS permissions, the NFS server keeps track of these internally.
- The third level is the Windows NT security system which is built into the Windows NT NTFS file system. By default, the NFS server verifies that the user is allowed to perform the functions they request by checking the NTFS security, but this can be disabled if desired. If disabled, it can reduce the CPU load somewhat on the server and, in some cases, also reduce the network load.

For a Network Station (or a user) to read, write, create, or execute files, it (or the user) must be granted access through all of these three levels. If different levels give the Network Station or the user different permissions, then the most restrictive permission is used.

To explain this, we go through all of these levels in more detail in the following sections.

8.9.1 NFS exports

When the eNetwork On-Demand Server exports a directory using the NFS server, it can export it either with read-only or with read-write permissions. If it's exported as read-only, then *no* client (Network Stations or a user) can write to the exported directory. If the directory is exported as read-write, then *all* clients (Network Stations or a user) can write to the directory (unless they're denied access by any of the other two levels, of course). The NFS server also has the capability to export a directory read-only for some hosts and read-write for others. This capability is not used by NSM. Also, when exporting a directory. The NFS server can control whether accesses to it also must be verified by the Windows NT NTFS security system. The NFS server has the capability of doing this on a global basis (for all exports) or down to an individual export.

When NSM is installed on a Windows NT server, it exports the directories shown in Table 32 by default.

Table 32. NSM default NFS exports

Directory	Alias	Permissions
x:\{float}\NetworkStationV2\prodbase	/NetworkStationV2/prodbase	read-only
x:\{float}\NetworkstationV2\userbase	/NetworkStationV2/userbase	read-write

The `x:\{float}` denotes the directory where NSM is installed, for example, `D:\Programs`.

As shown in Table 32, no Network Stations or users can write to the /NetworkStationV2/prodbase directory where the Network Station executables are. However, all users have write access to the /NetworkStationV2/userbase directory and access permissions for this directory. Its subdirectories are then controlled by the other two security levels (UNIX permission bits and NTFS security). This directory is exported with Windows NT NTFS security verification on.

In contrast, the NFS server exports the /NetworkStationV2/prodbase alias without checking the Windows NT NTFS security system. This is to support the separation of servers, which makes it possible for a user ID to exist on the authentication server but not on the boot server (where the /NetworkStationV2/prodbase exists). This does not, in anyway, compromise security. The /NetworkStationV2/prodbase directory contains no sensitive files (no user data) and is exported as read-only, so a user cannot overwrite any of the files there. Although the NTFS Access Control Lists (ACLs) are not checked by the NFS server in this directory, the ACLs are still set during installation to control access to these directories by processes on the Windows NT server.

8.9.2 UNIX permission bits

The next level of security involved is the UNIX permission bits in the NFS file system. UNIX systems divide their users into three “groups”:

- **User** or **owner**: This is the user that owns the file or directory.
- **Group**: This is the group (of users) that are associated with the file or directory.
- **Other**: This is, with Windows NT terminology, *everyone* else. This is sometimes also called *world* or *public*.

Each of these groups of users can be given three different access permissions:

- **R** — Read: All users/groups/other that have Read permissions are allowed to read files and list files in directories.
- **W** — Write: All users/groups/other that have Write permissions are allowed to write to files and to create new files and directories.
- **X** — Execute: All users/groups/other that have Execute permissions are allowed to execute scripts or binary executables.

UNIX allows these three different permissions to be set for users/group/other down to individual files and directories, just as Windows NT does.

When NSM is installed on a Windows NT server, the installation program sets these UNIX permission bits on all files it creates. In a regular UNIX system, these permission bits are heavily used, since that is what determines the users' access to files and directories.

The Network Station, however, does *not* use these permission bits for controlling access to files and directories. Instead, it uses the NFS server exports (read-only or read-write) and the Windows NT security (NTFS access control lists). The permission bits you see when doing an `ls -l` command in the Advanced diagnostics shell are not really used for controlling permissions.

Important note

Even though the Network Station does not use the permission bits to control access to files and directories, it *uses* these permission bits to determine which files are executable files and which are not in the /NetworkStationV2/prodbase directory. If these permissions, which are set during NSM installation, are not retained for some reason, the Network Station applications may not work properly.

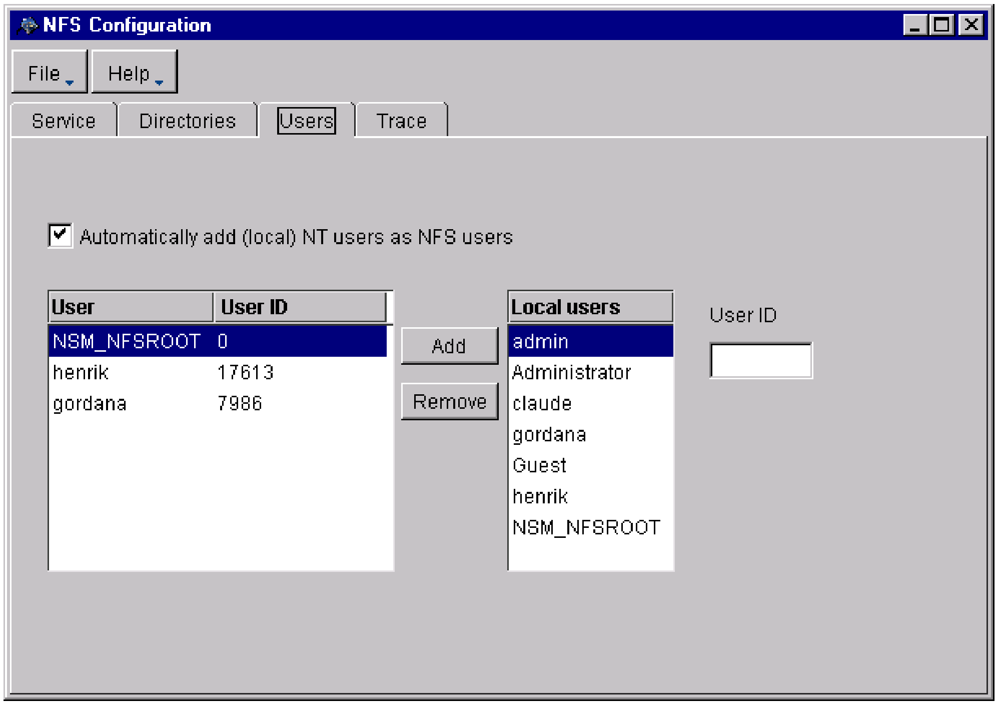
For example, you may decide to simply move /NetworkStationV2/prodbase to another location. You copy the files to the new location using, for example, the Windows NT Explorer or the `xcopy` command in a Windows NT command prompt. In doing so, you bypass the NFS server and the permission bits are then reset to their default values. The default values depend on how the directory is exported by the NFS server (read-only or read-write) and what extension the files have.

If you need to move the files in the /NetworkStationV2/prodbase directory, we strongly recommend that you back up the userbase directory, reinstall NSM specifying where you want it to be, and restore the userbase directory. When doing so, make sure you retain the correct NTFS permissions in the userbase directory as described in 8.9.3, "NTFS security" on page 206.

In the UNIX NFS file system, users are not identified with their user ID and password. Instead, they are identified with a UID and a GID, which correspond to the user ID and the user's group ID. These two are both numerical values.

When a user successfully logs on to the Network Station, the authentication service on the authentication server looks up the user's UID in a database. If it is the first time a user logs on, they are assigned a unique UID. All accesses done by the Network Station are then performed under the authority of the user's UID, according to the NFS standard.

You can see the UID for a user by starting the NFS Server Configuration program. Select **Start->Programs->eNetwork On-Demand Server->NFS Server Configuration** from the Windows NT desktop, as shown in Figure 150.



☑ Automatically add (local) NT users as NFS users

User	User ID
NSM_NFSROOT	0
henrik	17613
gordana	7986

Local users
admin
Administrator
claude
gordana
Guest
henrik
NSM_NFSROOT

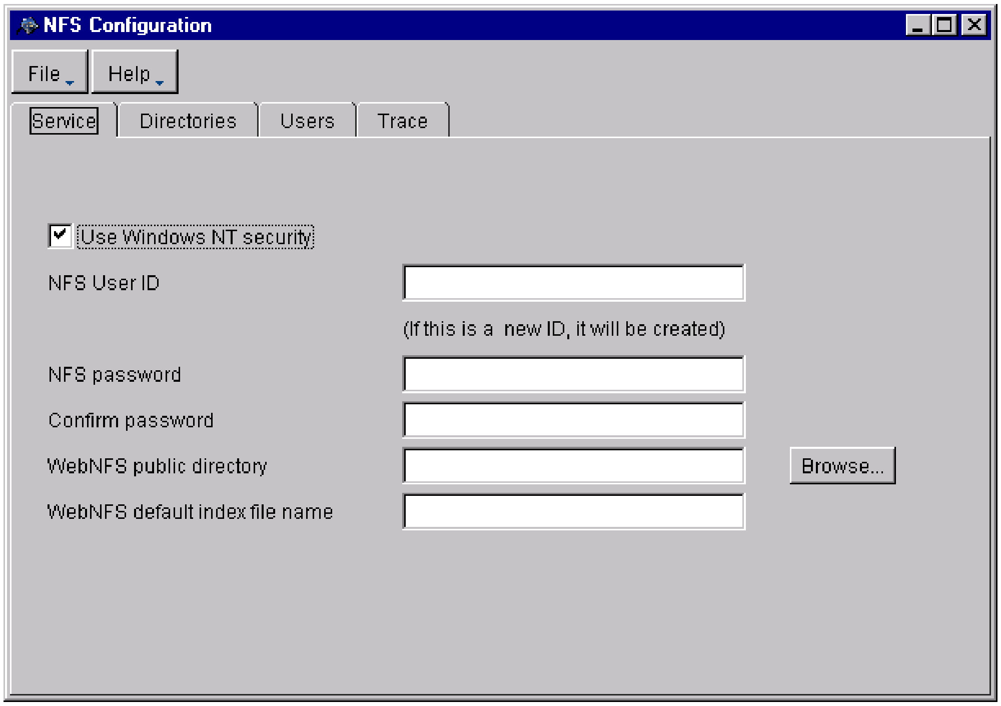
Figure 150. UID for Network Station users

As shown in Figure 150, the users henrik and gordana have logged on to their Network Stations and have both been assigned their unique UIDs. The users to the right are those defined on the server, but all of them have not logged on yet.

8.9.3 NTFS security

The third and last level involved in the security chain is the Windows NT NTFS security itself. Last, but not least, this is a very important level of security and the one with which all Windows NT administrators are familiar.

NTFS security can be used in two ways: either it *is* used or it *is not*. The parameter controlling whether it is used is the Use Windows NT Security check box in the NFS Server Configuration program, as shown in Figure 151.



☑ Use Windows NT security

NFS User ID

(If this is a new ID, it will be created)

NFS password

Confirm password

WebNFS public directory

WebNFS default index file name

Figure 151. NFS Server: Use Windows NT Security

The default is to use Windows NT security for the /NetworkStationV2/userbase directory, but not for the /NetworkStationV2/prodbase directory (which is exported as read-only and does not contain any sensitive files).

When NSM is installed, it creates two local groups, NSMUser and NSMAdmin, on the Windows NT server where it is installed as described earlier in this chapter. It also creates the user account NSM_NFSROOT. This account is made a member of the local NSMUser group.

Note

The NSM_NFSROOT user ID is used by the Network Station to access operating system files and workstation profiles. The user ID is given a program-generated password, which is set to never expire. Should you for any reason want to change this password, you can do so by using the Windows NT User Manager for Domains, just as with any other Windows NT user account.

If the Use Windows NT Security is selected (which is the default), for each and every file request made, the NFS server verifies that the requesting UID corresponds to a valid Windows NT account and that the account is on the NFS server's user list (as shown in Figure 150). If these two criteria are fulfilled, the NFS server tries to access the file using the NT user ID that corresponds to the requesting UID. If either the user or any of the groups to which they belong (NSMUSER or any other) have been given access to the file, the NFS server can successfully access it. The NFS server actually impersonates the user whose user ID it uses to access the file.

If the Use Windows NT Security is *not* selected, the NFS server does not verify that the requesting UID corresponds to a valid Windows NT user. It also bypasses the NTFS access control list. Even though the requesting user does not have access to the file, the NFS server (running as a Windows NT Service) can access the file and return it to the Network Station user who requested it.

This means that if Windows NT security is disabled, one user may be able to change their working directory to another user's home directory and read, write, create, and delete files there.

A note on Windows NT security and performance tuning

If Windows NT security is used, all the frequent lookups (to verify that the requesting UID corresponds to a valid Windows NT account., etc.) use up server CPU cycles and time. Therefore, they are being cached by the NFS server. If you want to fine tune the NFS cache, you can do that as described in 8.8.2, "Performance tuning the NFS server on Windows NT" on page 202.

If your users' home directories do not contain any sensitive data that needs to be protected between the users, for example if you only use the ICA client and an emulator, you can improve performance by completely disabling the use of Windows NT security. Note, however, that anyone can mount the /userbase directory (for example from a UNIX workstation) and read, write, create, and delete files in the user's home directories. They cannot, however, access directories not exported by the NFS server. Also, they cannot write to directories exported as read-only.

It has also been seen in some environments that when the NFS server needs to contact a PDC or BDC it generates a certain amount of network traffic. This is made for each and every file request that is not in the NFS cache. Therefore, if you disable the use of Windows NT security, you may also save some bandwidth, which can be important when working over WAN links.

When NSM is installed, it sets the file and directory permissions shown in Table 33 in the /NetworkStationV2 directory.

Table 33. NTFS permissions set by NSM installation

Directory	NSMUser	<user>	<group>
prodbase (exported as read-only)	RX		
servbase (not exported at all)	RX		
userbase (exported as read-write)	RX		
userbase\profiles	RX		
userbase\profiles\ncs	RX		
userbase\profiles\ncs\<nc-id>.nsm	R		
userbase\profiles\users	RX		
userbase\profiles\users\<user>.nsm		FC	
userbase\profiles\groups	RX		

Directory	NSMUser	<user>	<group>
userbase\profiles\groups\<group>.nsm			R
userbase\home	RX		
userbase\home\<user>		FC	
userbase\nsmshared	RX		
userbase\nsmshared\<user>	RX	FC	
Key: • "R" means read only. • "RX" means read and execute. • "FC" means full control. **Note**: The system, the administrators group, and the NSMAdmin group are given Full Control access to all directories.			

8.10 NSM service tool for Windows NT

As in NSM V1R3, NSM V2R1 also includes a service utility tool that can be used to extract diagnostic information from a Windows NT NSM server. Using this service utility tool, an administrator may easily gather such information as:

- Web server environment variables
- Hard disk information
- Registry settings
- List of running services
- Network port status
- TCP/IP information
- User information
- Network Station binary executables information

The utility can be executed in two ways:

- Locally, on the NSM server itself, by entering the following statement on a command line to direct the output to a file. The output is formatted as HTML and can be viewed in any Web browser.

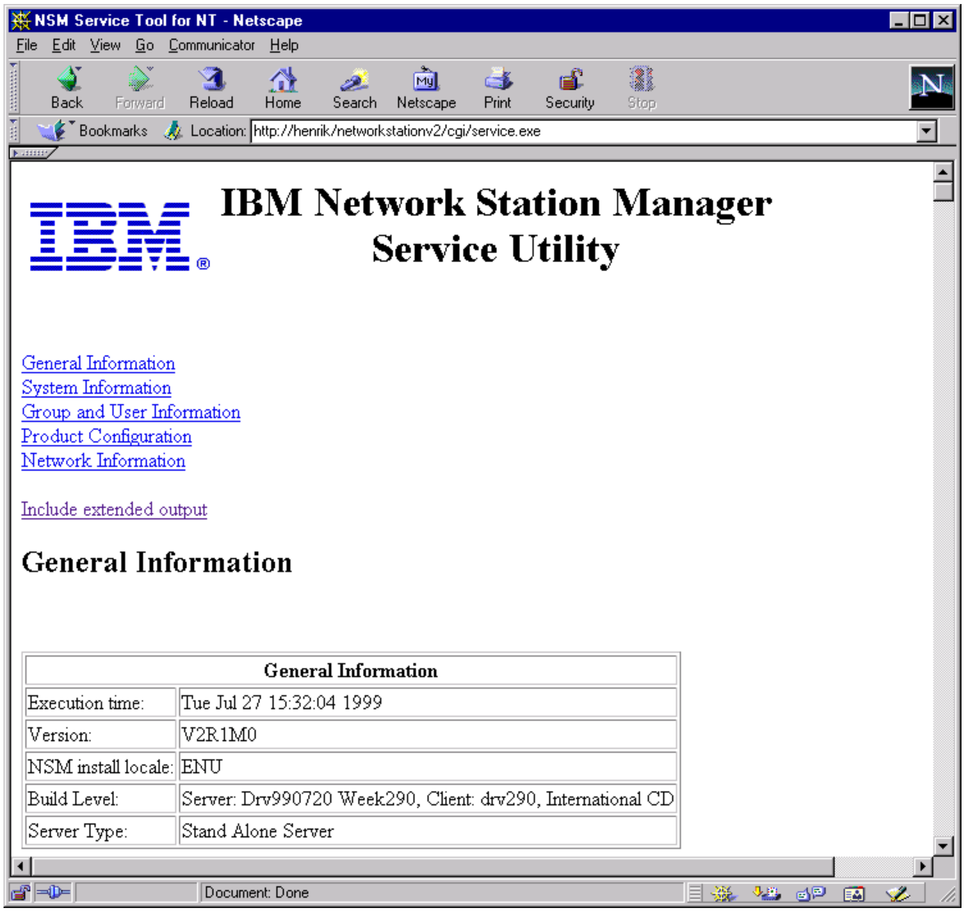
  ```
  \NetworkStationV2\servbase\cgi-bin\service > output_file.html
  ```

- Remotely using a Web browser by accessing the following URL:

  ```
  http://servername/NetworkStationV2/cgi/service
  ```

  If you are not already logged onto NSM, you need to enter an NSM administrator user ID and password.

The output is illustrated in Figure 152 on page 210. Any of the categories can be selected directly to view the relevant information.


NSM Service Tool for NT - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://henrik/networkstationv2/cgi/service.exe
Document: Done

IBM Network Station Manager Service Utility

General Information
System Information
Group and User Information
Product Configuration
Network Information

Include extended output

General Information

General Information	
Execution time:	Tue Jul 27 15:32:04 1999
Version:	V2R1M0
NSM install locale:	ENU
Build Level:	Server: Drv990720 Week290, Client: drv290, International CD
Server Type:	Stand Alone Server

Figure 152. NSM Service tool

Chapter 9. Coexistence of V1R3 and V2R1 IBM NSM

Your server system may already be running a version of the IBM Network Station Manager. the implementation of the new V2R1 IBM Network Station Manager on the same server system can be thought to have three distinct phases:

- Installation
- Coexistence
- Migration

This chapter is designed for those of you who are considering the implementation of the new V2R1 software in your existing environment of Network Stations. With the availability of the IBM Network Station Manager V2R1 software, the announcement came that the software can coexist with the previous version of Network Station Manager. This chapter deals with the coexistence of the V1R3 and V2R1 IBM Network Station Manager software.

Coexistence of both the V1R3 and V2R1 code should be thought as a transition stage until a full migration to the V2R1 code level can take place. The time that your system is in a coexistence phase can be anywhere from a day to an indefinite period of time. There are a number of reasons why a coexistence environment should be maintained. These reasons are covered in the following section.

Three scenarios involving only V1R3 of the IBM Network Station Manager will be introduced in 9.2, “V1R3 scenarios” on page 216. These scenarios will be the basis for all our examples in this chapter. The three scenarios are:

- “Scenario 1: V1R3 clients using NVRAM and BOOTP” on page 224
- “Scenario 2: V1R3 clients using BOOTP only” on page 231
- “Scenario 3: V1R3 clients using DHCP” on page 236

Then in 9.3, “V1R3 and V2R1 scenarios” on page 243, we add the coexistence of V2R1 of the IBM Network Station Manager to the scenarios to the same servers in scenarios 1 through 3. These new scenarios 4 through 6 show that both software levels can physically support various hardware models and can operate and be managed on one server. The scenarios are:

- “Scenario 4: V1R3 and V2R1 clients using NVRAM and BOOTP” on page 251
- “Scenario 5: V1R3 and V2R1 clients using BOOTP only” on page 261
- “Scenario 6: V1R3 and V2R1 clients using DHCP” on page 270

9.1 Determining the length of your coexistence phase

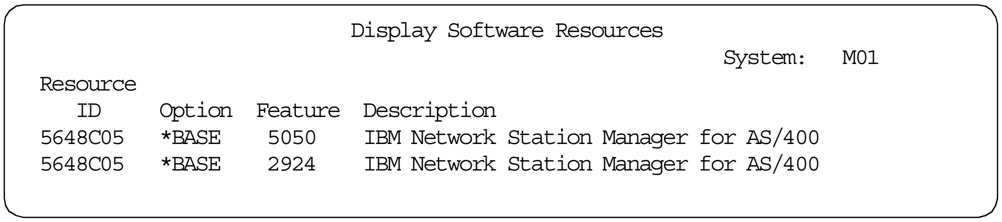
If you already have a IBM Network Station environment established in your business, there are several points to consider before moving to or implementing the V2R1 IBM Network Station Manager code. This chapter only deals with the issue of coexistence. Refer to Chapter 10, “Migration from V1R3 to V2R1 of NSM” on page 283, if you have already decided to migrate your network to a V2R1 level of IBM Network Station Manager.

If you are still not sure if a coexistence environment will be better suited to your situation, continue with this chapter.

The factors to consider before implementing a V2R1 standalone or V2R1/V1R3 coexistence environment on a server are discussed in the following section.

9.1.1 Current level of Network Station Manager installed

To ensure that your system is capable of running a coexistence environment, you need to check the current version of Network Station Manager you are running. On an AS/400 server, you can issue the Display Software Resource (DSPSFWRSC) command. For a coexistence scenario to exist, you *must* have the V1R3 product of Network Station Manager installed. This product is known as 5648C05 on an AS/400 system. The resulting screen for the software resource is shown in Figure 153.



```
                         Display Software Resources
                                                          System:   M01
Resource
   ID      Option  Feature  Description
5648C05    *BASE    5050    IBM Network Station Manager for AS/400
5648C05    *BASE    2924    IBM Network Station Manager for AS/400
```

Figure 153. AS/400 Display Software Resources

If you do not have 5648C05 installed, you may have a previous version of Network Station Manager installed. The products 5733A06 and 5733A07 represent previous IBM Network Station Manager code levels. If either of these levels exist on your system and you need to install the V2R1 code (5648C07) on your system, you must first upgrade your 5733A06 or 5733A07 product to the V1R3 product (5648C05). Table 34 shows the paths of upgrading for the different levels of IBM Network Station Manager.

Table 34. IBM Network Station Manager product upgrade paths

Product	Upgradeable	Coexist with 5648C05	Coexist with 5648C07
5733A06	Yes to 5648C05	No	No
5733A07	Yes to 5648C05	No	No
5648C05	Yes to 5648C07	Not applicable	Yes

For an RS/6000 server, you can see what level of Network Station Manager is installed. At the command prompt, type:

```
lslpp -l
```

9.1.2 Operating system level

Table 35 shows the different levels of the OS/400 operating system and the supported Network Station Manager (NSM) levels. It also shows whether a particular release of OS/400 can support a coexistence environment.

Table 35. OS/400 versions and supported Network Station Manage levels

OS/400 level installed	V1R3 NSM support	V2R1 NSM support	Coexistence of V1R3 and V2R1?
V3R7M0	Yes	No	No

OS/400 level installed	V1R3 NSM support	V2R1 NSM support	Coexistence of V1R3 and V2R1?
V4R1M0	Yes	No	No
V4R2M0	Yes	Yes	Yes
V4R3M0	Yes	Yes	Yes
V4R4M0	Yes	Yes	Yes

From Table 35, we can see that those systems that are currently running either V3R7M0 or V4R1M0 of OS/400 will not be able to run the V2R1 IBM Network Station Manager code. If it is necessary for the system to run the V2R1 code, then you should first consider upgrading your OS/400 release. Upgrading OS/400 is beyond the scope of this book. Information pertaining to upgrades can be found in *AS/400 Software Installation*, SC41-5120. This manual is also available on the Web at: `http://as400bks.rochester.ibm.com`

For the RS/6000 server, the operating system must be at version 4.2.1 or later.

9.1.3 IBM Network Station hardware models

Table 36 shows the available IBM Network Station hardware models and the levels of Network Station Manager (NSM) that are supported.

Table 36. Network Station hardware models and supported levels of NSM

Network Station Model/Interface	V1R3 NSM support only	V1R3 and V2R1 NSM support [1]	V2R1 NSM support only
Model 100/Token Ring and Ethernet	Yes	Yes	No [2]
Model 300/Twinax	Yes	Yes	No [2]
Model 300/Token Ring and Ethernet	Yes	Yes [3] [4] [5]	Yes [3] [4] [5]
Model 1000/Token Ring and Ethernet	Yes	Yes [3] [4] [5]	Yes [3] [4] [5]
Model 2200/Token Ring and Ethernet	No [6]	Yes [3] [4]	Yes
Model 2800/Token Ring and Ethernet	No [6]	Yes [3] [4]	Yes

Network Station Model/Interface	V1R3 NSM support only	V1R3 and V2R1 NSM support [1]	V2R1 NSM support only

Note 1 V1R3 and V2R1 exist on the same server. The particular hardware model may not be supported under both versions but will run on a server with both levels of NSM installed.

Note 2 If your network contains this type of model, you need to maintain the V1R3 level of NSM. This model will *not* operate on a V2R1 NSM only system.

Note 3 The installed memory, on the Network Station model, may be an issue depending on the applications being run and the NSM version on the server system. Refer to the following section.

Note 4 Network considerations should be considered when operating your models on the V2R1 level. Refer to 9.1.7, "Type of network" on page 215.

Note 5 The planned availability date for these models, under the V2R1 NSM level, is November 12, 1999 for the Model 1000 and first quarter of the year 2000 for the Model 300 (excluding the twinaxial model). These dates are published in Software Announcement Letter 299-259, which can be viewed at: `http://www.ibmlink.ibm.com`

Note 6 If your network contains this type of model, you need to install V2R1 level of NSM. This model will *not* operate on a V1R3 NSM only system.

A more detailed review of the different IBM Network Station hardware types is available in Chapter 3, "Planning and design issues and choices" on page 35.

9.1.4 Installed memory

You may now be at the point where you are strongly considering the implementation of the V2R1 code level of IBM Network Station Manager. If one of your reasons is to implement the new hardware models (2200 or 2800), you do not need to concern yourself with this section. However, if you are considering the implementation of either a Model 1000 or 300 (excluding twinaxial attached) IBM Network Station in a V2R1 code environment, continue with this section.

As per the announcement letter for the IBM Network Station Manager V2R1, the following hardware requirements are specified:

- IBM Network Station Manager V2R1
- Any model IBM Network Station (except 8361 models 100, 200 and 341) with at least 32 MB RAM

If you are planning on having your Model 300 or 1000 Network Stations working under the V2R1 code, you have to further analyze what applications they will be running. The memory capabilities of both models are shown in Table 37.

Table 37. Memory capabilities of Network Station Models 300 and 1000

Model	Minimum memory	Maximum memory
Series 300	16 MB	64 MB
Series 1000	32 MB	64 MB

The Model 300 needs to have memory added if it only has the minimum of 16 MB installed. An upgrade to either 32 MB or 64 MB will depend on the applications that are required to run on the Model 300. Likewise, a Model 1000 with a minimum 32 MB installed may be sufficient. Again, consideration must be given to the applications needed to run on the Model 1000.

See Appendix I, “V2R1 memory requirements and network load” on page 643, for more information and instructions on how to retrieve the document *NSM V2R1 - Memory requirements and performance recommendations* from the IBM Network Station home page at:

`http://www.pc.ibm.com/us/networkstation/tech_library.html`

9.1.5 National Language Support (NLS)

The announcement of the V1R3 code of Network Station Manager supplied an extensive list of supported locales. A listing of these locales can be found in *IBM Network Station Manager Installation and Use*, SC41-0664. The announcement of the V2R1 code of IBM Network Station Manager, however, reduced the National Language Support (NLS) to only the following Latin 1 locales:

- English and UK English
- French, Belgian French, Canadian French, and Swiss French
- German, Italian, Swiss German, and Swiss Italian
- Spanish, LA Spanish, Portuguese, and Brazilian Portuguese
- Dutch, Belgian Dutch, Danish, Finnish, and Norwegian

A listing of the locales that are currently not supported in the V2R1 code level can be found in 1.2.9, “NLS and euro support” on page 8.

If your requirement is to use one of these unsupported locales, you should maintain the V1R3 IBM Network Station Manager on your server system. Again, you can choose to install the V2R1 IBM Network Station Manager on your system as long as you have one of the supported Latin 1 locales installed.

9.1.6 Application dependencies

You or a business partner may have created a thin-client application for use in your network including the Network Station Manager at Release 3.0. While most of the features and functions should also work without modification on Version 2 Release 1 of the Network Station Manager, some differences exist. One such difference is that an application written to work with the Navio JVM may not work with the newer 1.1.8 JVM provided as part of the Version 2 Release 1 of the Network Station Manager. At the very least, your coexistence phase should include a period of time for testing.

9.1.7 Type of network

There may be up to a four-fold increase in the LAN traffic to boot a Network Station in NSM V2R1 as compared to NSM V1R3.4. This increased network traffic must be taken into account when planning for the eventual migration to V2R1 of the Network Station Manager.

See Appendix I, “V2R1 memory requirements and network load” on page 643, for more information and instructions on how to retrieve the document *NSM V2R1 - Memory requirements and performance recommendations* from the IBM Network Station home page at:

`http://www.pc.ibm.com/us/networkstation/tech_library.html`

9.1.8 PTF level of the IBM Network Station Manager product

We recommend that you always keep your PTFs current. If you are planning on a coexistence environment, it is a good idea to get to the latest PTF level for the

V1R3 product. To ensure you are at the latest fix level, you can electronically order the Group PTF for the 5648C05 product. From an AS/400 command line, you can issue the command:

```
SNDPTFORD SF99082
```

If the command runs successfully, a CD package will be sent to you. You then need to install this package as you would any other AS/400 PTF package.

9.1.9 Additional features provided in the V2R1 code level

With the announcement of the V2R1 IBM Network Station Manager code new and enhanced features were made available. These features are listed in 1.2, “What’s new in NSM V2R1” on page 3. Whether you are planning to purchase the new models of the IBM Network Station (2200 or 2800), which require you to install the V2R1 code, you may want to install the V2R1 code to take advantage of the new or enhanced features. If this is the case, you need to consider the information in 9.1.1, “Current level of Network Station Manager installed” on page 212, through 9.1.7, “Type of network” on page 215.

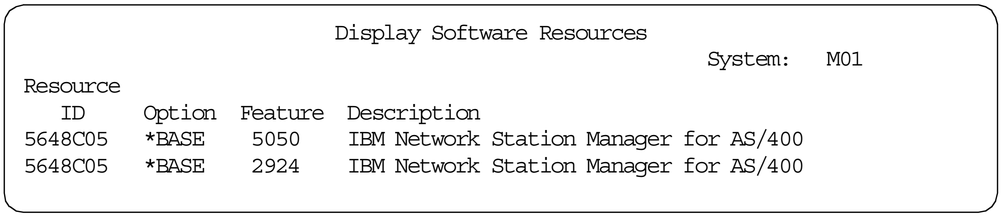
9.2 V1R3 scenarios

Three scenarios involving only the V1R3 IBM Network Station Manager code are presented in this section. We also discuss some common features and functionality of the V1R3 IBM Network Station Manager code as it pertains to an AS/400 server system.

AS/400 information

The V1R3 code is the only IBM Network Station Manager code installed on the AS/400 server system. We briefly explore some portions of the AS/400 system as a review of the elements of the V1R3 Network Station Manager Code.

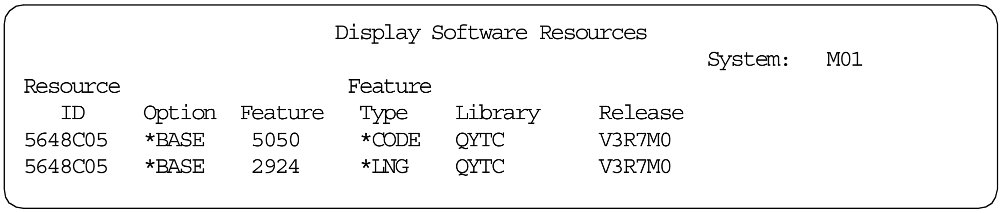
Figure 154 shows a listing of the installed code. The AS/400 command used is the Display Software Resources (DSPSFWRSC).



```
                          Display Software Resources
                                                          System:   M01
Resource
   ID      Option  Feature  Description
5648C05    *BASE    5050    IBM Network Station Manager for AS/400
5648C05    *BASE    2924    IBM Network Station Manager for AS/400
```

Figure 154. AS/400 Display Software Resource screen

Alternatively, pressing the F11 function key, on the screen in Figure 154, shows the libraries and release associated with the 5648C05 product. This is shown in Figure 155.



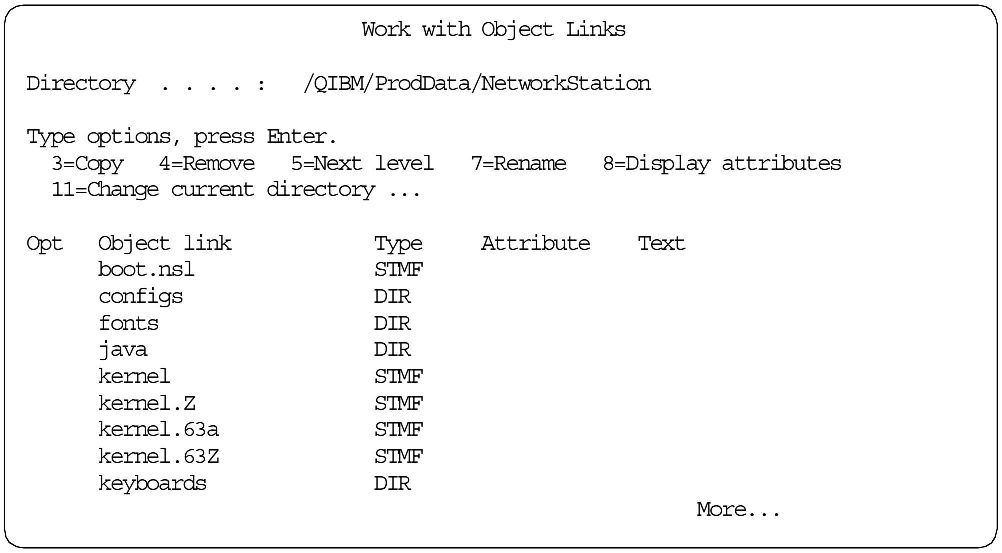
```
                        Display Software Resources
                                                         System:   M01
Resource                 Feature
   ID     Option  Feature  Type    Library    Release
5648C05   *BASE    5050   *CODE   QYTC       V3R7M0
5648C05   *BASE    2924   *LNG    QYTC       V3R7M0
```

Figure 155. AS/400 Display Software Resource screen: 5648C05 product alternate view

Much of the Network Station code is contained within the Integrated File System. This information can be viewed through a 5250 green-screen session or through Operations Navigator. The paths for these directories are:

- QIBM/PRODDATA/NETWORKSTATION
- QIBM/USERDATA/NETWORKSTATION

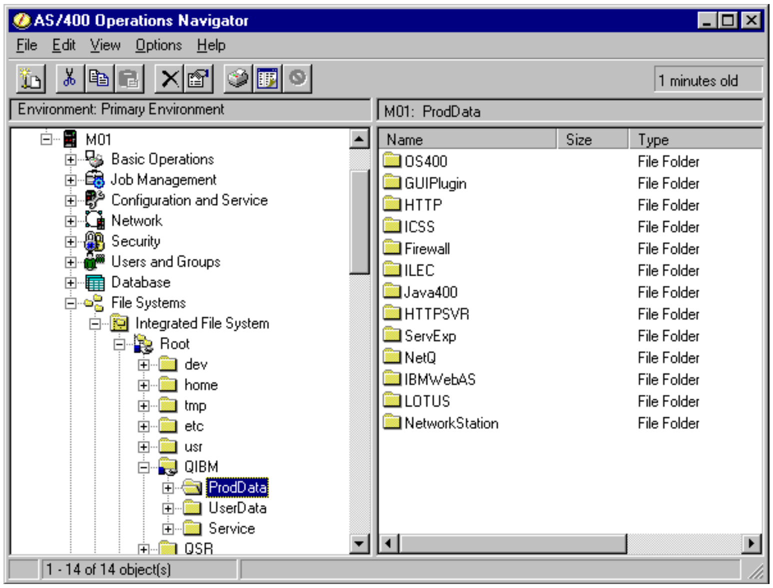
On a 5250 green-screen session, the Work Link (WRKLNK) command is used to navigate through the Integrated File System. Figure 156 shows this AS/400 screen.



```
                          Work with Object Links

Directory  . . . . :   /QIBM/ProdData/NetworkStation

Type options, press Enter.
  3=Copy   4=Remove   5=Next level   7=Rename   8=Display attributes
  11=Change current directory ...

Opt   Object link           Type     Attribute    Text
      boot.nsl              STMF
      configs               DIR
      fonts                 DIR
      java                  DIR
      kernel                STMF
      kernel.Z              STMF
      kernel.63a            STMF
      kernel.63Z            STMF
      keyboards             DIR
                                                         More...
```

Figure 156. AS/400 Work with Object Links screen (V1R3)

If you are using Operations Navigator, a screen similar to the example in Figure 157 on page 218 is shown when viewing the Integrated File System.



Name	Size	Type
OS400		File Folder
GUIPlugin		File Folder
HTTP		File Folder
ICSS		File Folder
Firewall		File Folder
ILEC		File Folder
Java400		File Folder
HTTPSVR		File Folder
ServExp		File Folder
NetQ		File Folder
IBMWebAS		File Folder
LOTUS		File Folder
NetworkStation		File Folder

Figure 157. AS/400 Operations Navigator: Viewing the Integrated File System

Other important parts of the Network Station code are the HTTP server directives. There are two server directives that are used with the V1R3 Network Station Manager code. These server directives can be viewed with a 5250 session. To see these directives, issue the following AS/400 command:

```
WRKHTTPCFG
```

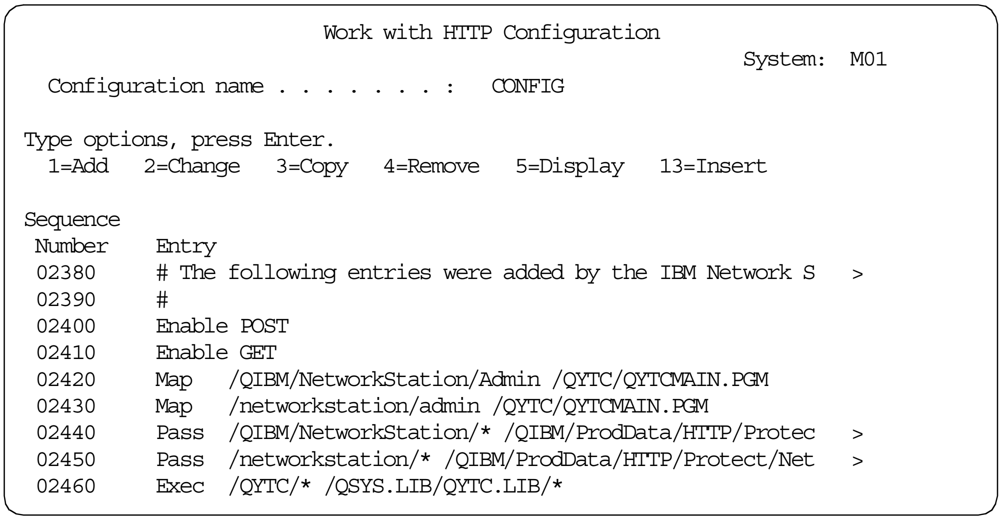
or

```
WRKHTTPCFG *ADMIN
```

The resulting screens are shown in Figure 158 and Figure 159. The instances show lines that were added when the System Administrator ran the AS/400 Setup Assistant. This Setup Assistant is part of the V1R3 IBM Network Station Manager code. The Setup Assistant is used initially when the V1R3 code is installed on the server system.

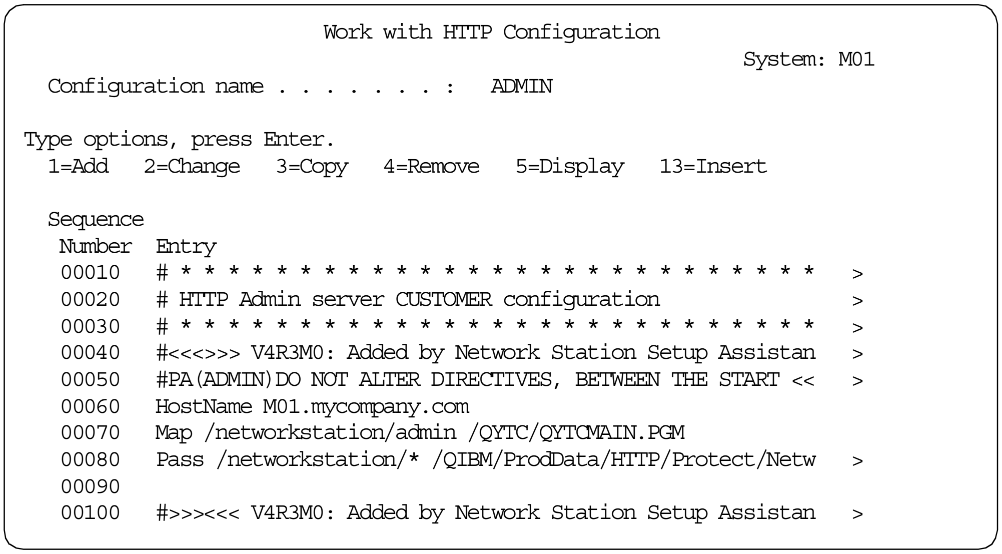
Tip

The operation of the AS/400 Setup Assistant is beyond the scope of this redbook. If further information is required, refer to *IBM Network Station Manager Installation and Use,* SC41-0664.



```
                          Work with HTTP Configuration
                                                                System:  M01
  Configuration name . . . . . . . :   CONFIG

Type options, press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display   13=Insert

Sequence
 Number    Entry
 02380     # The following entries were added by the IBM Network S   >
 02390     #
 02400     Enable POST
 02410     Enable GET
 02420     Map   /QIBM/NetworkStation/Admin /QYTC/QYTCMAIN.PGM
 02430     Map   /networkstation/admin /QYTC/QYTCMAIN.PGM
 02440     Pass  /QIBM/NetworkStation/* /QIBM/ProdData/HTTP/Protec   >
 02450     Pass  /networkstation/* /QIBM/ProdData/HTTP/Protect/Net   >
 02460     Exec  /QYTC/* /QSYS.LIB/QYTC.LIB/*
```

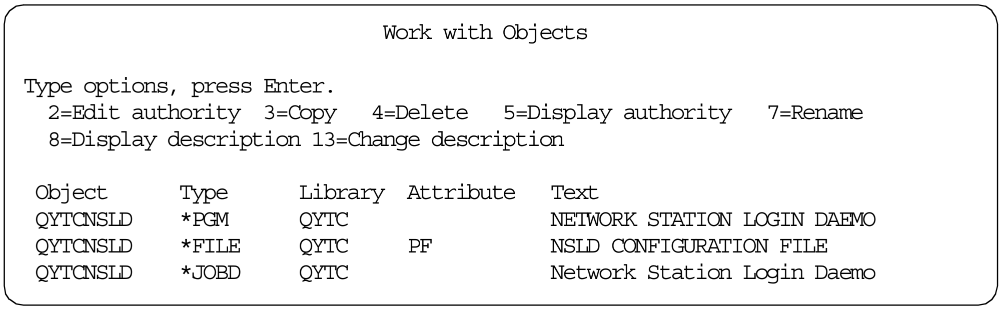
Figure 158. AS/400 Work with HTTP Configuration screen: Default instance



```
                          Work with HTTP Configuration
                                                                System: M01
  Configuration name . . . . . . . :   ADMIN

Type options, press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display   13=Insert

  Sequence
   Number  Entry
   00010   # * * * * * * * * * * * * * * * * * * * * * * * * * * *   >
   00020   # HTTP Admin server CUSTOMER configuration                 >
   00030   # * * * * * * * * * * * * * * * * * * * * * * * * * * *   >
   00040   #<<<>>> V4R3M0: Added by Network Station Setup Assistan   >
   00050   #PA(ADMIN)DO NOT ALTER DIRECTIVES, BETWEEN THE START <<   >
   00060   HostName M01.mycompany.com
   00070   Map /networkstation/admin /QYTC/QYTCMAIN.PGM
   00080   Pass /networkstation/* /QIBM/ProdData/HTTP/Protect/Netw   >
   00090
   00100   #>>><<< V4R3M0: Added by Network Station Setup Assistan   >
```

Figure 159. AS/400 Work with HTTP Configuration screen: Admin instance

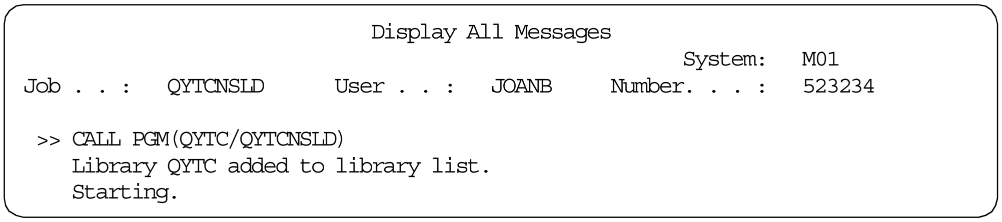
The Network Station Login Server job runs in the subsystem QSYSWRK. The job itself is called QYTCNSLD. In the V1R3 level of Network Station Manager, these program objects reside in the QYTC library. We show later that in the V2R1code, the Login Server objects are maintained in a different library on the AS/400 system. Figure 160 on page 220 shows the `WRKOBJ OBJ(*ALL/QYTCNSLD)` command.



```
                            Work with Objects

Type options, press Enter.
  2=Edit authority  3=Copy   4=Delete   5=Display authority   7=Rename
  8=Display description 13=Change description

 Object      Type      Library  Attribute   Text
 QYTCNSLD    *PGM      QYTC                 NETWORK STATION LOGIN DAEMO
 QYTCNSLD    *FILE     QYTC     PF          NSLD CONFIGURATION FILE
 QYTCNSLD    *JOBD     QYTC                 Network Station Login Daemo
```

Figure 160. AS/400 Work with Object screen

The job log for QYTCNSLD with the `WRKJOB QTYCNSLD` command shows the information that appears in Figure 161.



```
                           Display All Messages
                                                        System:   M01
Job . . :   QYTCNSLD      User . . :   JOANB     Number. . . :   523234

 >> CALL PGM(QYTC/QYTCNSLD)
    Library QYTC added to library list.
    Starting.
```

Figure 161. AS/400 job log for QYTCNSLD in the QYTC library

Network Station connectivity: AS/400 servers required

For the IBM Network Station clients, in the following scenarios, to successfully log on to the AS/400 server, certain TCP/IP servers must be started. Specifically the TFTP server must always be started. This server can be started with the AS/400 Start TCP/IP Server (`STRTCPSVR *TFTP`) command. This server is required whether the client is using the NVRAM, BOOTP, or DHCP method of booting.

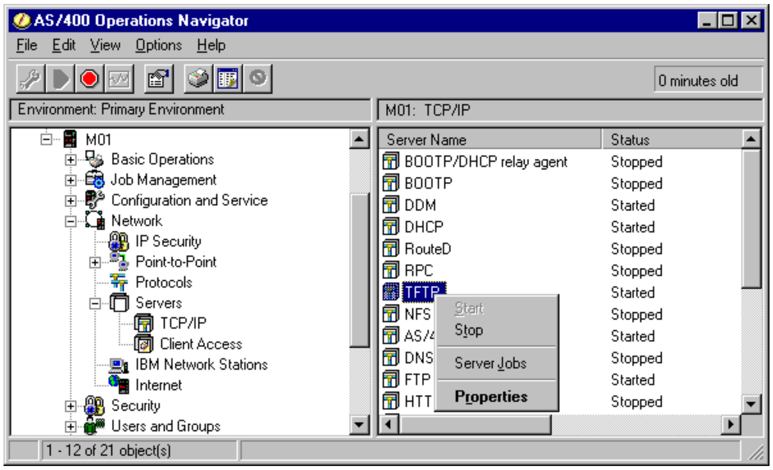
For the BOOTP clients, the BOOTP server must also be started. The AS/400 command to start this server is:

```
STRTCPSVR *BOOTP
```

For the DHCP clients, the DHCP server must be started in addition to the TFTP server. The AS/400 command to start this server is:

```
STRTCPSVR *DHCP
```

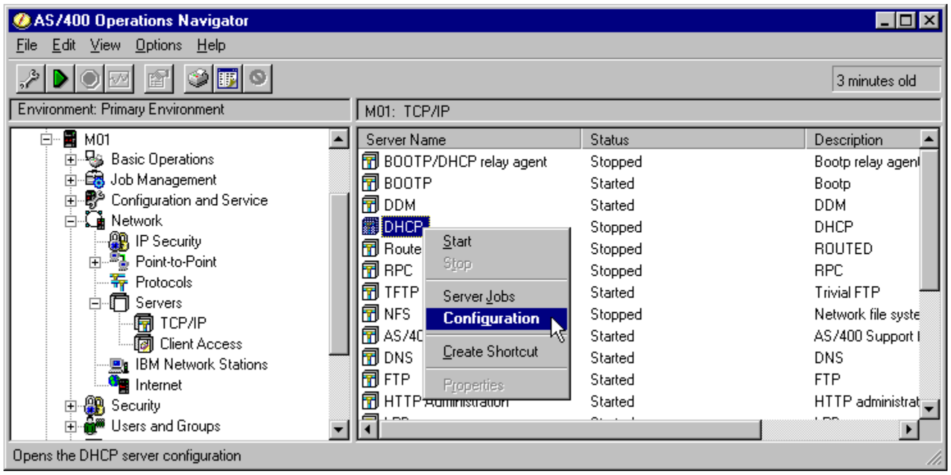
If there is a need to have these servers active after every IPL, they can be set to always autostart after an IPL of the system. You can modify the autostart parameter of the TCP/IP servers with a 5250 session or with Operations Navigator. With a 5250 session, issue the `CFGTCP` command. Then, select option **20**, Configure TCP/IP applications. Alternatively you can use Operations Navigator. Within the Operations Navigator screen, double-click **Network->Servers->TCP/IP**. At this point, a list of the servers should be presented in the right-hand side. The autostart parameter is shown within the properties for the TFTP and BOOTP. Right-click on the server of your choice. An example of this type of screen is shown in Figure 162.



Server Name	Status
BOOTP/DHCP relay agent	Stopped
BOOTP	Stopped
DDM	Started
DHCP	Started
RouteD	Stopped
RPC	Stopped
TFTP	Started
NFS	Stopped
AS/4	Started
DNS	Stopped
FTP	Started
HTT	Stopped

Figure 162. AS/400 Operations Navigator: TCP/IP servers

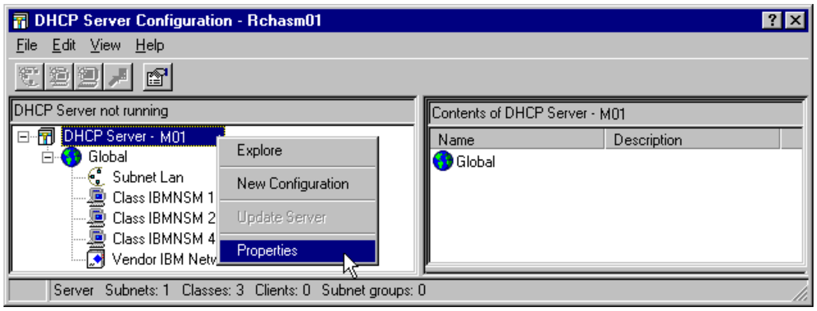
For the DHCP server, right-click the server, and then select **Configuration** as shown in Figure 163.



Server Name	Status	Description
BOOTP/DHCP relay agent	Stopped	Bootp relay agent
BOOTP	Started	Bootp
DDM	Started	DDM
DHCP	Stopped	DHCP
Route	Stopped	ROUTED
RPC	Stopped	RPC
TFTP	Started	Trivial FTP
NFS	Stopped	Network file syste
AS/40	Started	AS/400 Support I
DNS	Started	DNS
FTP	Started	FTP
HTTP Administration	Started	HTTP administrat

Figure 163. AS/400 Operations Navigator: DHCP server

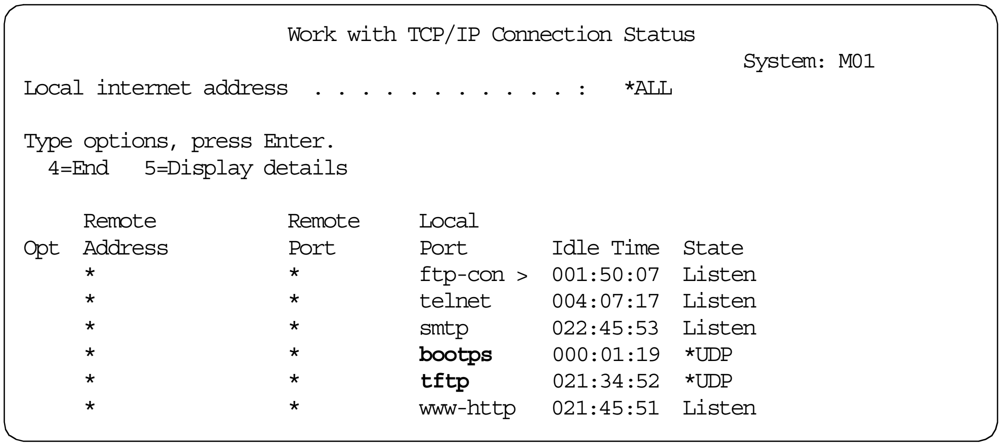
Once the DHCP configuration has been presented, right-click the **DHCP Server** and select **Properties**. Once in Properties you can set the autostart parameter. The DHCP configuration display is shown in Figure 164.



Name	Description
Global	

Figure 164. AS/400 Operations Navigator: DHCP server properties

Once you start these servers, either through a 5250 session or Operations Navigator, you can check to see that the servers are active. Figure 165 shows the output of the AS/400 command `NETSTAT *CNN`.



```
                       Work with TCP/IP Connection Status
                                                           System: M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          ftp-con >  001:50:07  Listen
     *                *          telnet     004:07:17  Listen
     *                *          smtp       022:45:53  Listen
     *                *          bootps     000:01:19  *UDP
     *                *          tftp       021:34:52  *UDP
     *                *          www-http   021:45:51  Listen
```

*Figure 165. AS/400 NETSTAT *CNN screen showing BOOTP and TFTP servers*

Alternatively, you can also check the status of these servers through Operations Navigator. Refer to Figure 163 on page 221 for a view of these servers and their status.

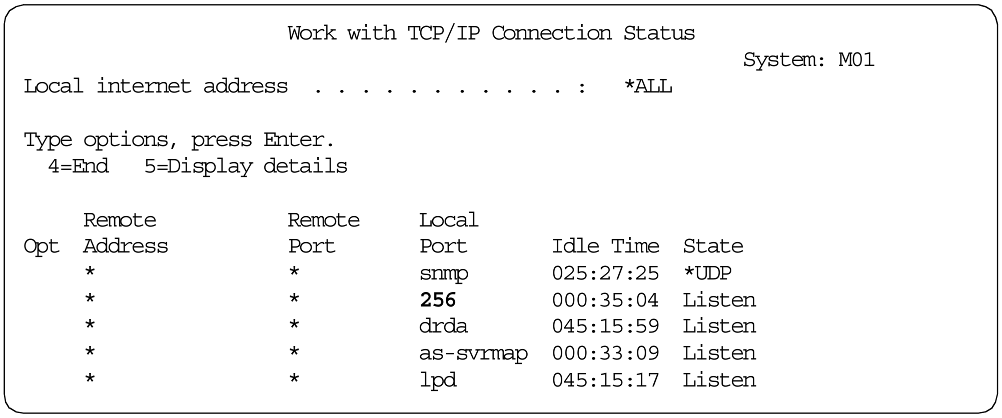
Lastly, the Network Station login server must also be running on your AS/400 system. This server allows your Network Station Users to log onto the AS/400 system. The command to start this server is:

```
CALL QYTC/QYTCUSVR ('STRTCPSVR ')
```

To show that the server is active, issue the following command from an AS/400 command line:

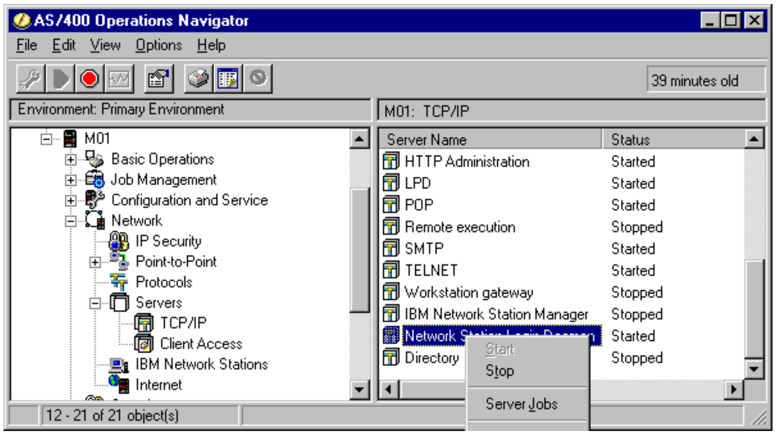
```
NETSTAT *CNN
```

The server uses port 256. Alternatively, you can also view and start this server in Operations Manager. Figure 166 shows the 5250 screen output and Figure 167 shows the Operations Navigator view.



```
                       Work with TCP/IP Connection Status
                                                           System: M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          snmp       025:27:25  *UDP
     *                *          256        000:35:04  Listen
     *                *          drda       045:15:59  Listen
     *                *          as-svrmap  000:33:09  Listen
     *                *          lpd        045:15:17  Listen
```

*Figure 166. AS/400 NETSTAT *CNN screen showing port 256*



Server Name	Status
HTTP Administration	Started
LPD	Started
POP	Started
Remote execution	Stopped
SMTP	Started
TELNET	Started
Workstation gateway	Stopped
IBM Network Station Manager	Stopped
Network Station Login Daemon	Started
Directory	Stopped

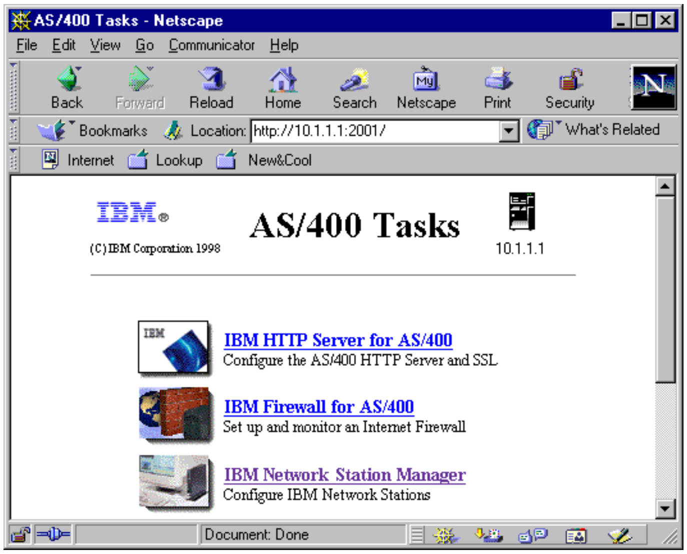
Figure 167. AS/400 Operations Navigator: Network Station login server

Managing the Network Station clients

The IBM Network Station Manager program is a browser-based application. This program allows the administrator to perform the setup and management tasks associated with the IBM Network Station Clients.

In the V1R3 Code of the IBM Network Station Manager, you can access the Manager Program with one of the following URLs:

- `http://serverIPaddress:2001` (Figure 171)
- `http://serverIPaddress/networkstation/admin`



AS/400 Tasks

IBM HTTP Server for AS/400
Configure the AS/400 HTTP Server and SSL

IBM Firewall for AS/400
Set up and monitor an Internet Firewall

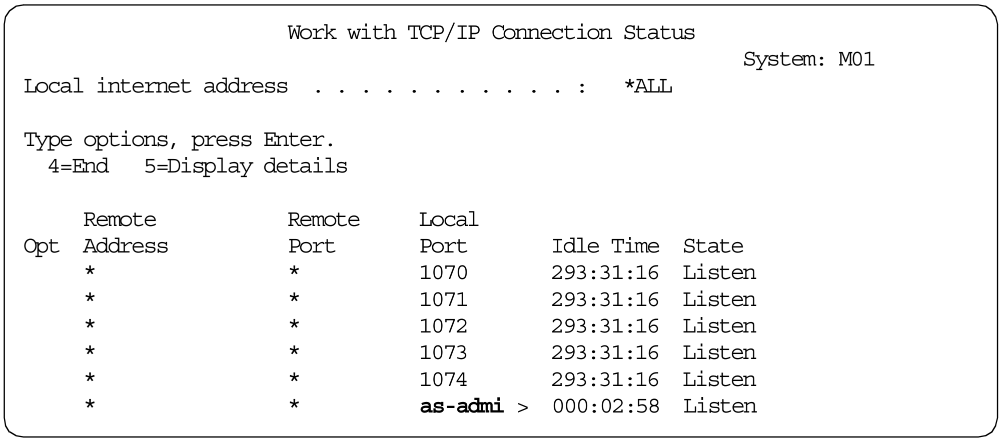
IBM Network Station Manager
Configure IBM Network Stations

Figure 168. AS/400 Tasks display

To successfully receive this display, you need to ensure that the ADMIN server is running on your AS/400 system. You can check this with the AS/400 command:

```
NETSTAT *CNN.
```

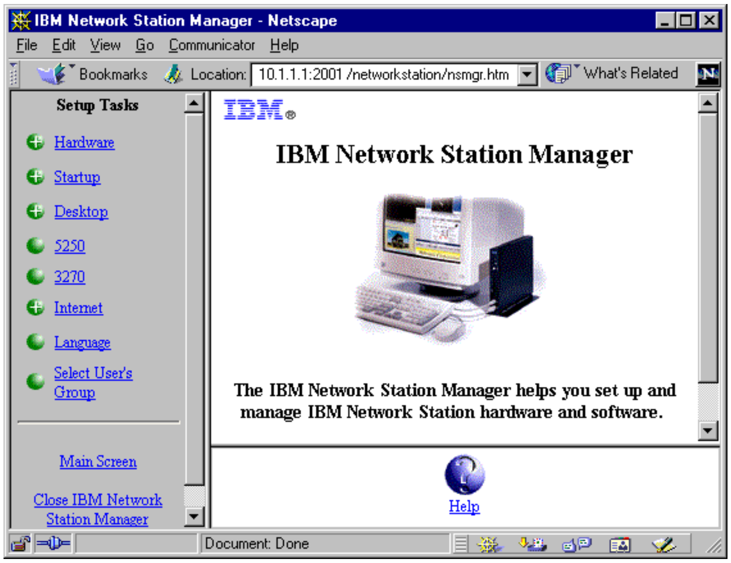
The server runs on port 2001. The resulting screen is shown in Figure 169 on page 224.



```
                      Work with TCP/IP Connection Status
                                                          System: M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          1070       293:31:16  Listen
     *                *          1071       293:31:16  Listen
     *                *          1072       293:31:16  Listen
     *                *          1073       293:31:16  Listen
     *                *          1074       293:31:16  Listen
     *                *          as-admi >  000:02:58  Listen
```

*Figure 169. AS/400 NETSTAT *CNN screen showing Admin port*

Once you receive the AS/400 tasks screen, on your browser, click the IBM Network Station Manager. A Sign In panel is presented, and then the main panel is shown (Figure 170).



IBM Network Station Manager

The IBM Network Station Manager helps you set up and manage IBM Network Station hardware and software.

IBM Network Station Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: 10.1.1.1:2001 /networkstation/nsmgr.htm
What's Related
Setup Tasks
Hardware
Startup
Desktop
5250
3270
Internet
Language
Select User's Group
Main Screen
Close IBM Network Station Manager
IBM
Help
Document: Done

Figure 170. IBM Network Station Manager main panel

The three Network Station clients, in the scenarios, are USER1, USER2, and USER3. Using the manager, two 5250 autostart sessions are configured for USER2 and USER3. One 5250 session starts a session for system M01 and the other starts a session for system M15. USER1 also has two 5250 autostart sessions, both for the M01 system.

More detailed information about using the IBM Network Station Manager can be found in *IBM Network Station Manager Installation and Use*, SC41-0664.

9.2.1 Scenario 1: V1R3 clients using NVRAM and BOOTP

This particular scenario shows a simple AS/400 environment with three Network Stations. Both LAN attached and twinaxial attached Network Stations are used.

The only Network Station Manager code running on the AS/400 system is the V1R3 level.

9.2.1.1 Scenario overview

This scenario shows an AS/400 system (M01) running V4R3M0 of OS/400. The AS/400 system supports one of each of the following models of Network Station:

- **Network Station Series 100:** Token-Ring attached
- **Network Station Series 300:** Twinaxial attached
- **Network Station Series 1000:** Token-Ring attached

Because these hardware models are supported under the V1R3 Network Station Manager code, this code level will be the only installed on the AS/400 system.

9.2.1.2 Scenario network configuration

Figure 171 shows the network topology of the AS/400 systems and the attached Network Station clients. An internal LAN exists for the Token-Ring attached Network Station models, and a different network addressing scheme is used for the twinaxial subnet.

Tip

For more information about attaching twinaxial Network Stations to an AS/400 system, consult *AS/400 IBM Network Station: Techniques for Deployment in a WAN*, SG24-5187.

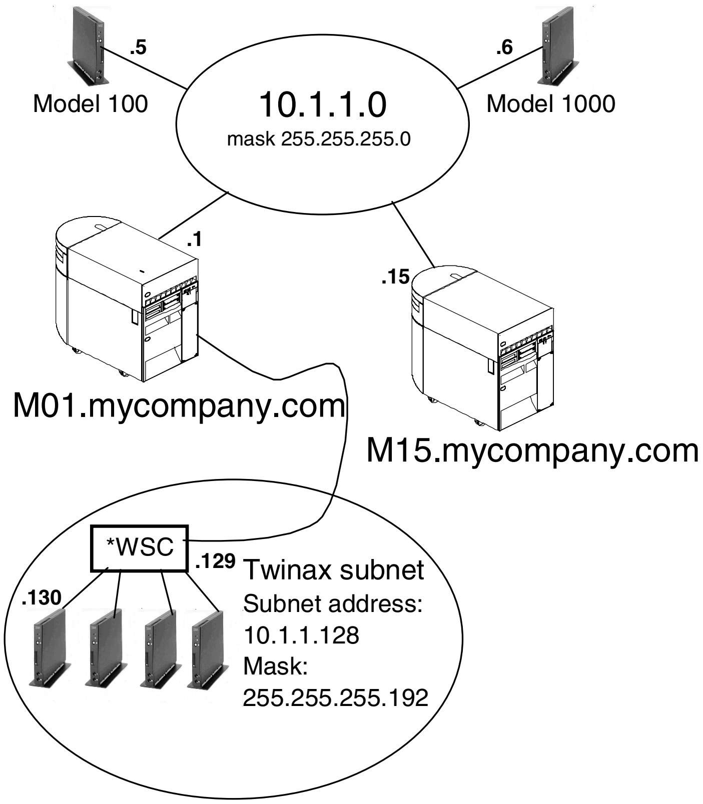
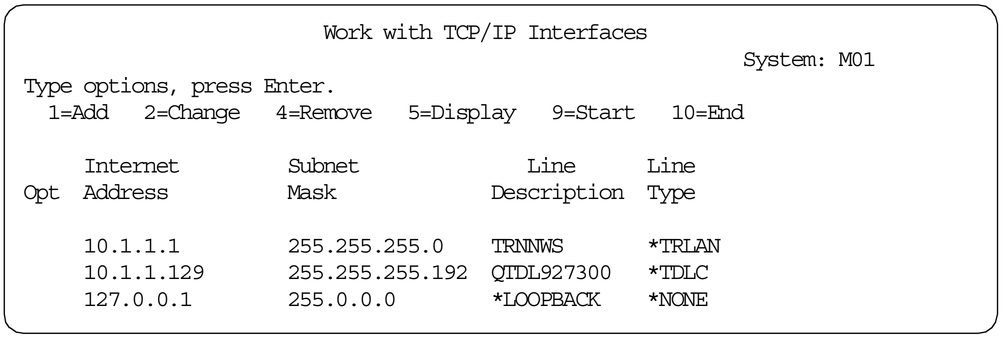


Figure 171. TCP/IP network topology for scenario 1 and scenario 2

The IP interfaces defined for this scenario are shown in Figure 172. The twinaxial network is a subnet of the main network 10.1.1.0.



```
                           Work with TCP/IP Interfaces
                                                               System: M01
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet            Line        Line
Opt  Address          Mask              Description Type

     10.1.1.1         255.255.255.0     TRNNWS      *TRLAN
     10.1.1.129       255.255.255.192   QTDL927300  *TDLC
     127.0.0.1        255.0.0.0         *LOOPBACK   *NONE
```

Figure 172. AS/400 Work with TCP/IP Interfaces screen

The twinaxial subnet range is from 10.1.1.128 to 10.1.1.191. This gives the subnet 61 available IP addresses.

Attention

During the testing and verification of this scenario, a problem with BOOTP was encountered when the twinaxial subnet was configured in the range of 10.1.1.192 to 10.1.1.255. Since this range is part of the main 10.1.1.0 network, transparent subnet masking is used. The range included the 10.1.1.0 network broadcast address (10.1.1.255), which is where a problem was discovered. At this time, we recommend that you *do not* configure a transparent subnet that would include the network broadcast address. For our scenarios, we chose a twinaxial subnet of 10.1.1.129.

Further information on this problem can be found in Informational APAR II12070. You can order this information with the following AS/400 command:

```
SNDPTFORD II12070
```

9.2.1.3 Network Station configuration

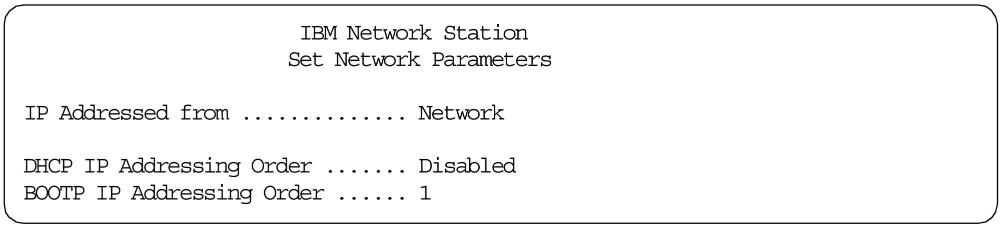
There are three IBM Network Stations used in this scenario. The Model 1000 and Model 100 use the BOOTP method for obtaining their IP address. The Model 341 uses its NVRAM setting to obtain an IP address. Further information about the different methods of obtaining an IP address can be found in 2.3.2, “Obtaining an IP address” on page 21.

Table 38 shows some of the IBM Network Station hardware specifications. The models shown are the ones that are being used in this scenario.

Table 38. IBM Network Station specifications

Network Station Model	Boot monitor version	Total DRAM memory	IP address
100	v3.0.7.6	16 MB	10.1.1.5
341 - Twinax	v3.0.7.2	32 MB	10.1.1.130
1000	v3.0.8.8	64 MB	10.1.1.6

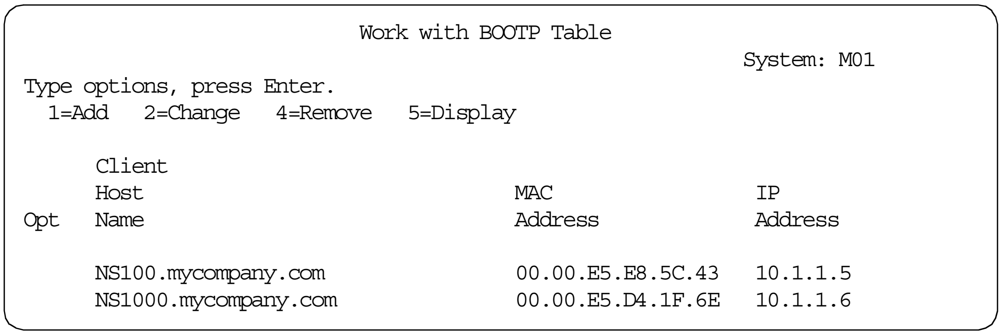
The configuration for the Model 100 and the Model 1000 are contained both on the Network Station and on the AS/400 system. The only configuration needed on the Network Station itself is in the Network Parameters. An example of this screen in shown in Figure 173.



```
                        IBM Network Station
                       Set Network Parameters

IP Addressed from ............. Network

DHCP IP Addressing Order ....... Disabled
BOOTP IP Addressing Order ...... 1
```

Figure 173. IBM Network Station: Network parameters for Models 100 and 1000

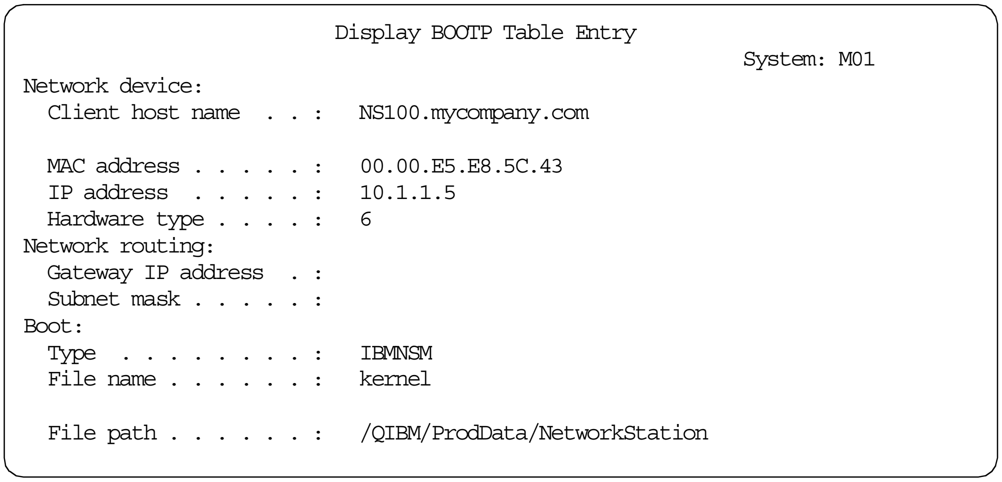
The remaining configuration screens on the Network Station do not need to be set. However, on the AS/400 system, you need to ensure that a BOOTP table entry exists for each Network Station. Figure 174 shows the output of the Work with BOOTP Table (WRKBPTBL) command on the AS/400 system.



```
                             Work with BOOTP Table
                                                            System: M01
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

      Client
      Host                               MAC                IP
Opt   Name                               Address            Address

      NS100.mycompany.com                00.00.E5.E8.5C.43  10.1.1.5
      NS1000.mycompany.com               00.00.E5.D4.1F.6E  10.1.1.6
```

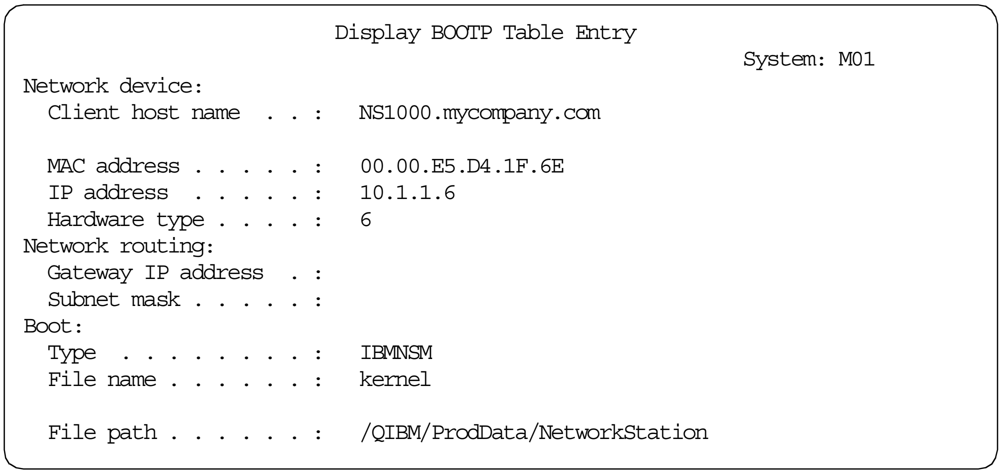
Figure 174. AS/400 Work with BOOTP Table entries screen

When option 5 is entered next to each client entry, the information appears as shown in Figure 175 and Figure 176 on page 228.



```
                           Display BOOTP Table Entry
                                                            System: M01
Network device:
  Client host name  . . :   NS100.mycompany.com

  MAC address . . . . . :   00.00.E5.E8.5C.43
  IP address  . . . . . :   10.1.1.5
  Hardware type . . . . :   6
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . . . . :   IBMNSM
  File name . . . . . . :   kernel

  File path . . . . . . :   /QIBM/ProdData/NetworkStation
```

Figure 175. AS/400 BOOTP Table Entry for Model 100 Network Station

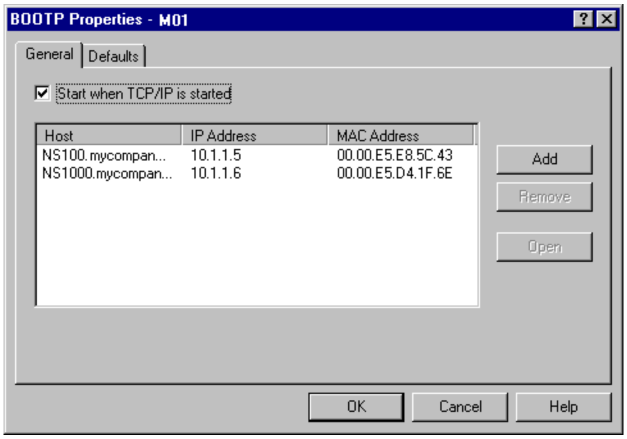


```
                              Display BOOTP Table Entry
                                                                   System: M01
Network device:
  Client host name  . . :   NS1000.mycompany.com

  MAC address . . . . . :   00.00.E5.D4.1F.6E
  IP address  . . . . . :   10.1.1.6
  Hardware type . . . . :   6
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . . . . :   IBMNSM
  File name . . . . . . :   kernel

  File path . . . . . . :   /QIBM/ProdData/NetworkStation
```

Figure 176. AS/400 BOOTP Table Entry for Model 1000 Network Station

These BOOTP entries can also be added or viewed in Operations Navigator. To do this, double-click **Network->Servers->TCP/IP**.

A list of servers appears in the right-hand side of the window. Left-click the **BOOTP** entry, and a pull-down menu appears. Right-click **Properties**. A window similar to the one shown in Figure 177 appears.



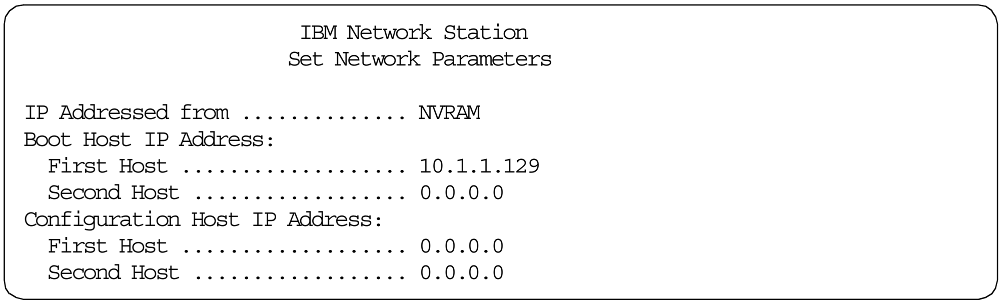
BOOTP Properties - M01

☑ Start when TCP/IP is started

Host	IP Address	MAC Address
NS100.mycompan...	10.1.1.5	00.00.E5.E8.5C.43
NS1000.mycompan...	10.1.1.6	00.00.E5.D4.1F.6E

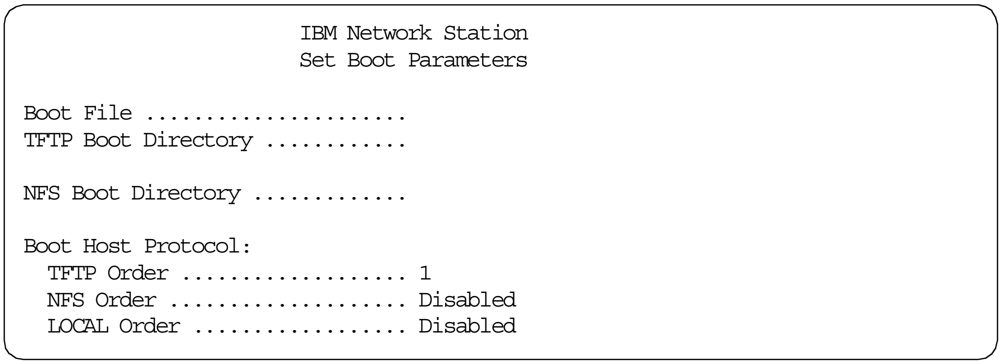
Figure 177. AS/400 Operations Navigator: BOOTP properties1

The configuration for Model 341 is contained in the NVRAM settings of the Network Station itself. There are minimal settings needed for Model 341 as shown in Figure 178 through Figure 180.



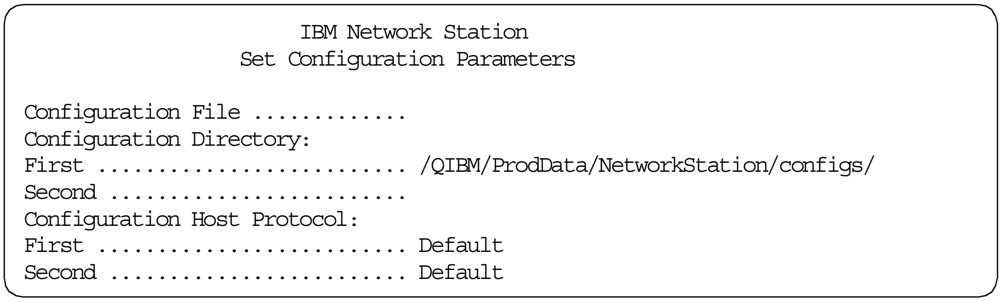
```
                         IBM Network Station
                       Set Network Parameters

IP Addressed from ............. NVRAM
Boot Host IP Address:
  First Host .................. 10.1.1.129
  Second Host ................. 0.0.0.0
Configuration Host IP Address:
  First Host .................. 0.0.0.0
  Second Host ................. 0.0.0.0
```

Figure 178. IBM Network Station: Network parameters for Model 341



```
                         IBM Network Station
                        Set Boot Parameters

Boot File .....................
TFTP Boot Directory ...........

NFS Boot Directory ............

Boot Host Protocol:
  TFTP Order .................. 1
  NFS Order ................... Disabled
  LOCAL Order ................. Disabled
```

Figure 179. IBM Network Station: Boot parameters for Model 341



```
                         IBM Network Station
                    Set Configuration Parameters

Configuration File ............
Configuration Directory:
First ......................... /QIBM/ProdData/NetworkStation/configs/
Second ........................
Configuration Host Protocol:
First ......................... Default
Second ........................ Default
```

Figure 180. IBM Network Station: Configuration parameters for Model 341

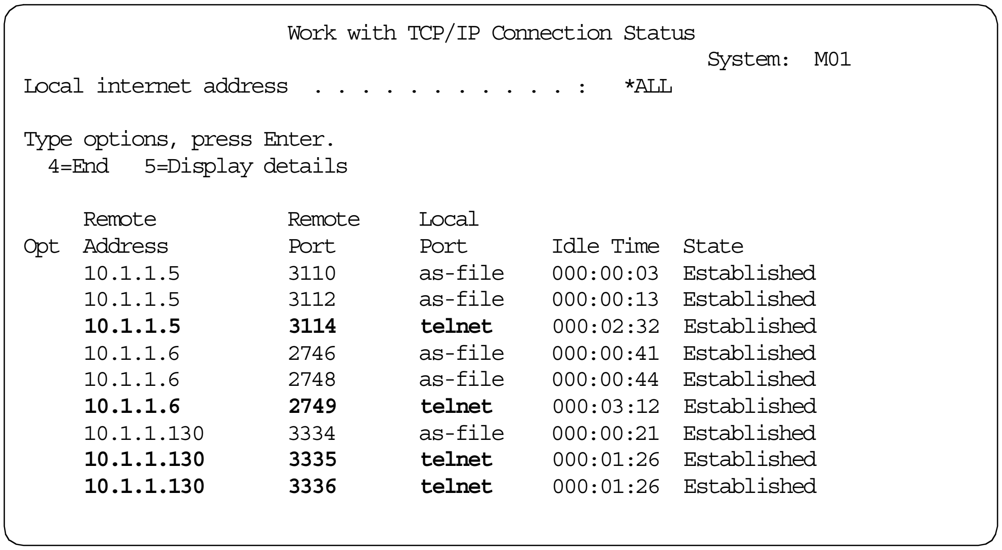
9.2.1.4 AS/400 requirements

In this scenario, it is necessary to have the TFTP and BOOTP servers started on the AS/400 server. After the boot-up process completes, a sign-on screen is present on all three client Network Stations. For each client user to sign on successfully, the Network Station Login Server needs to be started on port 256.

There are autostart 5250 sessions configured within the Network Station Manager. When the authentication of each user was completed, the appropriate 5250 sessions were autostarted on each client Network Station.

9.2.1.5 Connectivity verification

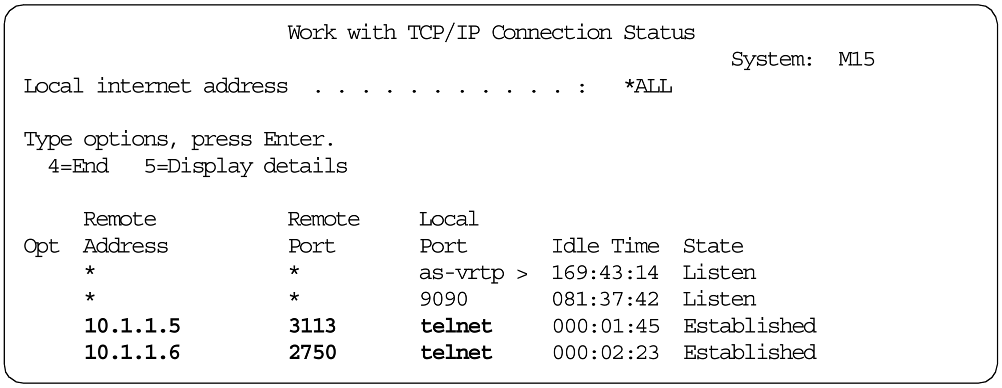
All three clients in this scenario have autostart 5250 sessions configured for the M01 system. To verify that these sessions are started, you can review the TCP/IP connection status screen, on the M01 system, by using the `NETSTAT *CNN` command. Figure 181 on page 230 shows that the 10.1.1.130 (twinaxial client) has two established sessions and the LAN clients have one each. This validates the configuration done for USER1, USER2, and USER3 in the Network Station Manager.



```
                      Work with TCP/IP Connection Status
                                                           System:  M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.5         3110       as-file    000:00:03  Established
     10.1.1.5         3112       as-file    000:00:13  Established
     10.1.1.5         3114       telnet     000:02:32  Established
     10.1.1.6         2746       as-file    000:00:41  Established
     10.1.1.6         2748       as-file    000:00:44  Established
     10.1.1.6         2749       telnet     000:03:12  Established
     10.1.1.130       3334       as-file    000:00:21  Established
     10.1.1.130       3335       telnet     000:01:26  Established
     10.1.1.130       3336       telnet     000:01:26  Established
```

Figure 181. AS/400 TCP/IP connections: M01 system verification

Alternatively, USER2 and USER3 also have an autostart session for the M15 system. On the M15 system, the `NETSTAT *CNN` is issued on a command line. The resulting screen is shown in Figure 182.



```
                      Work with TCP/IP Connection Status
                                                             System:  M15
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          as-vrtp >  169:43:14  Listen
     *                *          9090       081:37:42  Listen
     10.1.1.5         3113       telnet     000:01:45  Established
     10.1.1.6         2750       telnet     000:02:23  Established
```

Figure 182. AS/400 TCP/IP connections: M15 system verification

9.2.1.6 Summary

This scenario shows a network of two AS/400 systems and three IBM Network Station clients. One of the AS/400 systems (M01) is a boot server, which is set up to supply IP addresses to the IBM Network Station clients. The level of the IBM Network Station Manager is V1R3. Different parts of the IBM Network Station Manager code are discussed as they relate to the V1R3 version.

Different boot methods are used among the IBM Network Station clients, and all are successful in booting and logging on to the M01 (server) system. Two of the clients are also successful in getting a 5250 session to the M15 system. Through the IBM Network Station Manager, different autostart values can be made for each individual Network Station user.

9.2.2 Scenario 2: V1R3 clients using BOOTP only

This scenario follows 9.2.1, “Scenario 1: V1R3 clients using NVRAM and BOOTP” on page 224. In this scenario, we move our NVRAM clients to BOOTP. This scenario shows the same LAN attached and twinaxial attached IBM Network Stations. Again, only the V1R3 code of the IBM Network Station Manager is used in this scenario.

9.2.2.1 Scenario overview

This scenario shows an AS/400 system (M01) running V4R3M0 of OS/400. The AS/400 system supports one of each of the following models of Network Station:

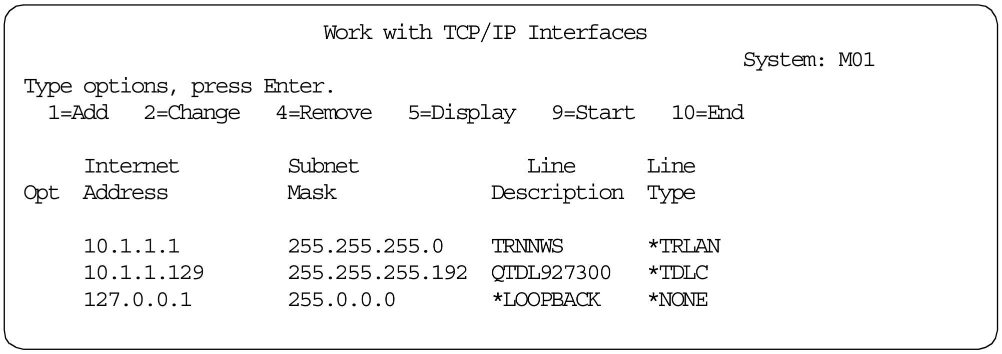
- **Network Station Series 100:** Token-Ring attached
- **Network Station Series 300:** Twinaxial attached
- **Network Station Series 1000:** Token-Ring attached

Because these hardware models are supported under the V1R3 Network Station Manager code, this code level will be the only level installed on the AS/400 system.

9.2.2.2 Scenario network configuration

Figure 171 on page 225 shows the network topology of the AS/400 systems and the attached Network Station clients. An internal LAN exists for the Token-Ring attached Network Station models, and a different network addressing scheme is used for the twinaxial subunit.

The IP interfaces defined for this scenario are shown in Figure 183. The twinaxial network is a subunit of the main network 10.1.1.0.



```
                         Work with TCP/IP Interfaces
                                                                System: M01
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet              Line      Line
Opt  Address          Mask                Description  Type

     10.1.1.1         255.255.255.0       TRNNWS       *TRLAN
     10.1.1.129       255.255.255.192     QTDL927300   *TDLC
     127.0.0.1        255.0.0.0           *LOOPBACK    *NONE
```

Figure 183. AS/400 Work with TCP/IP Interfaces screen

The twinaxial subunit range is from 10.1.1.128 to 10.1.1.191. This gives the subunit 61 available IP addresses.

Attention

During the testing and verification of this scenario, a problem with BOOTP was encountered when the twinaxial subnet was configured in the range of 10.1.1.192 to 10.1.1.255. Since this range is part of the main 10.1.1.0 network, transparent subnet masking is used. The range included the 10.1.1.0 network broadcast address (10.1.1.255), which is where a problem was discovered. At this time, we recommend that you *do not* configure a transparent subnet that would include the network broadcast address. For our scenarios, we chose a twinaxial subnet of 10.1.1.129.

Further information on this problem can be found in Informational APAR II12070. You can order this information with the following AS/400 command:

```
SNDPTFORD II12070
```

9.2.2.3 Network Station configuration

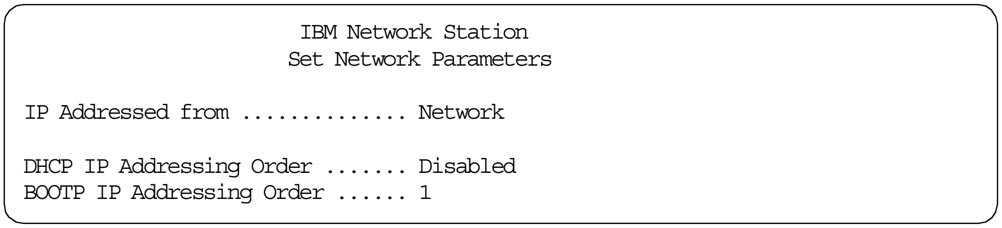
There are three IBM Network Stations used in this scenario. All three clients use the BOOTP method for obtaining their IP addresses.

Table 39 shows some of the IBM Network Station hardware specifications. The models shown are the ones that are being used in this scenario.

Table 39. IBM Network Station specifications

Network Station model	Boot monitor version	Total DRAM memory	IP address
100	v3.0.7.6	16 MB	10.1.1.5
341 - Twinaxial	v3.0.7.2	32 MB	10.1.1.130
1000	v3.0.8.8	64 MB	10.1.1.6

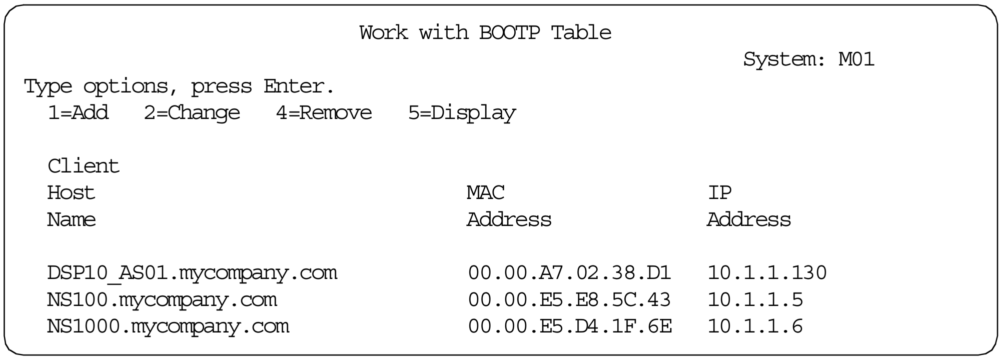
The configuration for all the models are contained both on the Network Station and on the AS/400 system. The only configuration needed on the Network Station itself is in the Network Parameters. An example of this screen in shown in Figure 184.



```
                       IBM Network Station
                      Set Network Parameters

IP Addressed from ............. Network

DHCP IP Addressing Order ....... Disabled
BOOTP IP Addressing Order ...... 1
```

Figure 184. IBM Network Station: Network parameters

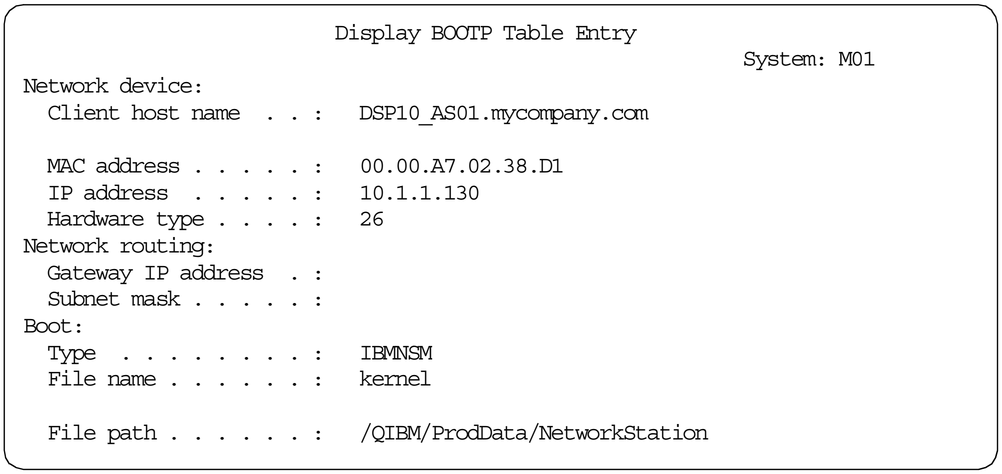
The remaining configuration screens on the Network Station do not need to be set. However, on the AS/400 system, you need to ensure that a BOOTP table entry exists for each Network Station. Figure 185 shows the output of the Work with BOOTP Table (WRKBPTBL) command on the AS/400 system.



```
                            Work with BOOTP Table
                                                              System: M01
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

  Client
  Host                                MAC                 IP
  Name                                Address             Address

  DSP10_AS01.mycompany.com            00.00.A7.02.38.D1   10.1.1.130
  NS100.mycompany.com                 00.00.E5.E8.5C.43   10.1.1.5
  NS1000.mycompany.com                00.00.E5.D4.1F.6E   10.1.1.6
```

Figure 185. AS/400 Work with BOOTP Table entries screen

When option 5 is entered next to a client entry, the information for the twinaxial client appears as shown in Figure 186. The information for the Model 100 and 1000 is shown in Figure 175 on page 227 and Figure 176 on page 228 respectively.

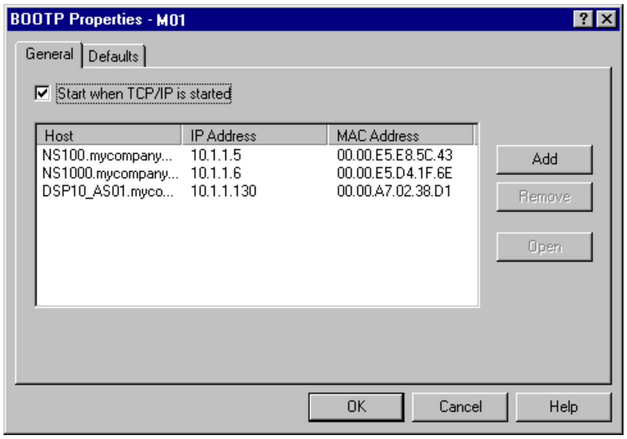


```
                          Display BOOTP Table Entry
                                                              System: M01
Network device:
  Client host name  . . :   DSP10_AS01.mycompany.com

  MAC address . . . . . :   00.00.A7.02.38.D1
  IP address  . . . . . :   10.1.1.130
  Hardware type . . . . :   26
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . . . . :   IBMNSM
  File name . . . . . . :   kernel

  File path . . . . . . :   /QIBM/ProdData/NetworkStation
```

Figure 186. AS/400 BOOTP Table Entry for Model 341 Network Station

These BOOTP entries can also be added or viewed in Operations Navigator. To do this, double-click **Network->Servers->TCP/IP**.

A list of servers appears in the right-hand side of the window. Left-click the **BOOTP** entry, and a pull-down menu appears. Right-click **Properties**. A window similar to the one shown in Figure 187 on page 234 appears.



☑ Start when TCP/IP is started

Host	IP Address	MAC Address
NS100.mycompany...	10.1.1.5	00.00.E5.E8.5C.43
NS1000.mycompany...	10.1.1.6	00.00.E5.D4.1F.6E
DSP10_AS01.myco...	10.1.1.130	00.00.A7.02.38.D1

Figure 187. AS/400 Operations Navigator: BOOTP properties

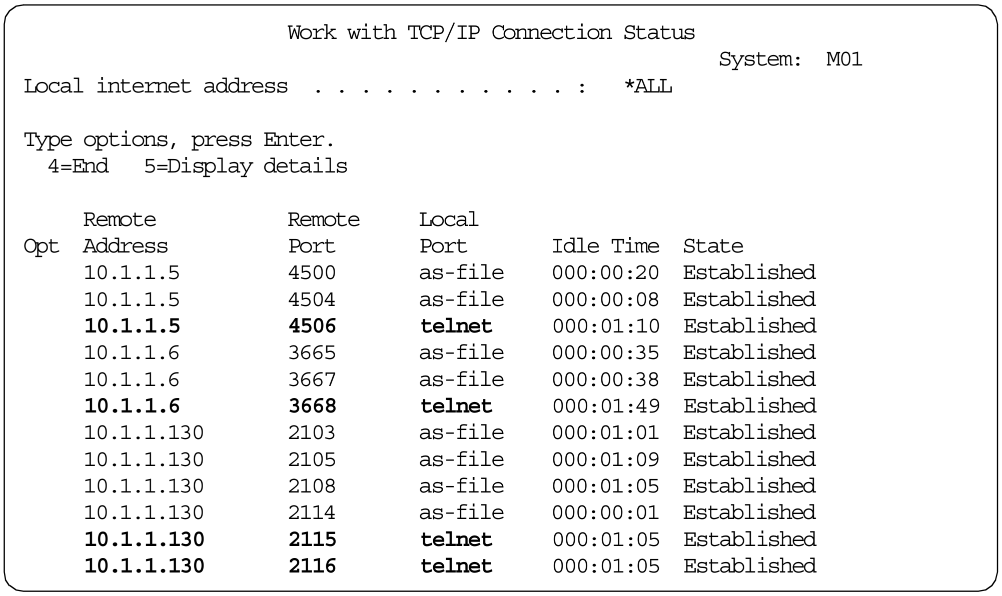
9.2.2.4 AS/400 requirements

In this scenario, it is necessary to have the TFTP and BOOTP servers started on the AS/400 server. After the boot-up process completes, a sign-on screen is present on all three client Network Stations. For each client user to sign on successfully, the Network Station Login Server needs to be started on port 256.

There are autostart 5250 sessions configured within the Network Station Manager. When the authentication of each user was completed, the appropriate 5250 sessions were autostarted on each client Network Station.

9.2.2.5 Connectivity verification

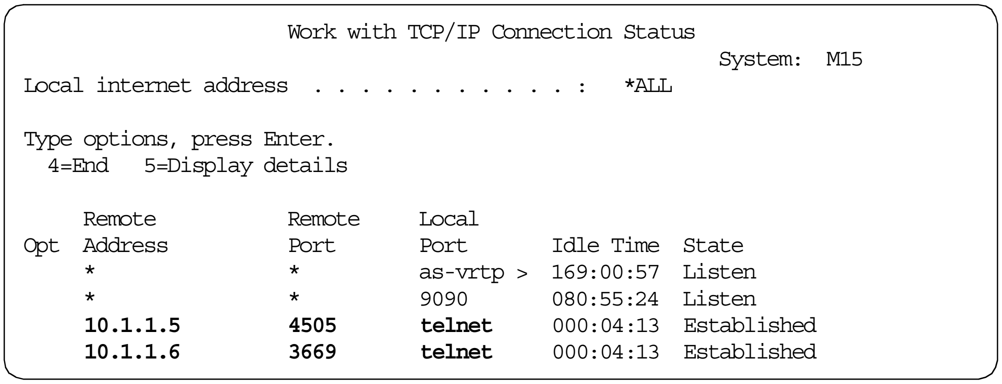
All three clients in this scenario have autostart 5250 sessions configured for the M01 system. To verify that these sessions are started, you can review the TCP/IP connection status screen on the M01 system by using the `NETSTAT *CNN` command. Figure 188 shows that the 10.1.1.130 (twinaxial client) has two established sessions and the LAN clients each have one. This validates the configuration done for USER1, USER2, and USER3 in the Network Station Manager.



```
                      Work with TCP/IP Connection Status
                                                           System:  M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.5         4500       as-file    000:00:20  Established
     10.1.1.5         4504       as-file    000:00:08  Established
     10.1.1.5         4506       telnet     000:01:10  Established
     10.1.1.6         3665       as-file    000:00:35  Established
     10.1.1.6         3667       as-file    000:00:38  Established
     10.1.1.6         3668       telnet     000:01:49  Established
     10.1.1.130       2103       as-file    000:01:01  Established
     10.1.1.130       2105       as-file    000:01:09  Established
     10.1.1.130       2108       as-file    000:01:05  Established
     10.1.1.130       2114       as-file    000:00:01  Established
     10.1.1.130       2115       telnet     000:01:05  Established
     10.1.1.130       2116       telnet     000:01:05  Established
```

Figure 188. AS/400 TCP/IP connections: M01 system verification

Alternatively, USER2 and USER3 also have an autostart session for the M15 system. On the M15 system, `NETSTAT *CNN` is issued on a command line. The resulting screen is shown in Figure 189.



```
                      Work with TCP/IP Connection Status
                                                           System:  M15
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          as-vrtp >  169:00:57  Listen
     *                *          9090       080:55:24  Listen
     10.1.1.5         4505       telnet     000:04:13  Established
     10.1.1.6         3669       telnet     000:04:13  Established
```

Figure 189. AS/400 TCP/IP connections: M15 system verification

9.2.2.6 Summary

This scenario shows a network of two AS/400 systems and three IBM Network Station clients. One of the AS/400 systems (M01) is a boot server, which is set up to supply IP addresses to the IBM Network Station clients. The level of the IBM Network Station Manager is V1R3. Different parts of the IBM Network Station Manager code are discussed as they relate to the V1R3 version.

Only the BOOTP boot method is used among the IBM Network Station clients, and all are successful in booting and logging on to the M01 (server) system. Two of the clients are also successful in getting a 5250 session to the M15 system. Through the IBM Network Station Manager, different autostart values can be made for each individual Network Station user.

9.2.3 Scenario 3: V1R3 clients using DHCP

This scenario is similar to 9.2.2, “Scenario 2: V1R3 clients using BOOTP only” on page 231. In some environments, DHCP may be used instead of BOOTP. This scenario shows the same LAN-attached and twinaxial-attached IBM Network Stations. Again, only the V1R3 code of the IBM Network Station Manager is used in this scenario.

9.2.3.1 Scenario overview

This scenario shows an AS/400 system (M01) running V4R3M0 of OS/400. The AS/400 system supports one of each of the following models of Network Station:

- **Network Station Series 100:** Token-Ring attached
- **Network Station Series 300:** Twinaxial attached
- **Network Station Series 1000:** Twinaxial attached

Because these hardware models are supported under the V1R3 Network Station Manager code, this code level will be the only level installed on the AS/400 system.

9.2.3.2 Scenario network configuration

Figure 190 shows the network topology of the AS/400 systems and the attached Network Station clients. An internal LAN exists for the Token-Ring attached Network Station models, and a different network addressing scheme is used for the twinaxial subnet.

Tip

For more information about attaching twinaxial Network Stations to an AS/400 system, refer to *AS/400 IBM Network Station: Techniques for Deployment in a WAN*, SG24-5187.

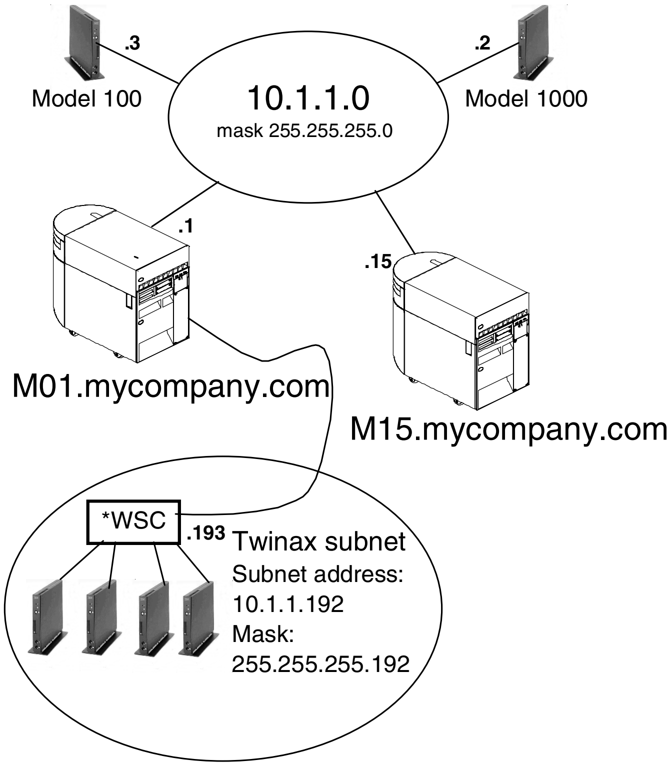


Figure 190. TCP/IP network topology for scenario 3

The IP interfaces defined for this scenario are shown in Figure 191. The twinaxial network is a subnet of the main network 10.1.1.0.

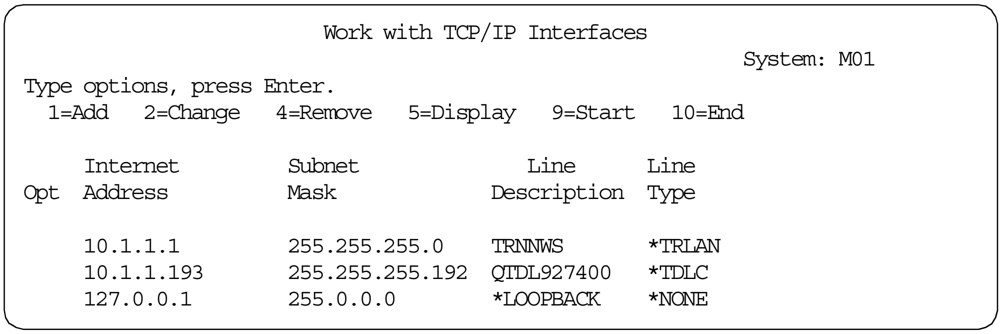

```
                          Work with TCP/IP Interfaces
                                                                System: M01
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet          Subnet              Line        Line
Opt  Address           Mask                Description  Type

     10.1.1.1          255.255.255.0      TRNNWS       *TRLAN
     10.1.1.193        255.255.255.192    QTDL927400   *TDLC
     127.0.0.1         255.0.0.0          *LOOPBACK    *NONE
```

Figure 191. AS/400 Work with TCP/IP Interfaces screen

The twinaxial subnet range is from 10.1.1.192 to 10.1.1.255. This gives the subnet 61 available IP addresses.

9.2.3.3 Network Station configuration

There are three IBM Network Stations used in this scenario. All three clients use the DHCP method for obtaining their IP addresses.

Table 40 shows some of the IBM Network Station hardware specifications. The models shown are the ones that are being used in this scenario.

Table 40. IBM Network Station specifications

Network Station model	Boot monitor Version	Total DRAM memory	IP address
100	v3.0.7.6	16 MB	10.1.1.5
341 - Twinax	v3.0.7.2	32 MB	10.1.1.130
1000	v3.0.8.8	64 MB	10.1.1.6

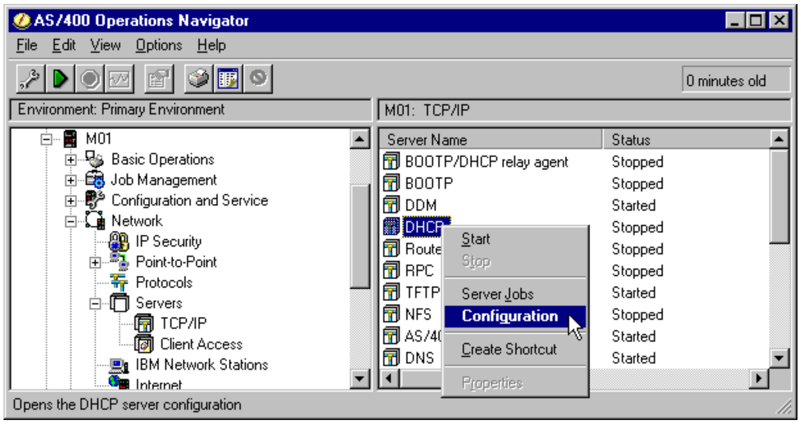
The configuration for all the models are contained both on the Network Station and on the AS/400 system. The only configuration needed on the Network Station itself is in the Network Parameters. An example of this screen in shown in Figure 192.

```
                         IBM Network Station
                        Set Network Parameters

IP Addressed from .............. Network

DHCP IP Addressing Order ....... 1
BOOTP IP Addressing Order ...... Disabled
```

Figure 192. IBM Network Station: Network parameters

The remaining configuration for these DHCP clients is contained in the DHCP server properties. You can access this server through Operations Navigator. When you are in Operations Navigator, double-click **Network->Servers->TCP/IP**.

A list of the TCP/IP servers appear on the right-hand side of the display. Left-click the **DHCP** server. A display similar to the one shown in Figure 193 appears.



Server Name	Status
BOOTP/DHCP relay agent	Stopped
BOOTP	Stopped
DDM	Started
DHCP	Stopped
Route	Stopped
RPC	Stopped
TFTP	Started
NFS	Stopped
AS/4(	Started
DNS	Started

Opens the DHCP server configuration

Figure 193. AS/400 Operations Navigator: DHCP server

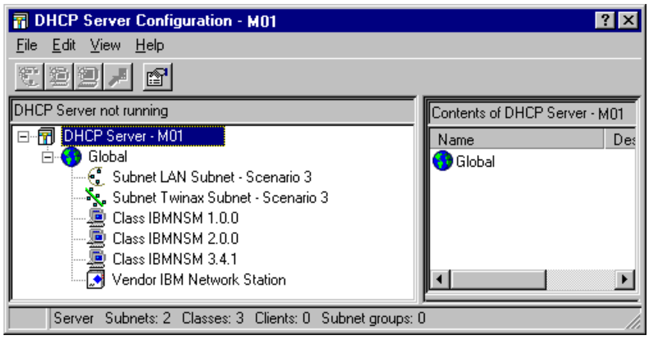
Note

> The configuration of DHCP on the AS/400 system is beyond the scope of this redbook. More detailed information can be found in *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, and *IBM Network Station Manager Installation and Use*, SC41-0664.

If you are configuring DHCP on a system that does not have an existing configuration, Operations Navigator will automatically start the DHCP configuration Wizard. This Wizard helps you create a basic DHCP server configuration. The DHCP Wizard automatically adds these classes:

- **IBMNSM 1.0.0:** Token Ring attached Network Stations
- **IBMNSM 2.0.0:** Ethernet attached Network Stations
- **IBMNSM 3.4.1:** Twinaxial attached Network Stations

For this scenario, there are two subnets configured within DHCP. One subnet is for the LAN and the other subnet is for the twinaxial subnet. These classes and the configured subnets are shown in Figure 194.



DHCP Server not running

- DHCP Server - M01
  - Global
    - Subnet LAN Subnet - Scenario 3
    - Subnet Twinax Subnet - Scenario 3
    - Class IBMNSM 1.0.0
    - Class IBMNSM 2.0.0
    - Class IBMNSM 3.4.1
    - Vendor IBM Network Station

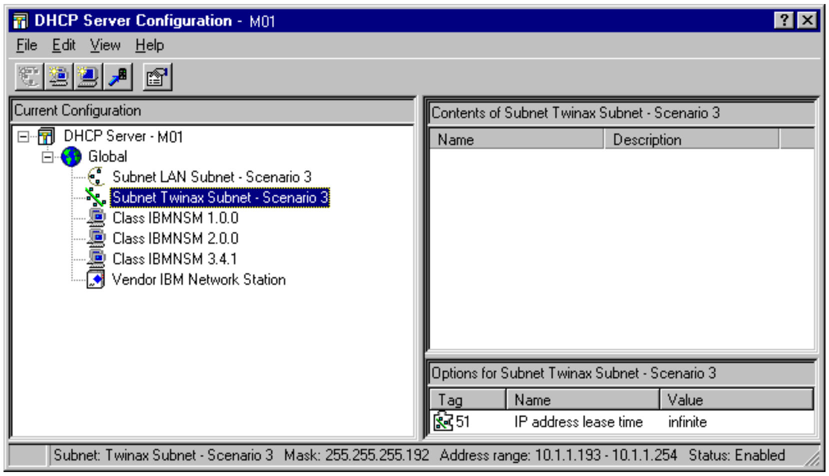
Contents of DHCP Server - M01

Name	Des
Global	

Server Subnets: 2 Classes: 3 Clients: 0 Subnet groups: 0

Figure 194. AS/400 Operations Navigator: DHCP configuration

When you left-click the Twinax subnet, its options are shown on the right side. On the bottom of the screen, you can see the mask and address range that has been configured for this subnet. This DHCP information is shown in Figure 195.



Current Configuration

- DHCP Server - M01
  - Global
    - Subnet LAN Subnet - Scenario 3
    - Subnet Twinax Subnet - Scenario 3
    - Class IBMNSM 1.0.0
    - Class IBMNSM 2.0.0
    - Class IBMNSM 3.4.1
    - Vendor IBM Network Station

Contents of Subnet Twinax Subnet - Scenario 3

Name	Description

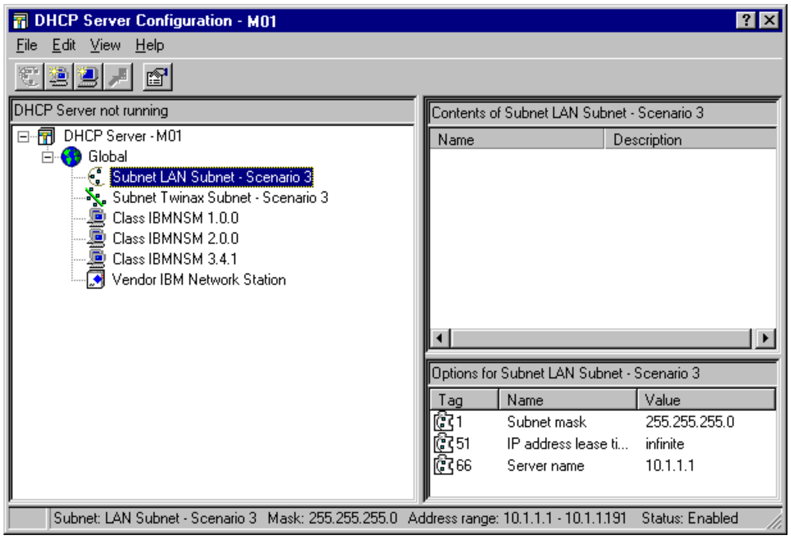
Options for Subnet Twinax Subnet - Scenario 3

Tag	Name	Value
51	IP address lease time	infinite

Subnet: Twinax Subnet - Scenario 3 Mask: 255.255.255.192 Address range: 10.1.1.193 - 10.1.1.254 Status: Enabled

Figure 195. AS/400 Operations Navigator: DHCP twinaxial subnet

When you left-click the LAN subnet, its options are shown on the right side of the display. On the bottom of the screen, you can see the mask and address range has been configured for this subnet. Figure 196 shows this DHCP information.


DHCP Server Configuration - M01
File
Edit
View
Help
DHCP Server not running
DHCP Server - M01
Global
Subnet LAN Subnet - Scenario 3
Subnet Twinax Subnet - Scenario 3
Class IBMNSM 1.0.0
Class IBMNSM 2.0.0
Class IBMNSM 3.4.1
Vendor IBM Network Station
Contents of Subnet LAN Subnet - Scenario 3
Name
Description
Options for Subnet LAN Subnet - Scenario 3

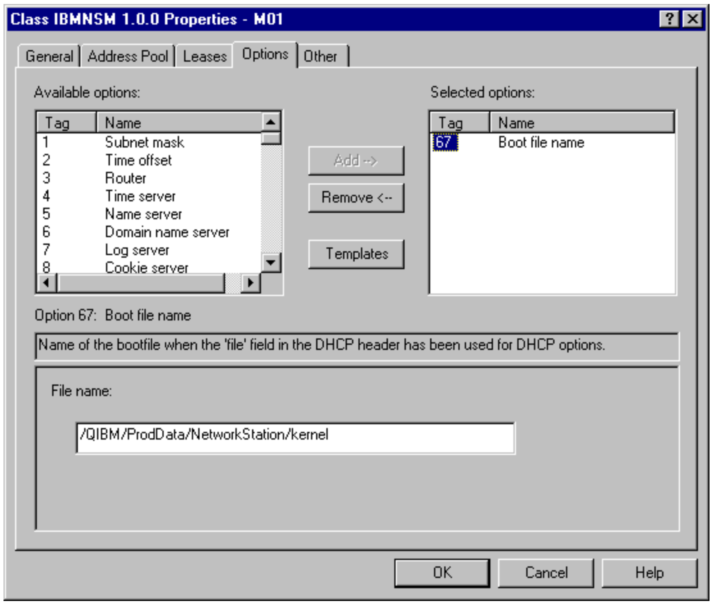
Tag	Name	Value
1	Subnet mask	255.255.255.0
51	IP address lease ti...	infinite
66	Server name	10.1.1.1

Subnet: LAN Subnet - Scenario 3 Mask: 255.255.255.0 Address range: 10.1.1.1 - 10.1.1.191 Status: Enabled

Figure 196. AS/400 Operations Navigator: DHCP LAN subnet

This range for the LAN was configured because the twinaxial subnet exists. The twinaxial subnet address is 10.1.1.192. This range of addresses, 10.1.1.192 to 10.1.1.255, is taken from the main 10.1.1.0 network. When the LAN subnet was created in the DHCP configuration, a subnet address of 10.1.1.0 was given. When Range to assign is chosen, the Wizard calculates a range of 10.1.1.1 to 10.1.1.254. In our scenario, we need to consider the twinaxial subnet. We can manually change the ending address (in the range) to be 10.1.1.191, as opposed to 10.1.1.254. This keeps the twinaxial subnet addresses from being used by the LAN attached devices.

When the DHCP Wizard configured the classes, it also defined Tag 67, Boot File Name. You should verify that the boot path and file name are correct. To show this, left-click any of the classes, and then choose **Properties**. Click the **Options** tab. A display like the example in Figure 197 is shown. You should see the following path in File name: /QIBM/ProdData/NetworkStation/kernel.



Class IBMNSM 1.0.0 Properties - M01

Available options:

Tag	Name
1	Subnet mask
2	Time offset
3	Router
4	Time server
5	Name server
6	Domain name server
7	Log server
8	Cookie server

Selected options:

Tag	Name
67	Boot file name

Option 67: Boot file name

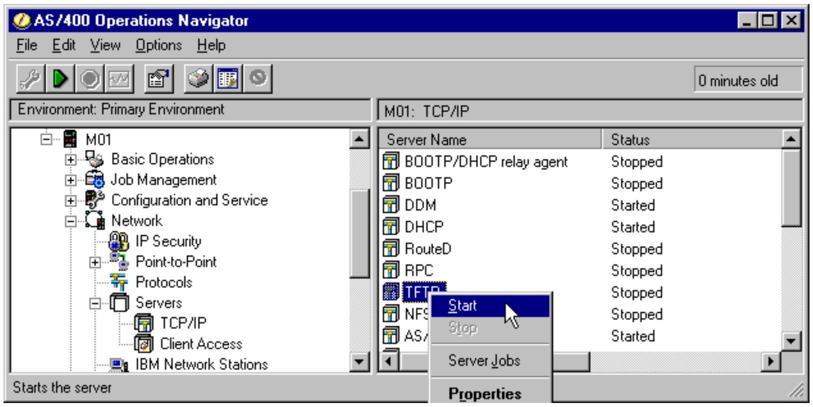
Name of the bootfile when the 'file' field in the DHCP header has been used for DHCP options.

File name: /QIBM/ProdData/NetworkStation/kernel

Figure 197. AS/400 Operations Navigator: Subnet properties

9.2.3.4 AS/400 requirements

Both the TFTP and the DHCP servers are required in this scenario. Both of these servers can be started from an AS/400 command line using either the `STRTCPSVR *TFTP` or `STRTCPSVR *DHCP` commands. Please ensure that the BOOTP server is not started. Both the BOOTP and DHCP servers cannot be running on the AS/400 system at the same time. Alternatively, you can start these servers from Operations Navigator. This is shown in Figure 198.



AS/400 Operations Navigator

Environment: Primary Environment

M01: TCP/IP

Server Name	Status
BOOTP/DHCP relay agent	Stopped
BOOTP	Stopped
DDM	Started
DHCP	Started
RouteD	Stopped
RPC	Stopped
TFTP	Stopped
NFS	Stopped
AS/	Started

Starts the server

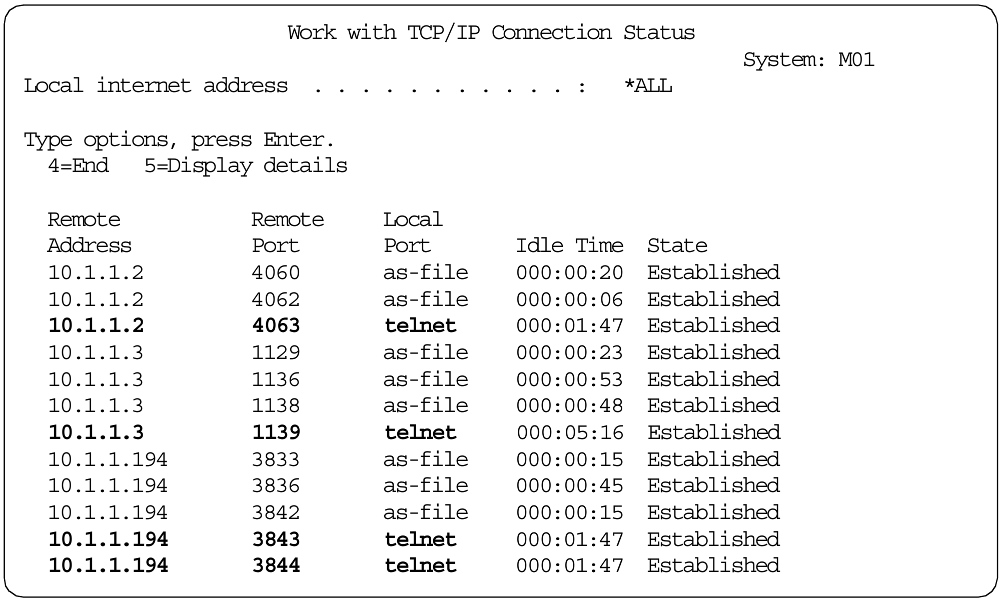
Figure 198. AS/400 Operations Navigator: TCP/IP servers

After the boot-up process completes, a sign-on screen is present on all three client Network Stations. For each client user to sign on successfully, the Network Station Login Server needs to be started on port 256.

There are autostart 5250 sessions configured within the Network Station Manager. When the authentication of each user was completed, the appropriate 5250 sessions were autostarted on each client Network Station.

9.2.3.5 Connectivity verification

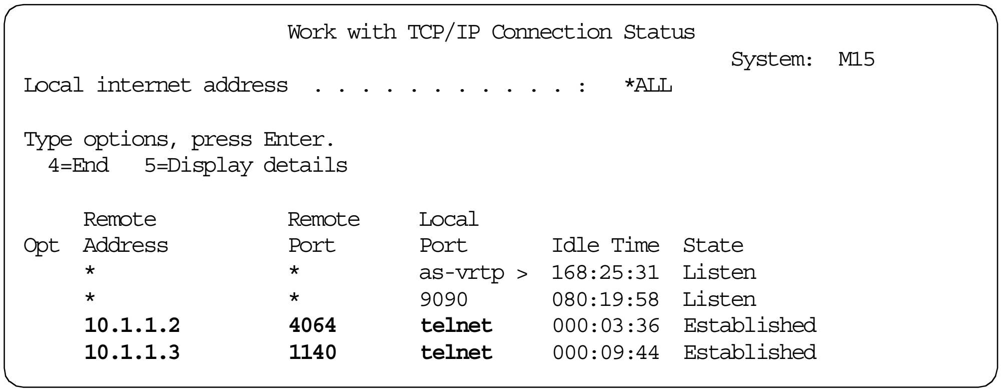
All three clients in this scenario have autostart 5250 sessions configured for the M01 system. To verify that these sessions are started, review the TCP/IP connection status screen, on the M01 system with the `NETSTAT *CNN` command. Figure 199 shows that the 10.1.1.194 (twinaxial client) has two established sessions and the LAN clients each have one. This validates the configuration done for USER1, USER2, and USER3 in the Network Station Manager.



```
                       Work with TCP/IP Connection Status
                                                           System: M01
Local internet address . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

  Remote           Remote     Local
  Address          Port       Port       Idle Time  State
  10.1.1.2         4060       as-file    000:00:20  Established
  10.1.1.2         4062       as-file    000:00:06  Established
  10.1.1.2         4063       telnet     000:01:47  Established
  10.1.1.3         1129       as-file    000:00:23  Established
  10.1.1.3         1136       as-file    000:00:53  Established
  10.1.1.3         1138       as-file    000:00:48  Established
  10.1.1.3         1139       telnet     000:05:16  Established
  10.1.1.194       3833       as-file    000:00:15  Established
  10.1.1.194       3836       as-file    000:00:45  Established
  10.1.1.194       3842       as-file    000:00:15  Established
  10.1.1.194       3843       telnet     000:01:47  Established
  10.1.1.194       3844       telnet     000:01:47  Established
```

Figure 199. AS/400 TCP/IP connections: M01 system verification

Alternatively, USER2 and USER3 also have an autostart session for the M15 system. On the M15 system, `NETSTAT *CNN` is issued on a command line. The resulting screen is shown in Figure 200.



```
                       Work with TCP/IP Connection Status
                                                          System:  M15
Local internet address . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          as-vrtp >  168:25:31  Listen
     *                *          9090       080:19:58  Listen
     10.1.1.2         4064       telnet     000:03:36  Established
     10.1.1.3         1140       telnet     000:09:44  Established
```

Figure 200. AS/400 TCP/IP connections: M15 system verification

9.2.3.6 Summary

This scenario shows a network of two AS/400 systems and three IBM Network Station clients. One of the AS/400 systems (M01) is a DHCP server which is set up to supply IP addresses to the IBM Network Station clients. The level of the IBM Network Station Manager is V1R3.

The LAN-attached Network Stations are part of a DHCP subnet, while the Model 341, twinaxial-attached Network Station is part of a different DHCP subnet. All three clients were successful in booting and logging on to the M01 (server) system. Their respective autostart sessions were also established.

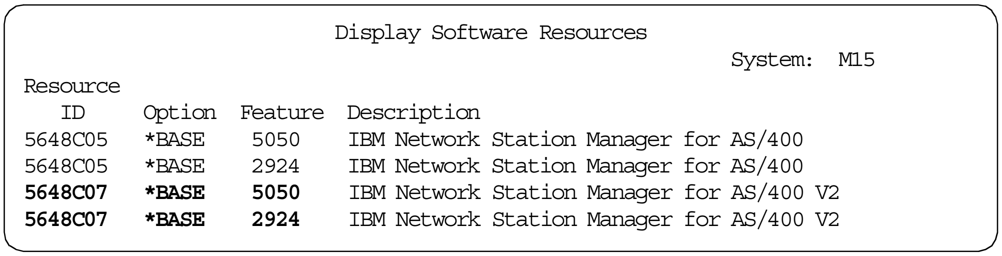
9.3 V1R3 and V2R1 scenarios

Three scenarios, involving both the V1R3 and V2R1 IBM Network Station Manager code, are presented in this section. We discuss some features and functionality of the V2R1 IBM Network Station Manager code as it pertains to an AS/400 server system.

AS/400 information

Both the V1R3 and V2R1 code is installed on the AS/400 server system. We briefly explore some portions of the AS/400 system as a review of the elements of the V2R1 Network Station Manager Code.

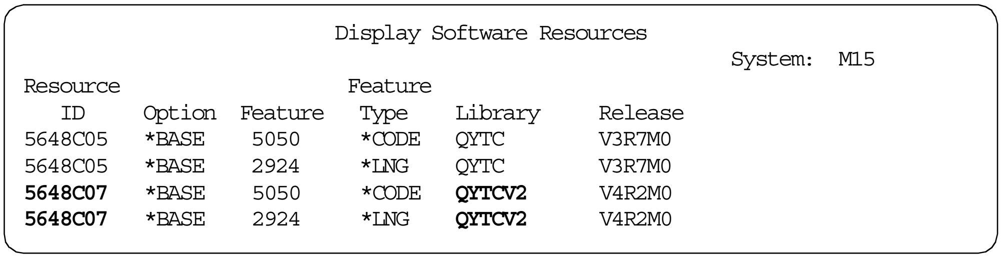
Figure 201 shows a listing of the installed code. The AS/400 `DSPSFWRSC` command used is.



```
                          Display Software Resources
                                                              System:   M15
Resource
   ID      Option  Feature  Description
5648C05    *BASE    5050    IBM Network Station Manager for AS/400
5648C05    *BASE    2924    IBM Network Station Manager for AS/400
5648C07    *BASE    5050    IBM Network Station Manager for AS/400 V2
5648C07    *BASE    2924    IBM Network Station Manager for AS/400 V2
```

Figure 201. AS/400 Display Software Resource screen (V1R3 and V2R1)

Alternatively, press the F11 function key on the screen shown in Figure 201 to see the libraries and release associated with the both products. The results are shown in Figure 202.



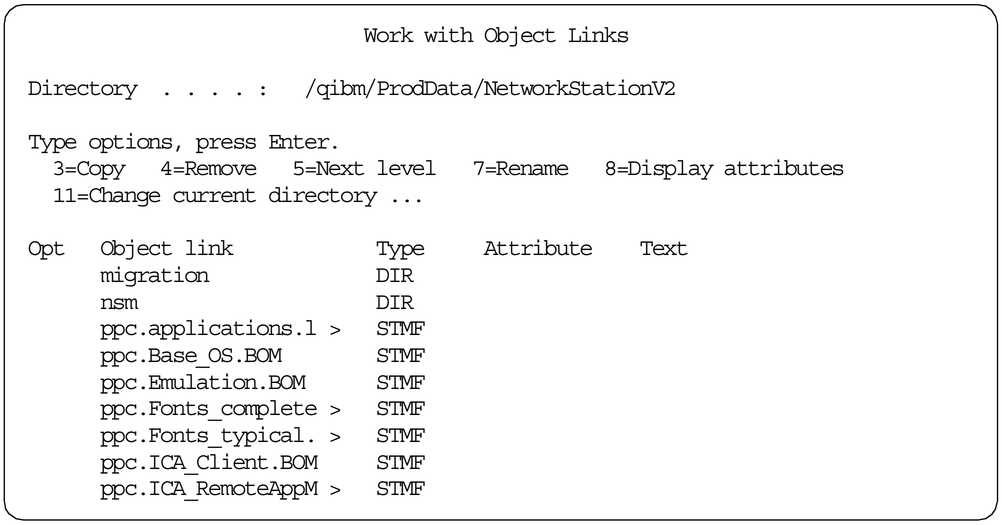
```
                          Display Software Resources
                                                              System:   M15
Resource                    Feature
   ID      Option  Feature   Type    Library     Release
5648C05    *BASE    5050     *CODE   QYTC        V3R7M0
5648C05    *BASE    2924     *LNG    QYTC        V3R7M0
5648C07    *BASE    5050     *CODE   QYTCV2      V4R2M0
5648C07    *BASE    2924     *LNG    QYTCV2      V4R2M0
```

Figure 202. AS/400 Display Software Resource screen: Alternate view for products

Much of the V2R1 Network Station code is contained within the Integrated File System. This information can be viewed with a 5250 green-screen session or with Operations Navigator. The paths for these directories are:

- QIBM/PRODDATA/NETWORKSTATIONV2
- QIBM/USERDATA/NETWORKSTATIONV2

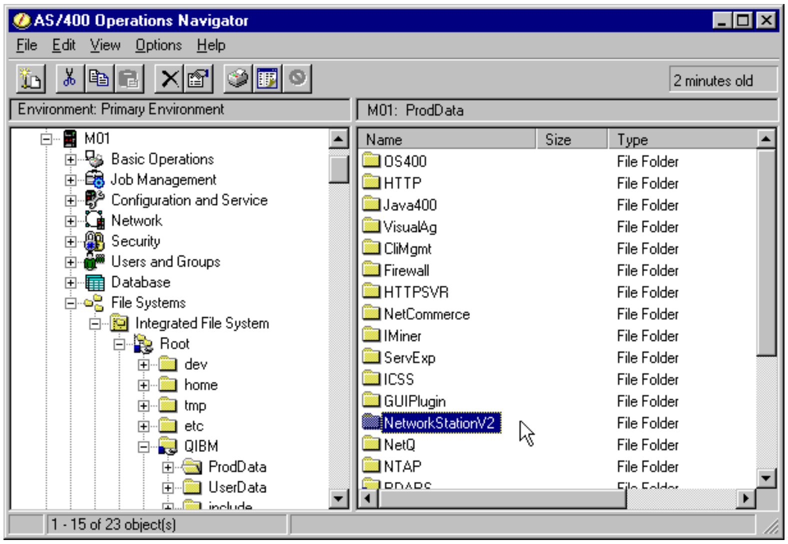
On a 5250 green-screen session, the Work Link (WRKLNK) command is used to navigate through the Integrated File System. Figure 203 shows this AS/400 screen.



```
                        Work with Object Links

Directory  . . . . :   /qibm/ProdData/NetworkStationV2

Type options, press Enter.
  3=Copy   4=Remove   5=Next level   7=Rename   8=Display attributes
  11=Change current directory ...

Opt   Object link            Type     Attribute    Text
      migration              DIR
      nsm                    DIR
      ppc.applications.l >   STMF
      ppc.Base_OS.BOM        STMF
      ppc.Emulation.BOM      STMF
      ppc.Fonts_complete >   STMF
      ppc.Fonts_typical. >   STMF
      ppc.ICA_Client.BOM     STMF
      ppc.ICA_RemoteAppM >   STMF
```

Figure 203. AS/400 Work with Object Links screen (V2R1)

If you are using Operations Navigator, a window similar to the example in Figure 204 appears when viewing the Integrated File System.



Name	Size	Type
OS400		File Folder
HTTP		File Folder
Java400		File Folder
VisualAg		File Folder
CliMgmt		File Folder
Firewall		File Folder
HTTPSVR		File Folder
NetCommerce		File Folder
IMiner		File Folder
ServExp		File Folder
ICSS		File Folder
GUIPlugin		File Folder
NetworkStationV2		File Folder
NetQ		File Folder
NTAP		File Folder

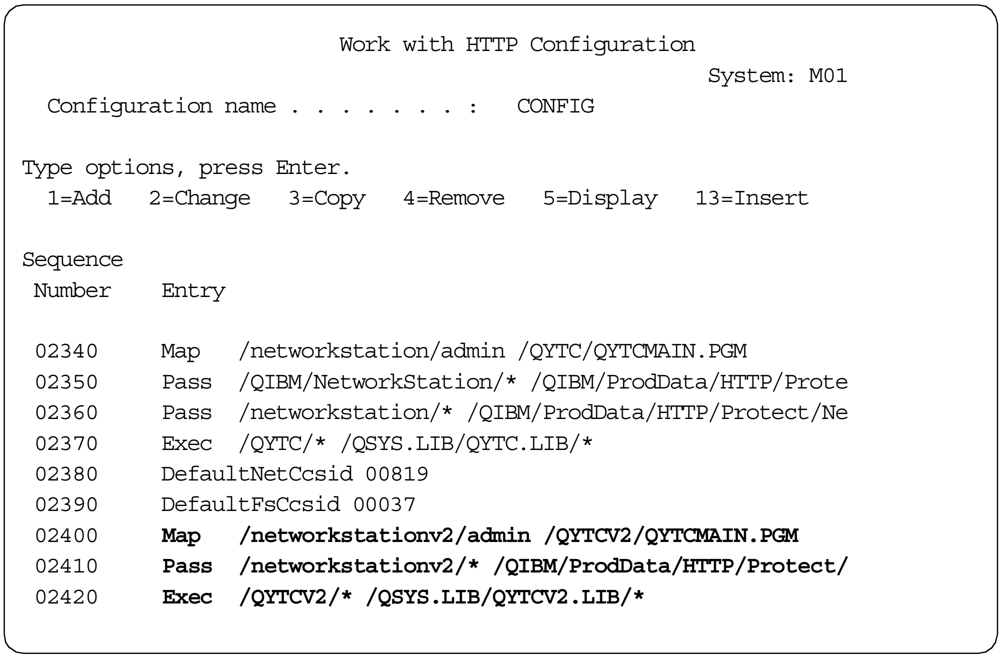
Figure 204. AS/400 Operations Navigator: Viewing the Integrated File System

Other important parts of the Network Station code are the HTTP server directives. There is one server directive that is used with the V2R1 Network Station Manager code. This server directive can be viewed with a 5250 session with the following AS/400 command:

```
WRKHTTPCFG
```

The resulting screen is shown in Figure 205. It shows lines that were added when the V2R1 Setup Wizard was run. This Setup Wizard is part of the V2R1 IBM

Network Station Manager code. For further information on the V2R1 Setup Wizard, refer to Chapter 4, “Installation and server setup” on page 83.

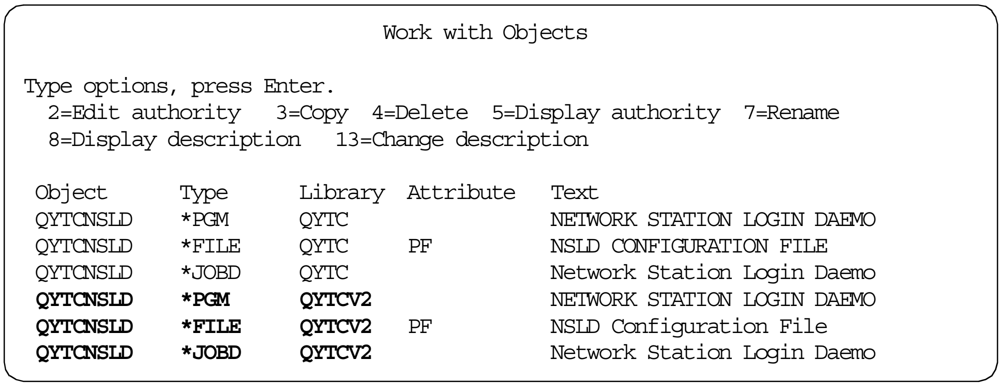


```
                         Work with HTTP Configuration
                                                          System: M01
  Configuration name . . . . . . . :   CONFIG

Type options, press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display   13=Insert

Sequence
 Number    Entry

 02340     Map   /networkstation/admin /QYTC/QYTCMAIN.PGM
 02350     Pass  /QIBM/NetworkStation/* /QIBM/ProdData/HTTP/Prote
 02360     Pass  /networkstation/* /QIBM/ProdData/HTTP/Protect/Ne
 02370     Exec  /QYTC/* /QSYS.LIB/QYTC.LIB/*
 02380     DefaultNetCcsid 00819
 02390     DefaultFsCcsid 00037
 02400     Map   /networkstationv2/admin /QYTCV2/QYTCMAIN.PGM
 02410     Pass  /networkstationv2/* /QIBM/ProdData/HTTP/Protect/
 02420     Exec  /QYTCV2/* /QSYS.LIB/QYTCV2.LIB/*
```

Figure 205. AS/400 Work with HTTP Configuration screen: Default instance

Lines 02400 to 02420, also shown in Figure 205, were added the V2R1 Setup Wizard.

The Network Station Login Server job runs in the QSYSWRK subsystem. The job itself is called QYTCNSLD. In the V1R3 level of Network Station Manager, these program objects reside in the QYTC library. In the V2R1 level of Network Station Manager, these program objects reside in the QYTCV2 library. Figure 206 shows the `WRKOBJ OBJ(*ALL/QYTCNSLD)` command on an AS/400 system that has both the V1R3 and V2R1 IBM Network Station Manager code installed.

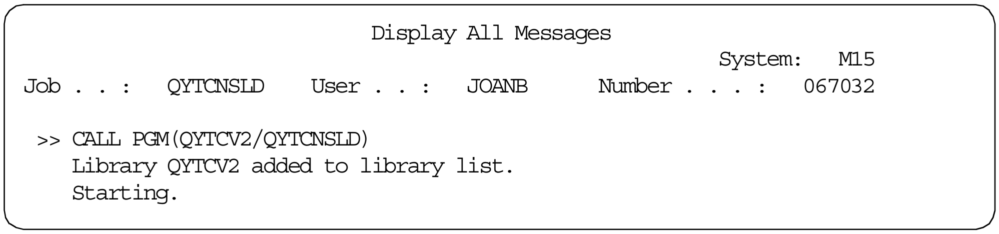


```
                             Work with Objects

Type options, press Enter.
  2=Edit authority   3=Copy  4=Delete  5=Display authority  7=Rename
  8=Display description   13=Change description

 Object      Type      Library  Attribute   Text
 QYTCNSLD    *PGM      QYTC                 NETWORK STATION LOGIN DAEMO
 QYTCNSLD    *FILE     QYTC     PF          NSLD CONFIGURATION FILE
 QYTCNSLD    *JOBD     QYTC                 Network Station Login Daemo
 QYTCNSLD    *PGM      QYTCV2               NETWORK STATION LOGIN DAEMO
 QYTCNSLD    *FILE     QYTCV2   PF          NSLD Configuration File
 QYTCNSLD    *JOBD     QYTCV2               Network Station Login Daemo
```

Figure 206. AS/400 Work with Object screen (V1R3 and V2R1)

In a coexistence scenario, *only* one of these login servers can run at any given time. The V2R1 login server can support both V1R3 and V2R1 clients, so the QYTCV2/QYTCNSLD server *should* be running in a coexistence environment.

You can determine which server is running on the system by viewing the job log for QYTCNSLD. The AS/400 `WRKJOB QTYCNSLD` command generates the information shown in Figure 207.



```
                            Display All Messages
                                                      System:   M15
Job . . :   QYTCNSLD    User . . :   JOANB      Number . . . :   067032

 >> CALL PGM(QYTCV2/QYTCNSLD)
    Library QYTCV2 added to library list.
    Starting.
```

Figure 207. AS/400 job log for QYTCNSLD in library QYTCV2

Network Station Connectivity: AS/400 servers required

In the following scenarios, for the IBM Network Station clients to successfully log on to the AS/400 server, certain TCP/IP servers must be started. Specifically the TFTP server must always be started. This server can be started with the AS/400 Start TCP/IP Server (`STRTCPSVR *TFTP`) command. This server is required whether the client is using the NVRAM, BOOTP, or DHCP method of booting.

For the BOOTP clients, the BOOTP server must also be started. The AS/400 command to start this server is:

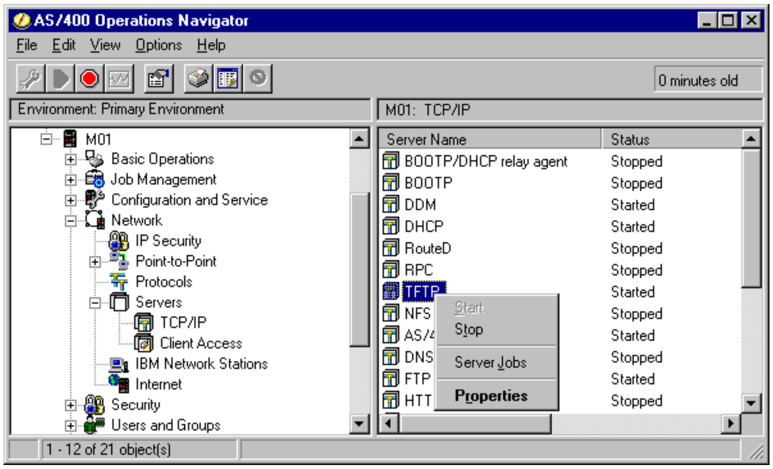
```
STRTCPSVR *BOOTP
```

For the DHCP clients, the DHCP server must be started in addition to the TFTP server. The AS/400 command to start this server is:

```
STRTCPSVR *DHCP
```

If there is a need to have these servers active after every IPL, they can be set to always autostart after an IPL of the system. You can modify the autostart parameter of the TCP/IP servers with a 5250 session or with Operations Navigator. With a 5250 session, issue the command `CFGTCP` and then select option **20**, Configure TCP/IP applications.

Alternatively, you can use Operations Navigator. Within the Operations Navigator screen, double-click **Network->Servers->TCP/IP**. At this point, a list of the servers appears in the right-hand side. The autostart parameter is shown within the properties for the TFTP and BOOTP. You need to right-click on the server of your choice. An example of this display is shown in Figure 208.

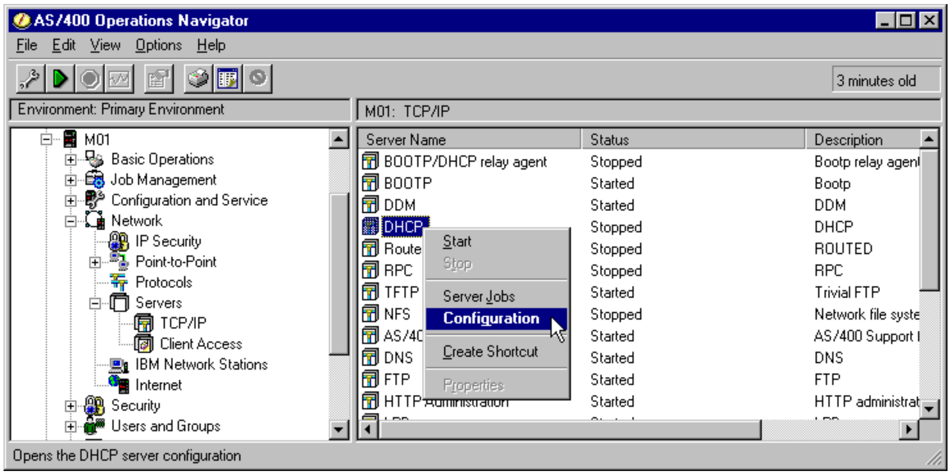


Server Name	Status
BOOTP/DHCP relay agent	Stopped
BOOTP	Stopped
DDM	Started
DHCP	Started
RouteD	Stopped
RPC	Stopped
TFTP	Started
NFS	Stopped
AS/4	Started
DNS	Stopped
FTP	Started
HTT	Stopped

1 - 12 of 21 object(s)

Figure 208. AS/400 Operations Navigator: TCP/IP servers

For the DHCP server, right-click the server, and then choose **Configuration** as shown in Figure 209.

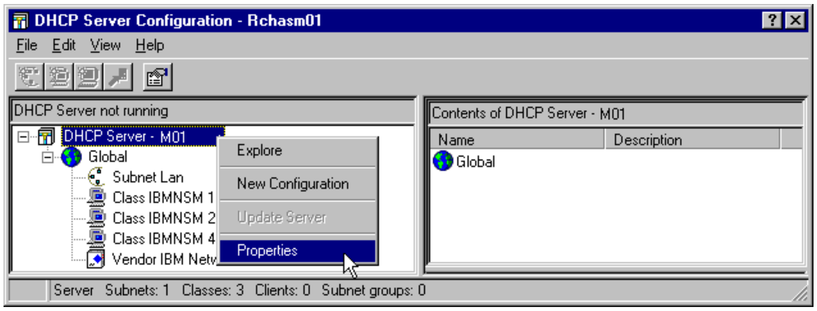


Server Name	Status	Description
BOOTP/DHCP relay agent	Stopped	Bootp relay agen
BOOTP	Started	Bootp
DDM	Started	DDM
DHCP	Stopped	DHCP
Route	Stopped	ROUTED
RPC	Stopped	RPC
TFTP	Started	Trivial FTP
NFS	Stopped	Network file syste
AS/40	Started	AS/400 Support I
DNS	Started	DNS
FTP	Started	FTP
HTTP Administration	Started	HTTP administrat

Opens the DHCP server configuration

Figure 209. AS/400 Operations Navigator: DHCP server

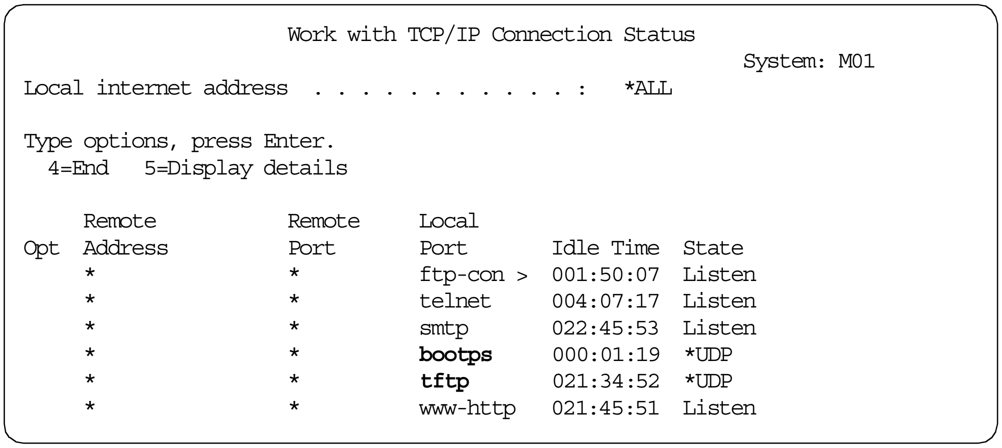
Once the DHCP configuration has been presented, right-click the **DHCP Server**, and select **Properties**. Once in Properties, you can set the autostart parameter. The DHCP configuration display is shown in Figure 210.



Server Subnets: 1 Classes: 3 Clients: 0 Subnet groups: 0

Figure 210. AS/400 Operations Navigator: DHCP server properties

Once you start these servers, either through a 5250 session or Operations Navigator, you can check to see that the servers are active. Figure 211 shows the output of the AS/400 NETSTAT *CNN command.



```
                       Work with TCP/IP Connection Status
                                                           System: M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          ftp-con >  001:50:07  Listen
     *                *          telnet     004:07:17  Listen
     *                *          smtp       022:45:53  Listen
     *                *          bootps     000:01:19  *UDP
     *                *          tftp       021:34:52  *UDP
     *                *          www-http   021:45:51  Listen
```

*Figure 211. AS/400 NETSTAT *CNN screen showing BOOTP and TFTP servers*

Alternatively, you can also check the status of these servers through Operations Navigator. Refer to Figure 209 on page 247 for a view of these servers and their status.

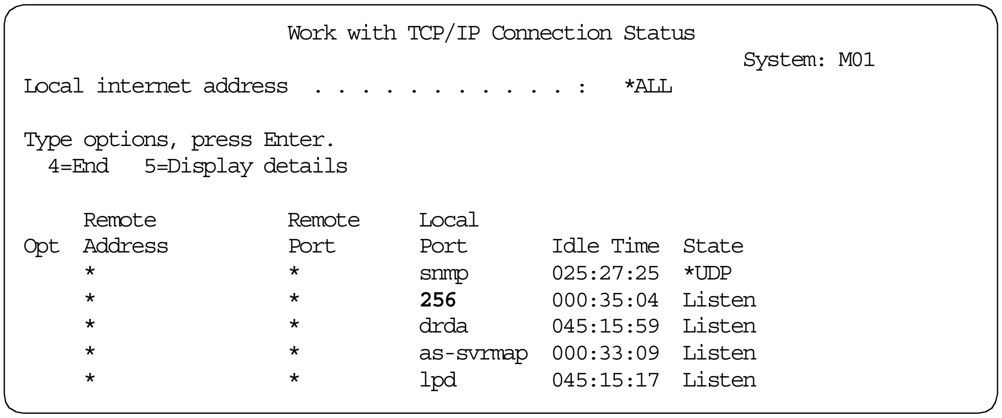
Lastly, the Network Station login server must also be running on your AS/400 system. This server allows your Network Station Users to log onto the AS/400 system. The command to start this server is:

```
CALL QYTCV2/QYTCUSVR ('STRTCPSVR ')
```

To show that the server is active, issue the following command from an AS/400 command line:

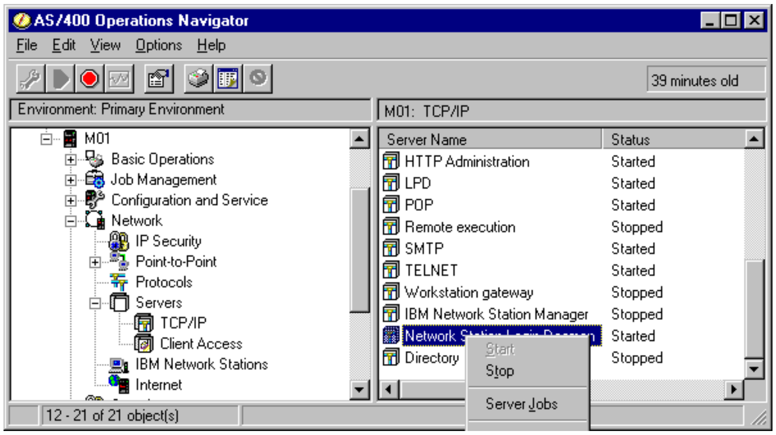
```
NETSTAT *CNN
```

The server uses port 256. Alternatively, you can also view and start this server in Operations Manager. Figure 212 shows the 5250 screen output, and Figure 213 shows the Operations Navigator view.



```
                       Work with TCP/IP Connection Status
                                                           System: M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          snmp       025:27:25  *UDP
     *                *          256        000:35:04  Listen
     *                *          drda       045:15:59  Listen
     *                *          as-svrmap  000:33:09  Listen
     *                *          lpd        045:15:17  Listen
```

*Figure 212. AS/400 NETSTAT *CNN screen showing port 256*



Server Name	Status
HTTP Administration	Started
LPD	Started
POP	Started
Remote execution	Stopped
SMTP	Started
TELNET	Started
Workstation gateway	Stopped
IBM Network Station Manager	Stopped
Network S[illegible]n	Started
Directory	Stopped

Figure 213. AS/400 Operations Navigator: Network Station login server

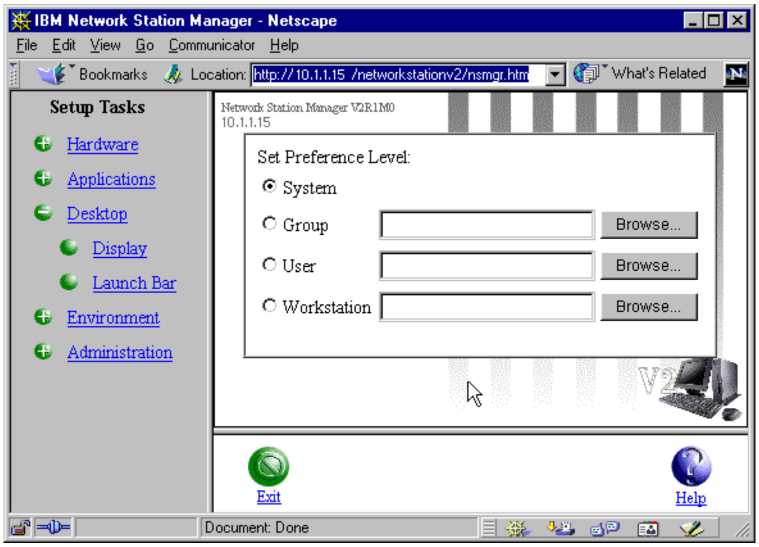
Managing the Network Station clients

The IBM Network Station Manager program is a browser-based application. This program allows the administrator to perform the setup and management tasks associated with the IBM Network Station Clients.

In the V2R1 Code of the IBM Network Station Manager, you can access the Manager Program with the following URL:

```
http://serverIPaddress/networkstationv2/admin
```

Once you sign on, the main display is presented as shown in Figure 214.



Set Preference Level:

● System

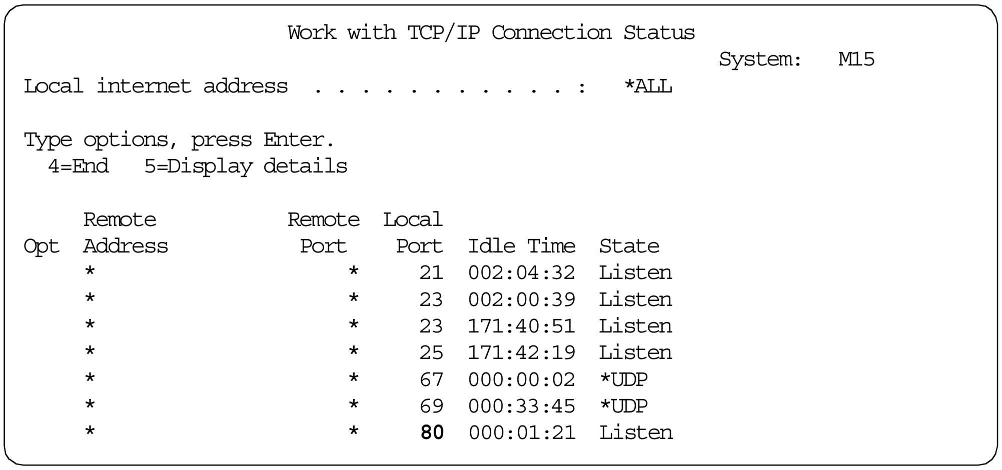
○ Group

○ User

○ Workstation

Figure 214. AS/400 Tasks page for V2R1 Network Station Manager

To successfully receive this page, you need to ensure that the DEFAULT server is running on your AS/400 system. You can check this with the AS/400 `NETSTAT *CNN.` command. The server runs on port 80. The resulting screen is shown in Figure 215 on page 250.



```
                       Work with TCP/IP Connection Status
                                                               System:   M15
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote  Local
Opt  Address           Port    Port  Idle Time  State
     *                    *      21  002:04:32  Listen
     *                    *      23  002:00:39  Listen
     *                    *      23  171:40:51  Listen
     *                    *      25  171:42:19  Listen
     *                    *      67  000:00:02  *UDP
     *                    *      69  000:33:45  *UDP
     *                    *      80  000:01:21  Listen
```

*Figure 215. AS/400 NETSTAT *CNN screen showing port 80*

The four Network Station clients in the scenarios are USER1, USER2, USER3, and USER4. Using both the V1R3 manager (see “Managing the Network Station clients” on page 223) and the V2R1 manager, the following 5250 autostart sessions are configured:

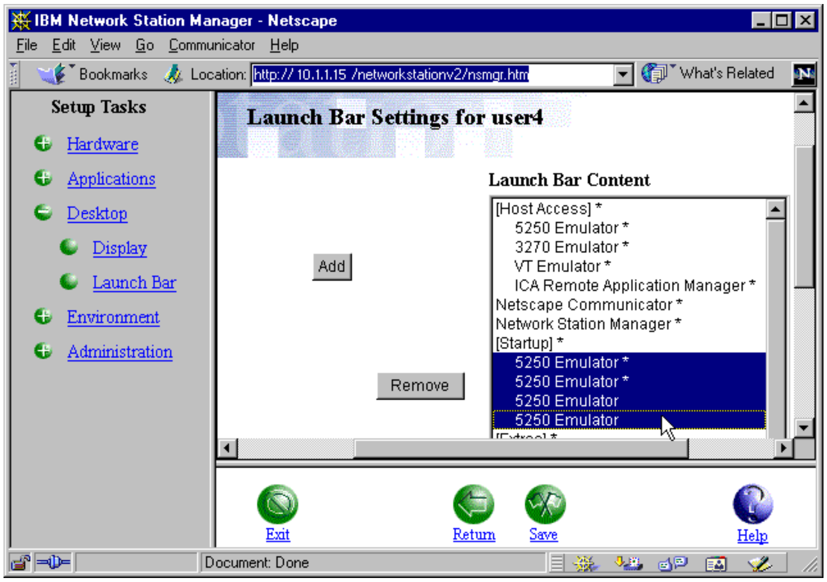
- **Global for V1R3 clients**: One session for system M15
- **USER1**: One session for system M15
- **USER2**: One session for system M01
- **USER3**: One session for M15 and one session for M01
- **Global for V2R1 clients**: One session for system M15 and M01
- **USER4**: One session for M15 and one session for M01

Information for using the V1R3 IBM Network Station Manager program can be found in *IBM Network Station Manager Installation and Use*, SC41-0664.

Information for using the V2R1 IBM Network Station Manager program can be found in *Using IBM Network Station Manager V2R1*, SC41-0690. We show a few key screens here.

On the main panel of the Manager program, the Preference Level is set to `user`. The user name (in this case USER4) is typed into the field. On the left side of the panel, click **Desktop->Launch Bar**. On the next panel, you can see what is configured in the Startup folder located in the Launch Bar Content window.

For USER4, there are four 5250 Emulator entries. The first two entries (shown with an *) are a System-level preference, while the remaining two entries are User-level preferences. This page is shown in Figure 216.



Launch Bar Settings for user4

Launch Bar Content

```
[Host Access] *
    5250 Emulator *
    3270 Emulator *
    VT Emulator *
    ICA Remote Application Manager *
Netscape Communicator *
Network Station Manager *
[Startup] *
    5250 Emulator *
    5250 Emulator *
    5250 Emulator
    5250 Emulator
[Extras] *
```

Figure 216. V2R1 Network Station Manager: User4 startup information

9.3.1 Scenario 4: V1R3 and V2R1 clients using NVRAM and BOOTP

This scenario shows an environment of two AS/400 systems and four Network Stations. This scenario is a continuation of 9.2.1, “Scenario 1: V1R3 clients using NVRAM and BOOTP” on page 224. In this scenario, IBM Network Station Model 2800 is introduced. Model 2800 is supported only under the V2R1 level of the IBM Network Station Manager. It will be required that both the V1R3 and V2R1 Network Station Manager levels are installed on the server system.

9.3.1.1 Scenario overview

This scenario shows an AS/400 system (M15) running V4R3M0 of OS/400. The AS/400 supports one of each of the following models of Network Station:

- **Network Station Series 100:** Token-Ring attached
- **Network Station Series 300:** Twinaxial attached
- **Network Station Series 1000:** Token-Ring attached
- **Network Station Series 2800:** Token-Ring attached

The 2800 model is supported only under the V2R1 Network Station Manager code. The remaining three models are currently supported under the V1R3 Network Station Manager code. Because not all of the models are supported under the same IBM Network Station Manager level, it will be necessary to have both code levels (V1R3 and V2R1) coexisting on the server system (M15).

9.3.1.2 Scenario Network configuration

Figure 217 on page 252 shows the network topology of the AS/400 systems and the attached Network Station clients. An internal LAN exists for the Token-Ring attached Network Station models, and a different network addressing scheme is used for the twinaxial subnet.

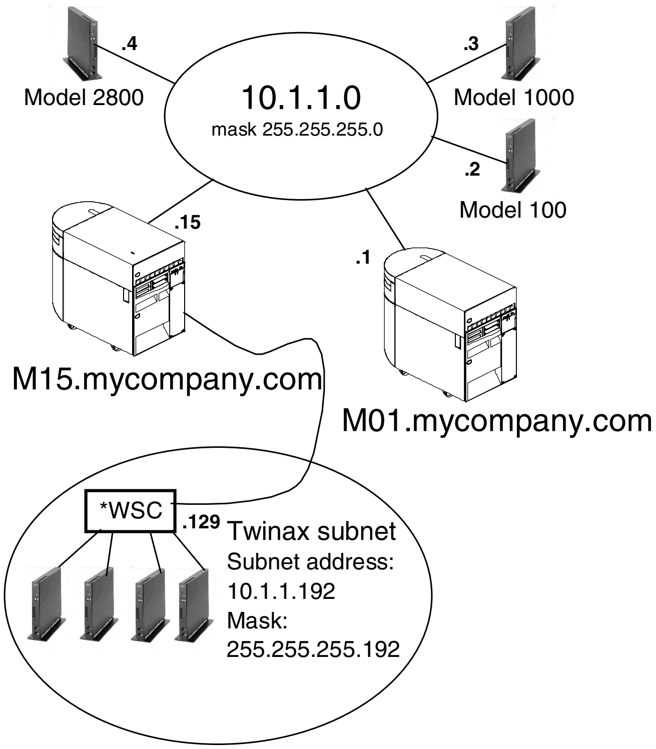


Figure 217. TCP/IP network topology for Scenario 4 and Scenario 5

The IP interfaces defined for this scenario are shown in Figure 218. The twinaxial network is a subnet of the main network 10.1.1.0.

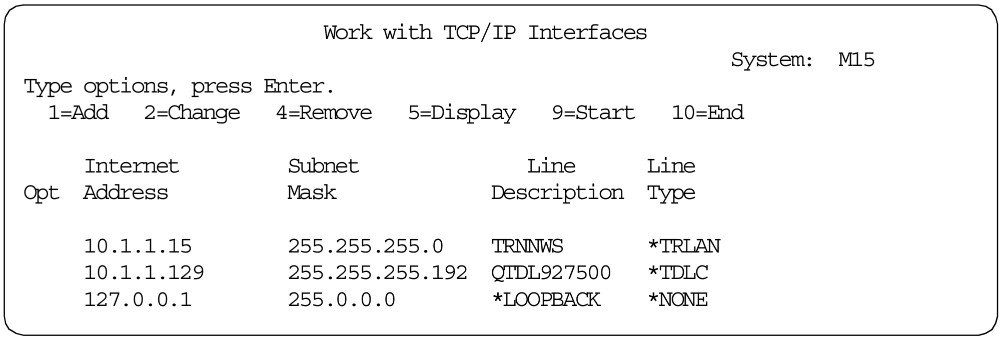

```
                            Work with TCP/IP Interfaces
                                                            System:  M15
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet              Line       Line
Opt  Address          Mask                Description Type

     10.1.1.15        255.255.255.0       TRNNWS      *TRLAN
     10.1.1.129       255.255.255.192     QTDL927500  *TDLC
     127.0.0.1        255.0.0.0           *LOOPBACK   *NONE
```

Figure 218. AS/400 Work with TCP/IP Interfaces screen

Attention

During the testing and verification of this scenario, a problem with BOOTP was encountered when the twinaxial subnet was configured in the range of 10.1.1.192 to 10.1.1.255. Since this range is part of the main 10.1.1.0 network, transparent subnet masking is used. The range included the 10.1.1.0 network broadcast address (10.1.1.255), which is where a problem was discovered. At this time, we recommend that you *do not* configure a transparent subnet that would include the network broadcast address. For our scenarios, we chose a twinaxial subnet of 10.1.1.129.

Further information on this problem can be found in Informational APAR II12070. You can order this information by using the following AS/400 command:

```
SNDPTFORD II12070
```

9.3.1.3 Network Station configuration

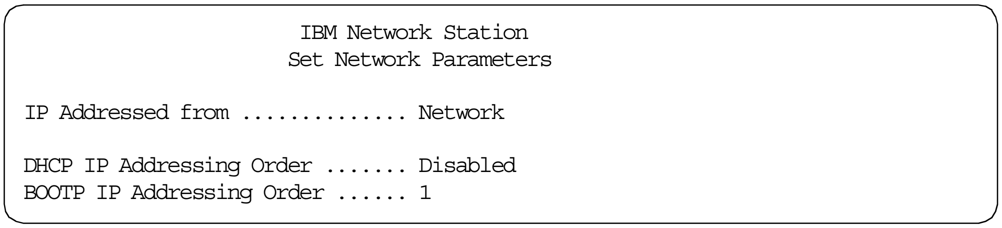
There are four IBM Network Stations used in this scenario. The Model 100 and Model 1000 use the BOOTP method for obtaining their IP address. The Model 341 and Model 2800 are using their NVRAM settings for obtaining an IP address.

Table 41 shows some of the IBM Network Station hardware specifications. The models shown are the ones being used in this scenario.

Table 41. IBM Network Station specifications

Network Station Model	Boot monitor version	Total DRAM memory	IP address
100	v3.0.7.6	16 MB	10.1.1.2
341 - Twinax	v3.0.7.2	32 MB	10.1.1.130
1000	v3.0.8.8	64 MB	10.1.1.3
2800	H2082090	64 MB	10.1.1.4

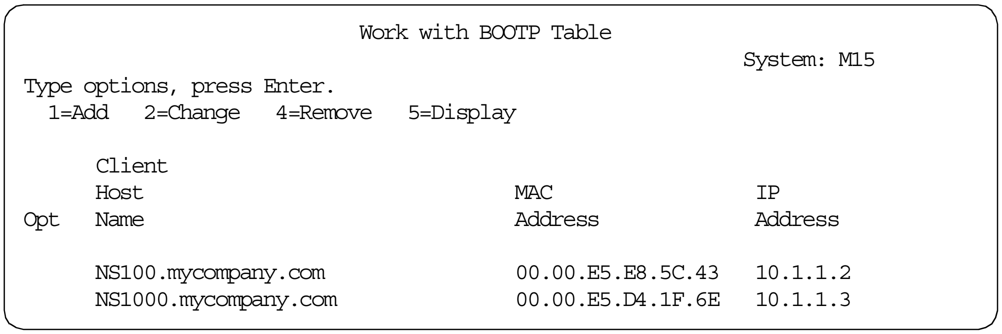
The configurations for Model 100 and Model 1000 are contained both on the Network Station and on the AS/400 system. The only configuration needed on the Network Station itself is in the Network Parameters. An example of this screen in shown in Figure 219.



```
                       IBM Network Station
                      Set Network Parameters

IP Addressed from .............. Network

DHCP IP Addressing Order ....... Disabled
BOOTP IP Addressing Order ...... 1
```

Figure 219. IBM Network Station: Network parameters for Model 1000 and Model 100

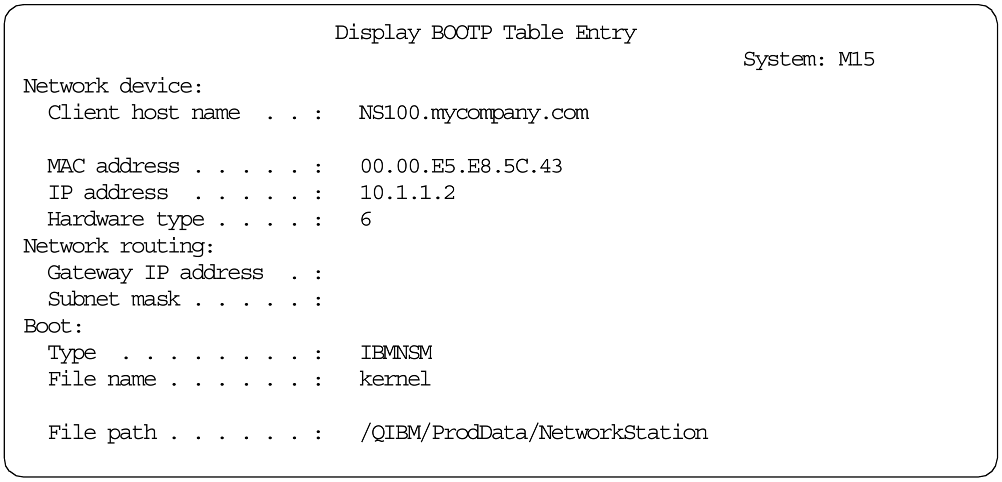
The remaining configuration screens on the Network Station do not need to be set. However, on the AS/400 system, you need to ensure that a BOOTP table entry exists for each Network Station. Figure 220 shows the output of the `WRKBPTBL` command on the AS/400 system.



```
                              Work with BOOTP Table
                                                            System:  M15
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

      Client
      Host                                 MAC                 IP
Opt   Name                                 Address             Address

      NS100.mycompany.com                  00.00.E5.E8.5C.43   10.1.1.2
      NS1000.mycompany.com                 00.00.E5.D4.1F.6E   10.1.1.3
```

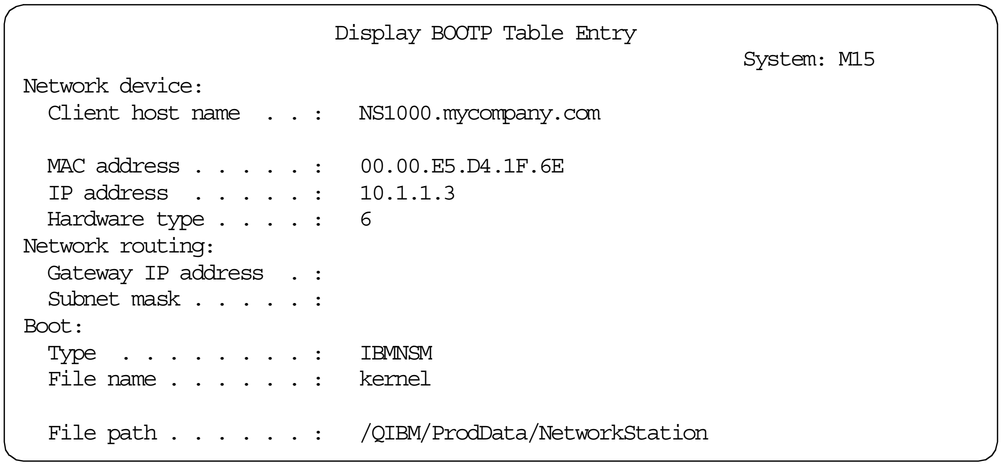
Figure 220. AS/400 Work with BOOTP Table entries screen

When option 5 is entered next to each client entry, the resulting information appears as shown in Figure 221 and Figure 222.



```
                            Display BOOTP Table Entry
                                                            System:  M15
Network device:
  Client host name  . . :   NS100.mycompany.com

  MAC address . . . . . :   00.00.E5.E8.5C.43
  IP address  . . . . . :   10.1.1.2
  Hardware type . . . . :   6
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . . . . :   IBMNSM
  File name . . . . . . :   kernel

  File path . . . . . . :   /QIBM/ProdData/NetworkStation
```

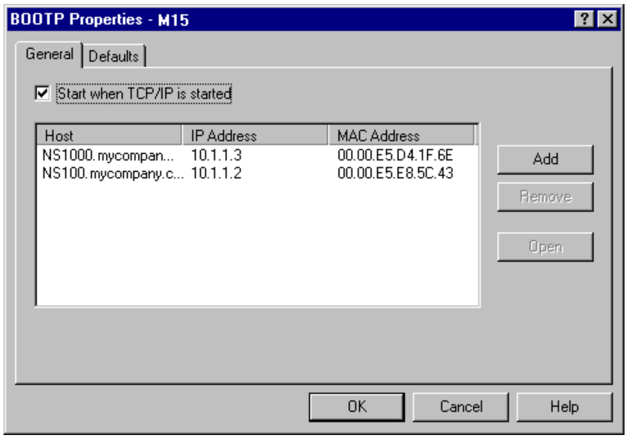
Figure 221. AS/400 BOOTP Table Entry for the Model 100 Network Station



```
                            Display BOOTP Table Entry
                                                            System:  M15
Network device:
  Client host name  . . :   NS1000.mycompany.com

  MAC address . . . . . :   00.00.E5.D4.1F.6E
  IP address  . . . . . :   10.1.1.3
  Hardware type . . . . :   6
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . . . . :   IBMNSM
  File name . . . . . . :   kernel

  File path . . . . . . :   /QIBM/ProdData/NetworkStation
```

Figure 222. AS/400 BOOTP Table Entry for the Model 1000 Network Station

These BOOTP entries can also be added/viewed in Operations Navigator. To do this, double-click **Network->Servers->TCP/IP**. A list of servers appears in the right-hand side of the display. Left-click the **BOOTP** entry. Right-click **Properties** from the pull-down menu and you see a window similar to the one shown in Figure 223.



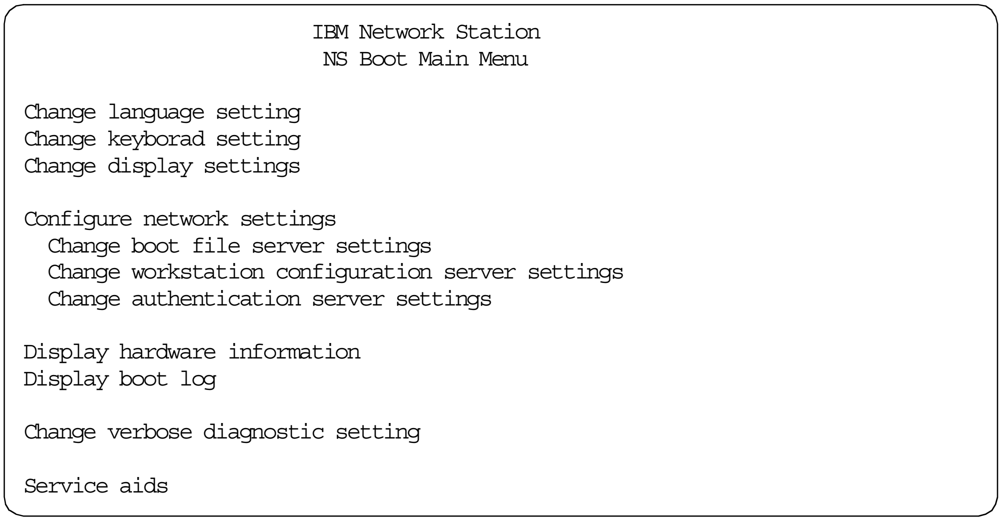
☑ Start when TCP/IP is started

Host	IP Address	MAC Address
NS1000.mycompan...	10.1.1.3	00.00.E5.D4.1F.6E
NS100.mycompany.c...	10.1.1.2	00.00.E5.E8.5C.43

Figure 223. AS/400 Operations Navigator: BOOTP properties

The configuration for Model 341 is contained in the NVRAM settings of the Network Station itself. There are minimal settings needed for Model 341 as shown in Figure 178 on page 229 through Figure 180 on page 229.

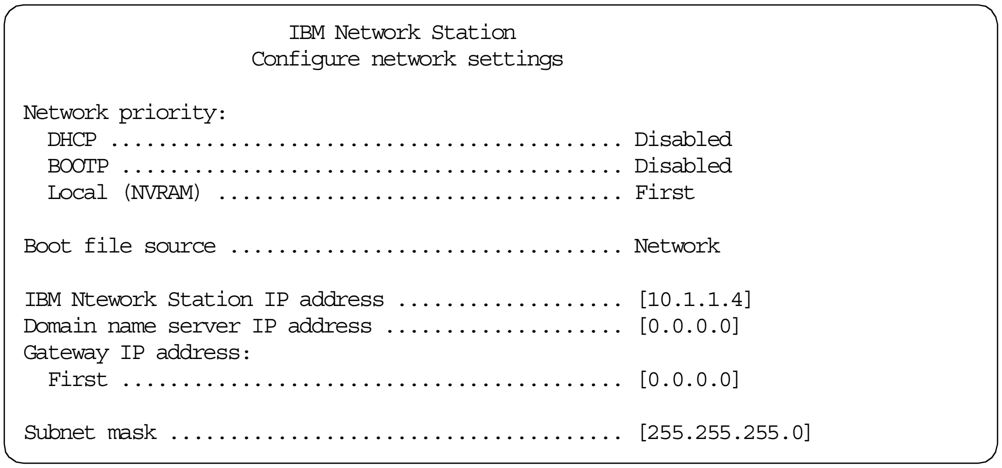
The configuration for Model 2800 is contained in the NVRAM settings of the Network Stations itself. There are a number of screens needed for this configuration. The main menu is shown in Figure 224. To configure this station for NVRAM, select **Configure network settings** on the main menu.



```
                          IBM Network Station
                           NS Boot Main Menu

Change language setting
Change keyborad setting
Change display settings

Configure network settings
  Change boot file server settings
  Change workstation configuration server settings
  Change authentication server settings

Display hardware information
Display boot log

Change verbose diagnostic setting

Service aids
```

Figure 224. IBM Network Station: Main menu for Model 2800

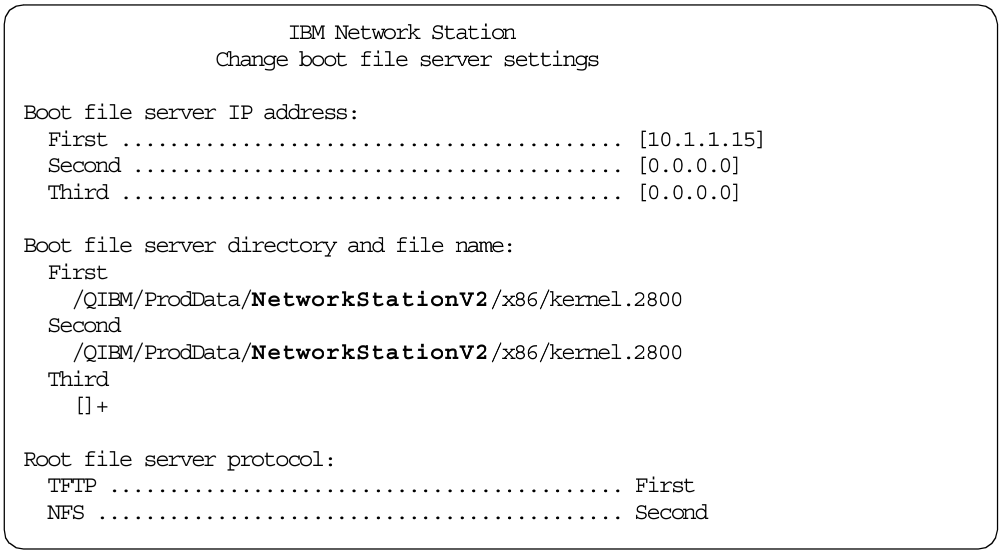
The next screen that is presented is the Configure network settings screen. Although the entire screen is not shown in Figure 225 on page 256, this example shows the important fields.



```
                     IBM Network Station
                  Configure network settings

Network priority:
  DHCP ......................................... Disabled
  BOOTP ........................................ Disabled
  Local (NVRAM) ................................ First

Boot file source ............................... Network

IBM Ntework Station IP address ................. [10.1.1.4]
Domain name server IP address .................. [0.0.0.0]
Gateway IP address:
  First ........................................ [0.0.0.0]

Subnet mask .................................... [255.255.255.0]
```

Figure 225. IBM Network Station: Configure network settings screen

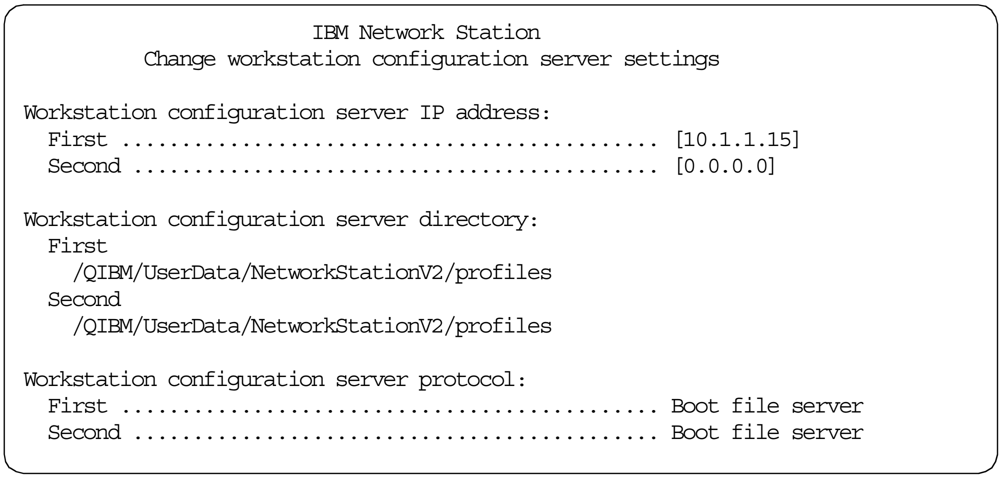
Once this screen has been completed, press Enter. The Change boot file server settings screen is displayed (Figure 226). Note the new file path for Model 2800.



```
                     IBM Network Station
               Change boot file server settings

Boot file server IP address:
  First ........................................ [10.1.1.15]
  Second ....................................... [0.0.0.0]
  Third ........................................ [0.0.0.0]

Boot file server directory and file name:
  First
    /QIBM/ProdData/NetworkStationV2/x86/kernel.2800
  Second
    /QIBM/ProdData/NetworkStationV2/x86/kernel.2800
  Third
    []+

Root file server protocol:
  TFTP ......................................... First
  NFS .......................................... Second
```

Figure 226. IBM Network Station: Change boot file server settings screen

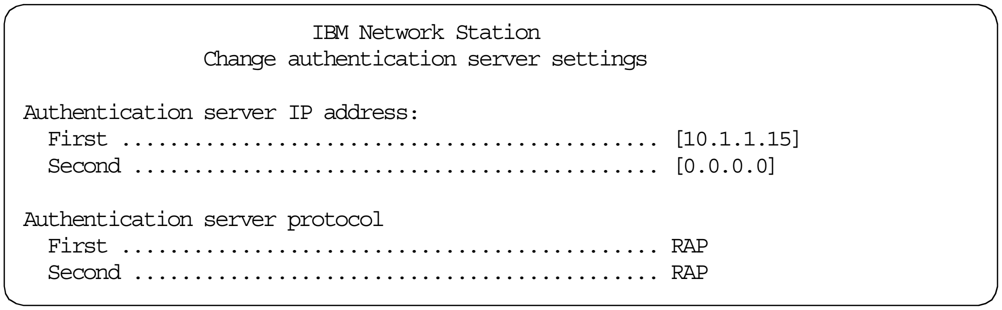
Once this screen has been completed, press Enter. The Change workstation configuration server settings screen is displayed (Figure 227). Here again, notice that the directory is changed from what the V1R3 IBM Network Station code used.



```
                         IBM Network Station
          Change workstation configuration server settings

Workstation configuration server IP address:
  First ........................................... [10.1.1.15]
  Second .......................................... [0.0.0.0]

Workstation configuration server directory:
  First
    /QIBM/UserData/NetworkStationV2/profiles
  Second
    /QIBM/UserData/NetworkStationV2/profiles

Workstation configuration server protocol:
  First ........................................... Boot file server
  Second .......................................... Boot file server
```

Figure 227. IBM Network Station: Change workstation configuration server settings screen

Once this screen has been completed, press Enter. The Change authentication server settings screen is displayed (Figure 228). There are only a few fields present on this screen. Once this screen is completed, press Enter. You return to the NS Boot Main Menu as shown in Figure 224 on page 255.



```
                         IBM Network Station
               Change authentication server settings

Authentication server IP address:
  First ........................................... [10.1.1.15]
  Second .......................................... [0.0.0.0]

Authentication server protocol
  First ........................................... RAP
  Second .......................................... RAP
```

Figure 228. IBM Network Station: Change authentication server settings screen

9.3.1.4 AS/400 requirements

With the addition of the V2R1 Network Station hardware model, the V2R1 IBM Network Station Manger code needs to be installed on the AS/400 system. After this step, the V2R1 Setup Wizard needs to be run. This wizard ensures the correct setup of the V2R1 hardware clients and that the correct servers are started on the AS/400 server system.

The V2R1 Setup Wizard is discussed in detail in 4.1, “AS/400 V2R1 installation: The basics” on page 83. For the addition of Model 2800 in this scenario, we cover a few of the Setup Wizard screens in this section.

Attention

Before running the V2R1 Setup Wizard, ensure that the V1R3 Network Station Login Server is ended. To do this, issue the AS/400 command:

```
CALL QYTC/QYTCUSVR ('ENDTCPSVR ')
```

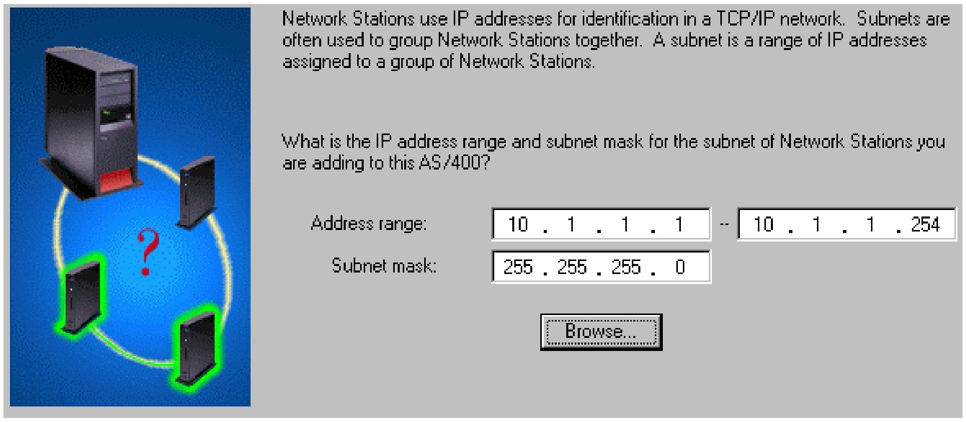
If this is not done, the Setup Wizard will not start the V2R1 Network Station Login Server. This can be corrected by manually ending the V1R3 server (as shown above) and then manually starting the V2R1 server with the following AS/400 command:

```
CALL QYTCV2/QYTCUSVR ('STRTCPSVR ')
```

Also be aware that the V2R1 Setup Wizard will end all of your HTTP instances. At the time this redbook was written, a PTF was not yet available for this problem. To ensure correct operation of the IBM Setup Wizard, ensure that you end all of the HTTP instances running on your system. Use the AS/400 command:

```
ENDTCPSVR *HTTP
```

The Model 2800 will be added to our existing 10.1.1.0 LAN. In the Setup Wizard, select the address range 10.1.1.1 to 10.1.1.254 (Figure 229). Once this range is chosen, click **Next**.



Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

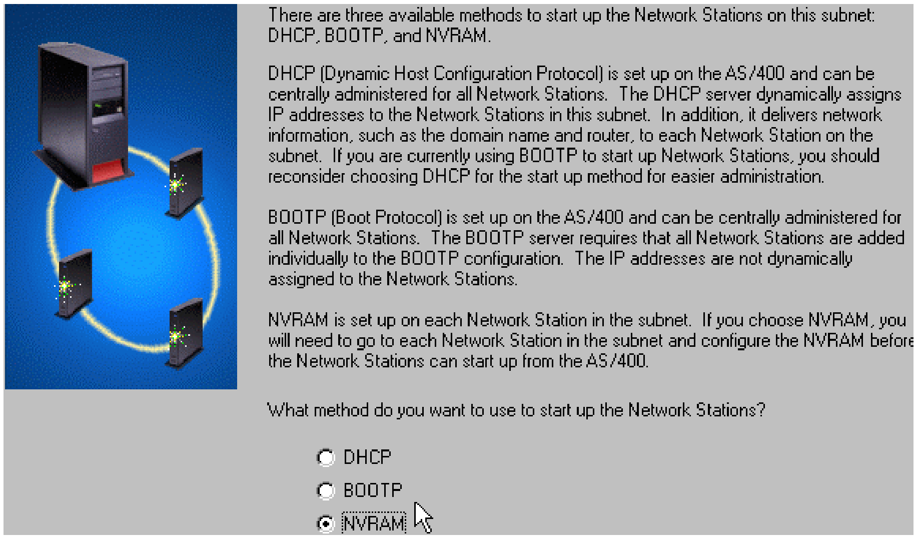
What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

Address range: 10 . 1 . 1 . 1 -- 10 . 1 . 1 . 254

Subnet mask: 255 . 255 . 255 . 0

Figure 229. AS/400 Setup Wizard: Choosing an IP address range

We have chosen to use the NVRAM method of booting for Model 2800. On the next display (Figure 230), choose the **NVRAM** method.



There are three available methods to start up the Network Stations on this subnet: DHCP, BOOTP, and NVRAM.

DHCP (Dynamic Host Configuration Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The DHCP server dynamically assigns IP addresses to the Network Stations in this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station on the subnet. If you are currently using BOOTP to start up Network Stations, you should reconsider choosing DHCP for the start up method for easier administration.

BOOTP (Boot Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The BOOTP server requires that all Network Stations are added individually to the BOOTP configuration. The IP addresses are not dynamically assigned to the Network Stations.

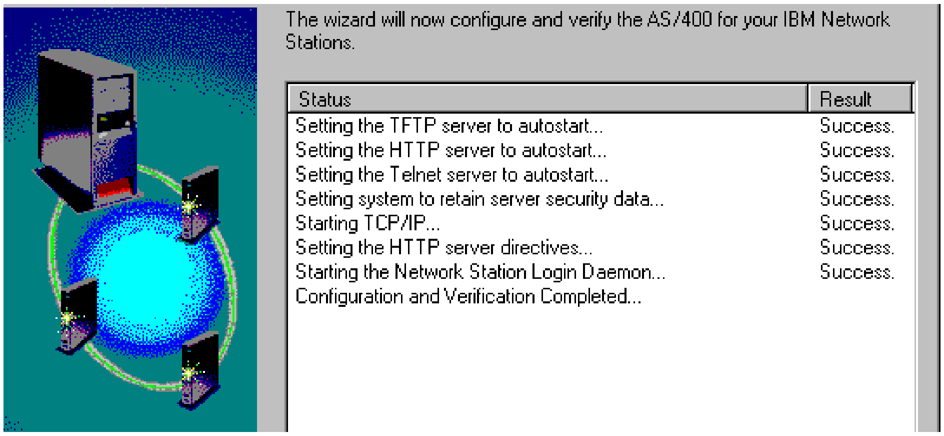
NVRAM is set up on each Network Station in the subnet. If you choose NVRAM, you will need to go to each Network Station in the subnet and configure the NVRAM before the Network Stations can start up from the AS/400.

What method do you want to use to start up the Network Stations?

○ DHCP
○ BOOTP
● NVRAM

Figure 230. AS/400 Setup Wizard: Choosing a boot method

Click **Next**. The next display shows is a listing of what the Setup Wizard will perform. Click **Finish**. The resulting display shown in Figure 231 appears.



The wizard will now configure and verify the AS/400 for your IBM Network Stations.

Status	Result
Setting the TFTP server to autostart...	Success.
Setting the HTTP server to autostart...	Success.
Setting the Telnet server to autostart...	Success.
Setting system to retain server security data...	Success.
Starting TCP/IP...	Success.
Setting the HTTP server directives...	Success.
Starting the Network Station Login Daemon...	Success.
Configuration and Verification Completed...	

Figure 231. AS/400 Setup Wizard: Configuration and verification

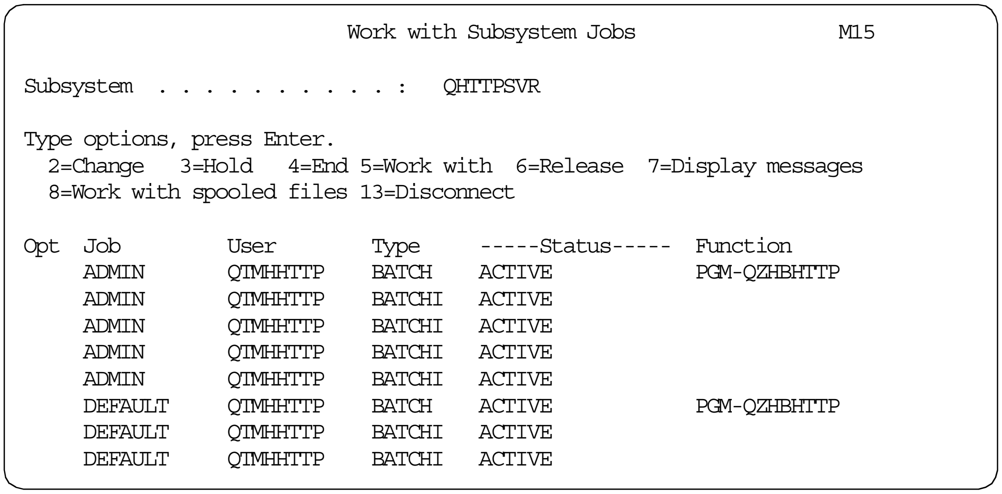
Click **Close** to return to the main Operations Navigator session.

In this scenario, it is necessary to have the TFTP and BOOTP servers started on the AS/400 server. After the boot-up process completes, a sign-on screen is present on all four client Network Stations. For each client user to sign on successfully, the Network Station Login Server needs to be started on port 256. This Login Server is the V2R1 server, which supports both V1R3 and V2R1 clients. When the authentication of each user is completed, the appropriate autostart programs will run on each client Network Station.

There are autostart 5250 sessions configured within the Network Station Managers. To access both of these managers, both the *Admin* and *Default* servers should be active on the AS/400 system. To verify this, issue the command

```
WRKSBSJOB QHTTPSVR
```

The resulting screen is shown in Figure 232.

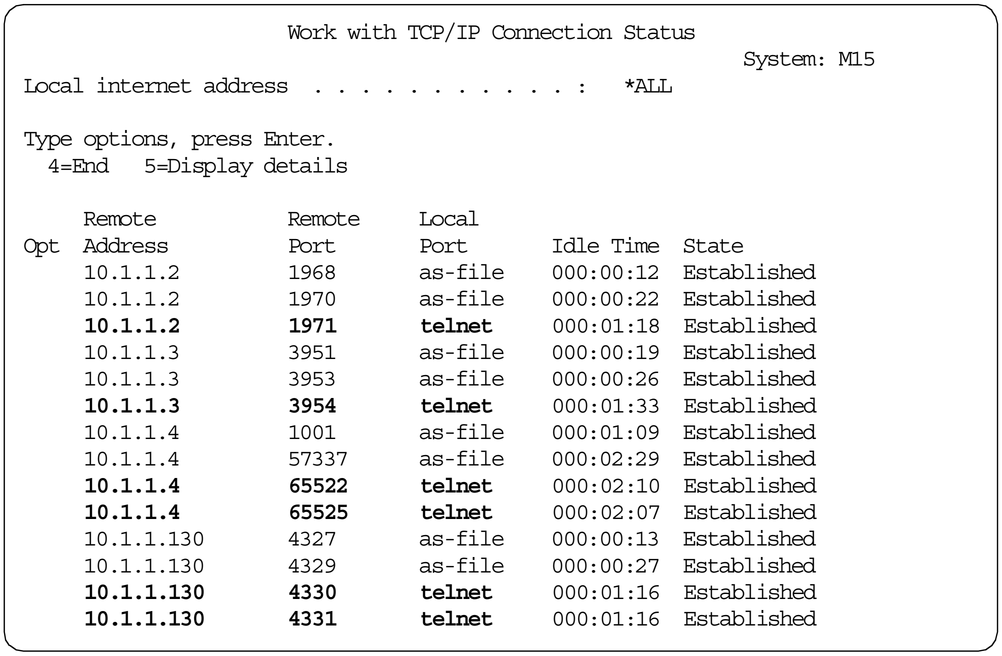


```
                             Work with Subsystem Jobs                M15

Subsystem  . . . . . . . . . . :   QHTTPSVR

Type options, press Enter.
  2=Change   3=Hold   4=End 5=Work with  6=Release  7=Display messages
  8=Work with spooled files 13=Disconnect

Opt  Job         User        Type     -----Status-----  Function
     ADMIN       QTMHHTTP    BATCH    ACTIVE            PGM-QZHBHTTP
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     DEFAULT     QTMHHTTP    BATCH    ACTIVE            PGM-QZHBHTTP
     DEFAULT     QTMHHTTP    BATCHI   ACTIVE
     DEFAULT     QTMHHTTP    BATCHI   ACTIVE
```

Figure 232. AS/400 Work with Subsystem Jobs for QHTTPSVR

9.3.1.5 Connectivity verification

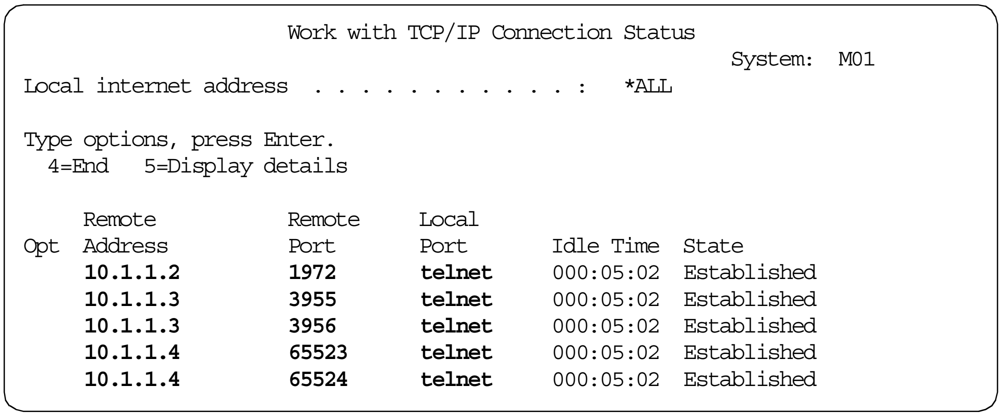
All four clients in this scenario have autostart 5250 sessions configured for the M15 system. To verify that these sessions are started, review the TCP/IP connection status screen on the M15 system by using the `NETSTAT *CNN` command. Figure 233 shows the 10.1.1.130 (twinaxial client) with two established sessions. Each of the LAN clients have any number of autostarted sessions.



```
                        Work with TCP/IP Connection Status
                                                             System: M15
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.2         1968       as-file    000:00:12  Established
     10.1.1.2         1970       as-file    000:00:22  Established
     10.1.1.2         1971       telnet     000:01:18  Established
     10.1.1.3         3951       as-file    000:00:19  Established
     10.1.1.3         3953       as-file    000:00:26  Established
     10.1.1.3         3954       telnet     000:01:33  Established
     10.1.1.4         1001       as-file    000:01:09  Established
     10.1.1.4         57337      as-file    000:02:29  Established
     10.1.1.4         65522      telnet     000:02:10  Established
     10.1.1.4         65525      telnet     000:02:07  Established
     10.1.1.130       4327       as-file    000:00:13  Established
     10.1.1.130       4329       as-file    000:00:27  Established
     10.1.1.130       4330       telnet     000:01:16  Established
     10.1.1.130       4331       telnet     000:01:16  Established
```

Figure 233. AS/400 TCP/IP connections: M15 system verification

The LAN-attached clients also have autostart 5250 sessions for the M01 system. Issuing the `NETSTAT *CNN` command on the M01 system shows us the established connections (Figure 234).



```
                       Work with TCP/IP Connection Status
                                                             System:  M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.2         1972       telnet     000:05:02  Established
     10.1.1.3         3955       telnet     000:05:02  Established
     10.1.1.3         3956       telnet     000:05:02  Established
     10.1.1.4         65523      telnet     000:05:02  Established
     10.1.1.4         65524      telnet     000:05:02  Established
```

Figure 234. AS/400 TCP/IP connections: M01 system verification

9.3.1.6 Summary

This scenario shows a network of two AS/400 systems and four IBM Network Station clients. One of the AS/400 systems (M15) is a boot server, which is set up to supply IP addresses to the IBM Network Station clients. There are both V1R3 and V2R1 hardware client environments and so both levels of the IBM Network Station Manager (V1R3 and V2R1) are installed on the system.

Different boot methods are used among the IBM Network Station clients and all are successful in booting and logging on to the M15 (server) system. All clients are successful in getting 5250 sessions established. Through the IBM Network Station Managers, different autostart values can be made for each individual Network Station user.

9.3.2 Scenario 5: V1R3 and V2R1 clients using BOOTP only

This scenario follows 9.3.1, “Scenario 4: V1R3 and V2R1 clients using NVRAM and BOOTP” on page 251. In this scenario, we move our NVRAM clients to BOOTP. This scenario shows the same LAN and twinaxial-attached IBM Network Stations. Again, both the V1R3 and V2R1 code of the Network Station Manager are used in this scenario.

9.3.2.1 Scenario overview

This scenario shows an AS/400 system (M15) running V4R3M0 of OS/400. The AS/400 system supports one of each of the following models of Network Station:

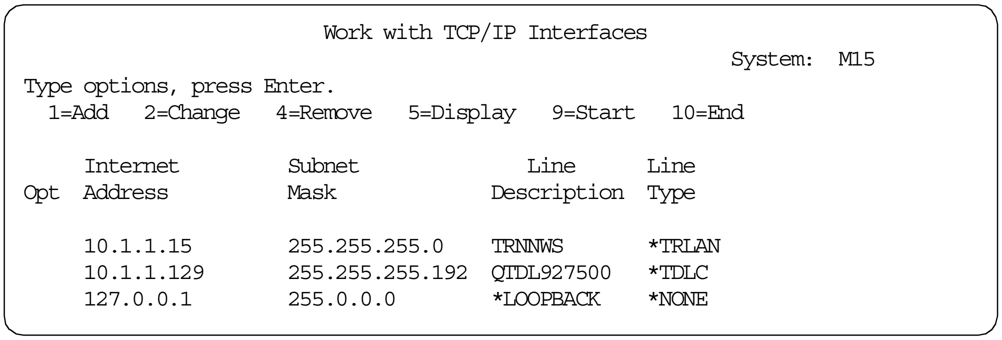
- **Network Station Series 100:** Token-Ring attached
- **Network Station Series 300:** Twinaxial attached
- **Network Station Series 1000:** Token-Ring attached
- **Network Station Series 2800:** Token-Ring attached

The Model 2800 is supported only under the V2R1 Network Station Manager code. The remaining three models currently are supported under the V1R3 Network Station Manager code. Because not all of the models are supported under the same IBM Network Station Manager level, it will be necessary to have both code levels (V1R3 and V2R1) coexisting on the server system (M15).

9.3.2.2 Scenario Network configuration

Figure 217 on page 252 shows the network topology of the AS/400 systems and the attached Network Station clients. An internal LAN exists for the Token-Ring attached Network Station models, and a different network addressing scheme is used for the twinaxial subnet.

The IP interfaces defined for this scenario are shown in Figure 235. The twinaxial network is a subnet of the main network 10.1.1.0.



```
                          Work with TCP/IP Interfaces
                                                                System:   M15
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line        Line
Opt  Address          Mask               Description Type

     10.1.1.15        255.255.255.0      TRNNWS      *TRLAN
     10.1.1.129       255.255.255.192    QTDL927500  *TDLC
     127.0.0.1        255.0.0.0          *LOOPBACK   *NONE
```

Figure 235. AS/400 Work with TCP/IP Interfaces screen

Attention

During the testing and verification of this scenario, a problem with BOOTP was encountered when the twinaxial subnet was configured in the range of 10.1.1.192 to 10.1.1.255. Because this range is part of the main 10.1.1.0 network, transparent subnet masking is used. The range included the 10.1.1.0 network broadcast address (10.1.1.255), which is where a problem was discovered. At this time, we recommend that you *do not* configure a transparent subnet that would include the network broadcast address. For our scenarios, we chose a twinaxial subnet of 10.1.1.129.

Further information on this problem can be found in Informational APAR II12070. You can order this information by using the following AS/400 command:

```
SNDPTFORD II12070
```

9.3.2.3 Network Station configuration

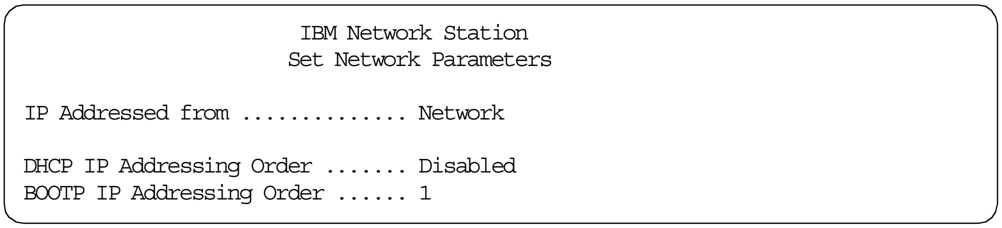
There are four IBM Network Stations used in this scenario. All models use the BOOTP method for obtaining their IP address.

Table 42 shows some of the IBM Network Station hardware specifications. The models shown are the ones that are used in this scenario

Table 42. IBM Network Station specifications

Network Station Model	Boot monitor version	Total DRAM memory	IP address
100	v3.0.7.6	16 MB	10.1.1.2
341 - Twinax	v3.0.7.2	32 MB	10.1.1.130
1000	v3.0.8.8	64 MB	10.1.1.3
2800	H2082090	64 MB	10.1.1.4

The configuration for the all the models is contained both on the Network Station and on the AS/400 system. The only configuration needed on the Network Station itself is in the Network Parameters. An example of the V1R3 clients configuration is shown in Figure 236.

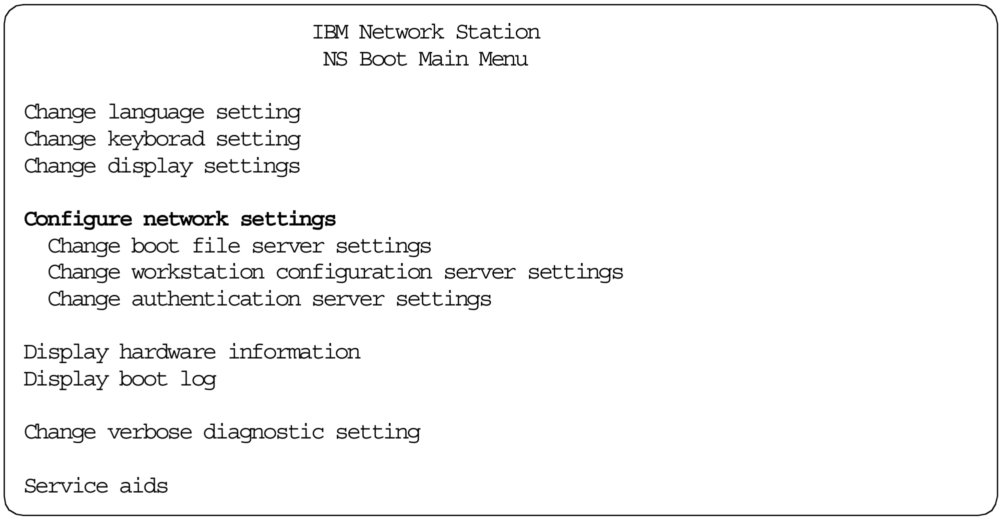


```
                        IBM Network Station
                      Set Network Parameters

IP Addressed from ............. Network

DHCP IP Addressing Order ....... Disabled
BOOTP IP Addressing Order ...... 1
```

Figure 236. IBM Network Station: Network parameters for Models 100, 341, and 1000

The remaining configuration screens on the V1R3 Network Station do not need to be set.

The configuration for Model 2800 is set in only two screens. The main menu is shown in Figure 237. To configure this station for BOOTP, select **Configure network settings** on the main menu.



```
                         IBM Network Station
                          NS Boot Main Menu

Change language setting
Change keyborad setting
Change display settings

Configure network settings
  Change boot file server settings
  Change workstation configuration server settings
  Change authentication server settings

Display hardware information
Display boot log

Change verbose diagnostic setting

Service aids
```

Figure 237. IBM Network Station: Main menu for Model 2800

The next screen that is presented is the Configure network settings screen (Figure 238 on page 264). Although the entire screen is not shown, you can see the important fields.

```
                    IBM Network Station
                 Configure network settings

Network priority:
  DHCP ........................................ Disabled
  BOOTP ....................................... First
  Local (NVRAM) ............................... Disabled

Boot file source .............................. Network

Domain name server IP address ................... [0.0.0.0]
```

Figure 238. IBM Network Station: Configure network settings screen

Once this screen is completed, press Enter. The Change boot file server settings screen is displayed (Figure 239).

```
                    IBM Network Station
              Change boot file server settings

Root file server protocol:
  TFTP ........................................ First
  NFS ......................................... Second
```

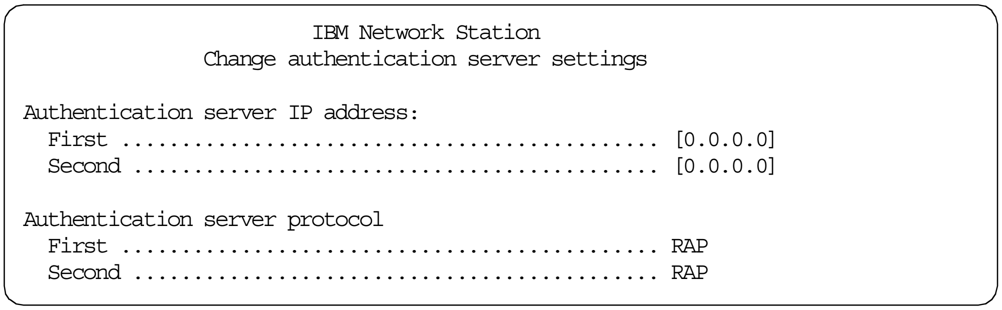
Figure 239. IBM Network Station: Change boot file server settings screen

Once this screen is completed, press Enter. The Change workstation configuration server settings screen is displayed (Figure 240). There is no configuration required here when using BOOTP.

```
                      IBM Network Station
          Change workstation configuration server settings

Workstation configuration server IP address:
  First ........................................... [0.0.0.0]
  Second .......................................... [0.0.0.0]

Workstation configuration server directory:
  First
    []+
  Second
    []+

Workstation configuration server protocol:
  First ........................................... Boot file server
  Second .......................................... Boot file server
```

Figure 240. IBM Network Station: Change workstation configuration server settings screen

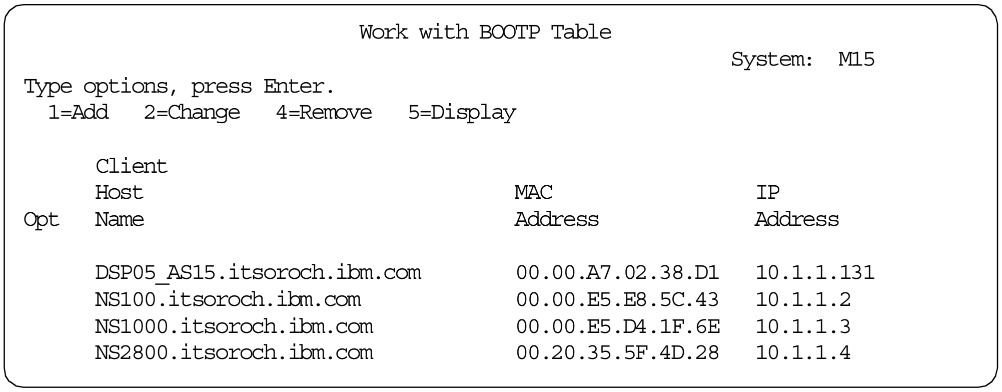
Once this screen is completed, press Enter. The Change authentication server settings screen is displayed (Figure 241). Again, for this scenario, this screen will not be needed. Once this screen is completed, press Enter. You return to the NS Boot Main Menu as shown in Figure 237 on page 263.



```
                         IBM Network Station
                 Change authentication server settings

Authentication server IP address:
  First .......................................... [0.0.0.0]
  Second ......................................... [0.0.0.0]

Authentication server protocol
  First .......................................... RAP
  Second ......................................... RAP
```

Figure 241. IBM Network Station: Change authentication server settings screen

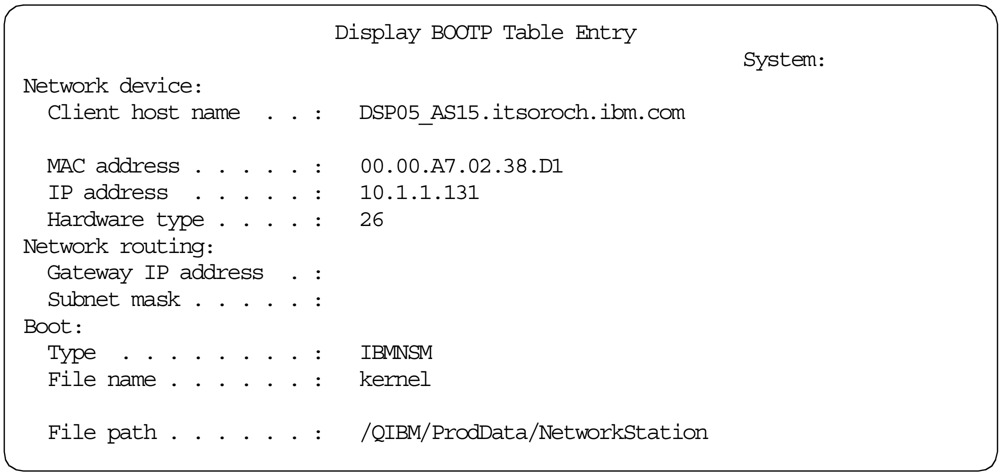
On the AS/400 system, you need to ensure that a BOOTP table entry exists for each Network Station. Figure 242 shows the output of the `WRKBPTBL` command on the AS/400 system.



```
                            Work with BOOTP Table
                                                         System:  M15
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

      Client
      Host                              MAC                 IP
Opt   Name                              Address             Address

      DSP05_AS15.itsoroch.ibm.com       00.00.A7.02.38.D1   10.1.1.131
      NS100.itsoroch.ibm.com            00.00.E5.E8.5C.43   10.1.1.2
      NS1000.itsoroch.ibm.com           00.00.E5.D4.1F.6E   10.1.1.3
      NS2800.itsoroch.ibm.com           00.20.35.5F.4D.28   10.1.1.4
```

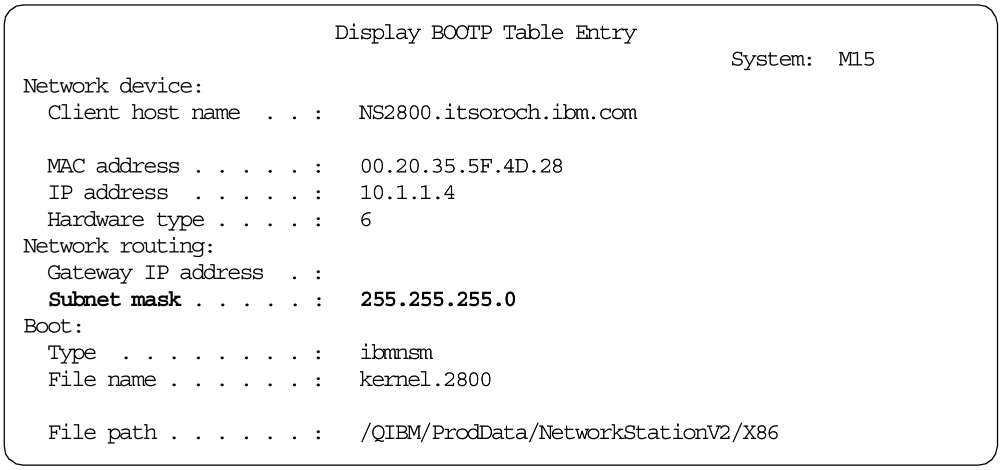
Figure 242. AS/400 Work with BOOTP Table entries

When option 5 is entered next to a client entry, the resulting information for the twinaxial client appears as shown in Figure 243. For the Model 2800, the entry is shown in Figure 244 on page 266. The information for Model 100 and Model 1000 is shown in Figure 221 on page 254 and Figure 222 on page 254 respectively.



```
                          Display BOOTP Table Entry
                                                          System:
Network device:
  Client host name  . . :   DSP05_AS15.itsoroch.ibm.com

  MAC address . . . . . :   00.00.A7.02.38.D1
  IP address  . . . . . :   10.1.1.131
  Hardware type . . . . :   26
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . . . . :   IBMNSM
  File name . . . . . . :   kernel

  File path . . . . . . :   /QIBM/ProdData/NetworkStation
```

Figure 243. AS/400 BOOTP Table Entry for Model 341 Network Station



```
                          Display BOOTP Table Entry
                                                            System:   M15
Network device:
  Client host name  . . :   NS2800.itsoroch.ibm.com

  MAC address . . . . . :   00.20.35.5F.4D.28
  IP address  . . . . . :   10.1.1.4
  Hardware type . . . . :   6
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :   255.255.255.0
Boot:
  Type  . . . . . . . . :   ibmnsm
  File name . . . . . . :   kernel.2800

  File path . . . . . . :   /QIBM/ProdData/NetworkStationV2/X86
```

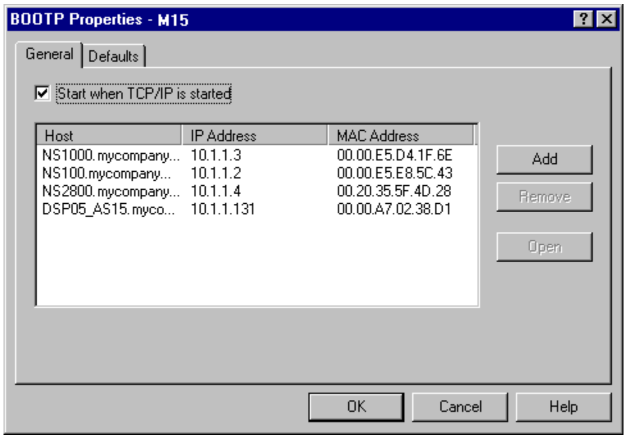
Figure 244. AS/400 BOOTP Table Entry for Model 2800 Network Station

The subnet mask is a *required* parameter for Model 2800. If this parameter is left blank, then the Network Station will fail to boot successfully. During our testing, the following message was posted on the Network Station:

```
NSB86509: Subnet mask not valid
```

This same parameter, in our scenario, is not needed for the V1R3 Network Station hardware models.

These BOOTP entries can also be added or viewed in Operations Navigator. To do this, double-click **Network->Servers->TCP/IP**. A list of servers appears in the right-hand side of the display. Left-click the **BOOTP** entry and a pull-down menu appears. Right-click **Properties**. Then, you see a window similar to the one shown in Figure 245.



☑ Start when TCP/IP is started

Host	IP Address	MAC Address
NS1000.mycompany...	10.1.1.3	00.00.E5.D4.1F.6E
NS100.mycompany...	10.1.1.2	00.00.E5.E8.5C.43
NS2800.mycompany...	10.1.1.4	00.20.35.5F.4D.28
DSP05_AS15.myco...	10.1.1.131	00.00.A7.02.38.D1

Figure 245. AS/400 Operations Navigator: BOOTP properties

9.3.2.4 AS/400 requirements

With the addition of the V2R1 Network Station hardware model, the V2R1 IBM Network Station Manger code needs to be installed on the AS/400 system. After this step, the V2R1 Setup Wizard needs to be run. This wizard ensures the correct setup of the V2R1 hardware clients and that the correct servers are started on the AS/400 server system.

The V2R1 Setup Wizard is discussed in detail in Chapter 4, “Installation and server setup” on page 83. For the addition of Model 2800 in this scenario, we cover a few of the Setup Wizard screens in this section.

Attention

Before running the V2R1 Setup Wizard, ensure that the V1R3 Network Station Login Server is ended. To do this, issue the AS/400 command:

```
CALL QYTC/QYTCUSVR ('ENDTCPSVR ')
```

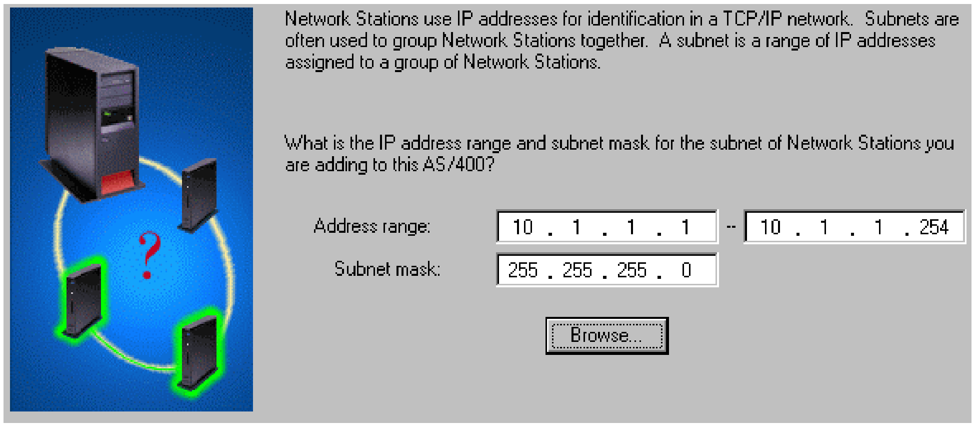
If this is not done, the Setup Wizard will not start the V2R1 Network Station Login Server. This can be corrected by manually ending the V1R3 server (as shown above) and then manually starting the V2R1 server with the following AS/400 command:

```
CALL QYTCV2/QYTCUSVR ('STRTCPSVR ')
```

Also be aware that the V2R1 Setup Wizard will end all of your HTTP instances. At the time this redbook was written, a PTF was not yet available for this problem. To ensure correct operation of the IBM Setup Wizard, ensure that you end all of the HTTP instances running on your system. The AS/400 command is:

```
ENDTCPSVR *HTTP
```

Model 2800 will be added to our existing 10.1.1.0 LAN. In the Setup Wizard, select the address range 10.1.1.1 to 10.1.1.254 as shown in Figure 246. Once this range is chosen, click **Next**.



Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

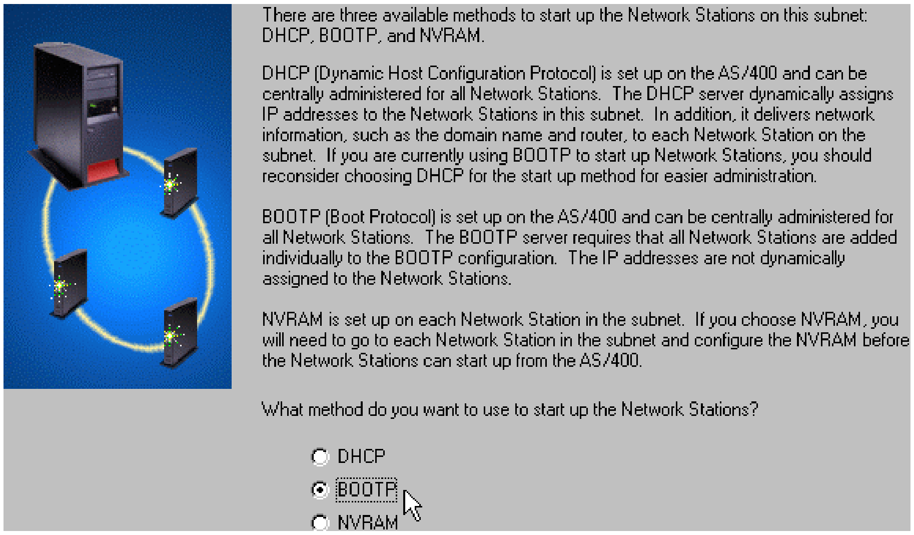
What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

Address range: 10 . 1 . 1 . 1 -- 10 . 1 . 1 . 254

Subnet mask: 255 . 255 . 255 . 0

Figure 246. AS/400 Setup Wizard: Choosing an IP address range

We have chosen to use the BOOTP method of booting for Model 2800. On the next display, select the **BOOTP** method (Figure 247 on page 268).



There are three available methods to start up the Network Stations on this subnet: DHCP, BOOTP, and NVRAM.

DHCP (Dynamic Host Configuration Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The DHCP server dynamically assigns IP addresses to the Network Stations in this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station on the subnet. If you are currently using BOOTP to start up Network Stations, you should reconsider choosing DHCP for the start up method for easier administration.

BOOTP (Boot Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The BOOTP server requires that all Network Stations are added individually to the BOOTP configuration. The IP addresses are not dynamically assigned to the Network Stations.

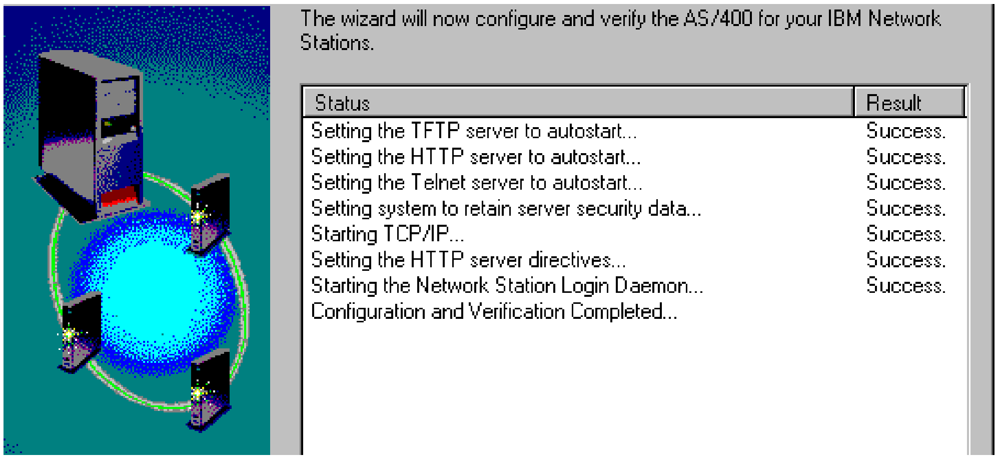
NVRAM is set up on each Network Station in the subnet. If you choose NVRAM, you will need to go to each Network Station in the subnet and configure the NVRAM before the Network Stations can start up from the AS/400.

What method do you want to use to start up the Network Stations?

○ DHCP
● BOOTP
○ NVRAM

Figure 247. AS/400 Setup Wizard: Choosing a boot method

Click **Next**. The next display shows a listing of what the Setup Wizard will perform. Click **Finish**. The resulting display appears as shown in Figure 248.



The wizard will now configure and verify the AS/400 for your IBM Network Stations.

Status	Result
Setting the TFTP server to autostart...	Success.
Setting the HTTP server to autostart...	Success.
Setting the Telnet server to autostart...	Success.
Setting system to retain server security data...	Success.
Starting TCP/IP...	Success.
Setting the HTTP server directives...	Success.
Starting the Network Station Login Daemon...	Success.
Configuration and Verification Completed...	

Figure 248. AS/400 Setup Wizard: Configuration and verification

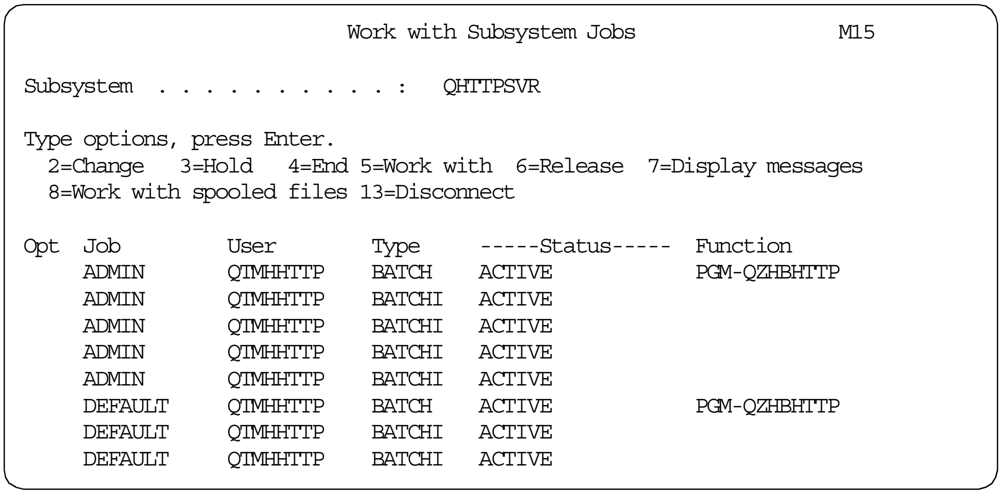
Click **Close** to return to the main Operations Navigator session.

In this scenario, it is necessary to have the TFTP and BOOTP servers started on the AS/400 server. After the boot-up process completes, a sign-on screen is present on all four client Network Stations. For each client user to sign on successfully, the Network Station Login Server needs to be started on port 256. This Login Server is the V2R1 server, which supports both V1R3 and V2R1 clients. When the authentication of each user is completed, the appropriate autostart programs will be run on each client Network Station.

There are autostart 5250 sessions configured within the Network Station Managers. To access both of these managers, both the *Admin* and *Default* servers should be active on the AS/400 system. To verify this, issue the command:

```
WRKSBSJOB QHTTPSVR
```

The resulting screen is shown in Figure 249.

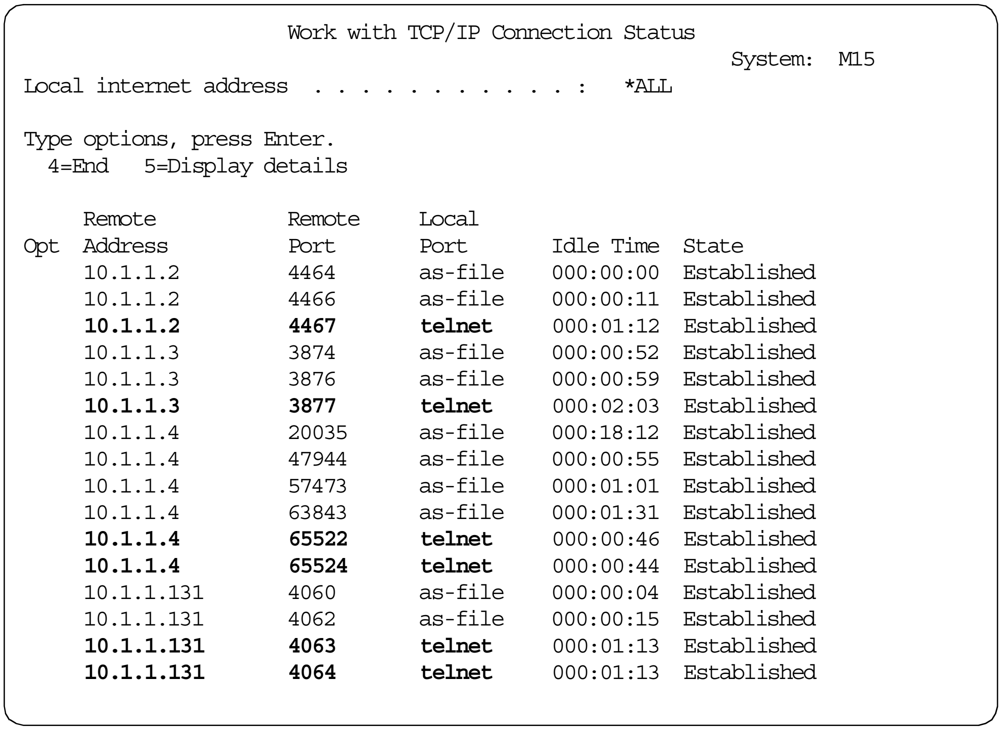


```
                           Work with Subsystem Jobs                M15

Subsystem  . . . . . . . . . . :   QHTTPSVR

Type options, press Enter.
  2=Change   3=Hold   4=End 5=Work with  6=Release  7=Display messages
  8=Work with spooled files 13=Disconnect

Opt  Job         User        Type     -----Status-----  Function
     ADMIN       QTMHHTTP    BATCH    ACTIVE            PGM-QZHBHTTP
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     ADMIN       QTMHHTTP    BATCHI   ACTIVE
     DEFAULT     QTMHHTTP    BATCH    ACTIVE            PGM-QZHBHTTP
     DEFAULT     QTMHHTTP    BATCHI   ACTIVE
     DEFAULT     QTMHHTTP    BATCHI   ACTIVE
```

Figure 249. AS/400 Work with Subsystem Jobs for QHTTPSVR

9.3.2.5 Connectivity verification

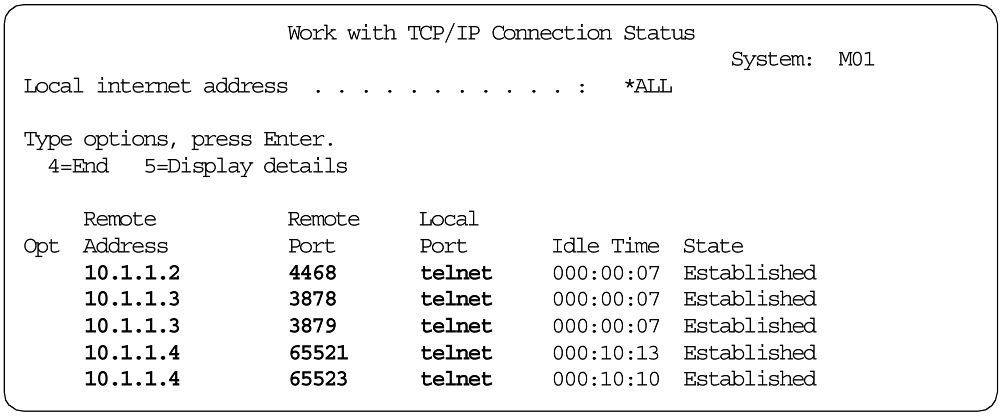
All four clients in this scenario have autostart 5250 sessions configured for the M15 system. To verify that these sessions are started, review the TCP/IP connection status screen on the M15 system by using the `NETSTAT *CNN` command. Figure 250 shows that the 10.1.1.131 (twinaxial client) has two established sessions, and each of the LAN clients have any number of autostarted sessions.



```
                      Work with TCP/IP Connection Status
                                                            System:  M15
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.2         4464       as-file    000:00:00  Established
     10.1.1.2         4466       as-file    000:00:11  Established
     10.1.1.2         4467       telnet     000:01:12  Established
     10.1.1.3         3874       as-file    000:00:52  Established
     10.1.1.3         3876       as-file    000:00:59  Established
     10.1.1.3         3877       telnet     000:02:03  Established
     10.1.1.4         20035      as-file    000:18:12  Established
     10.1.1.4         47944      as-file    000:00:55  Established
     10.1.1.4         57473      as-file    000:01:01  Established
     10.1.1.4         63843      as-file    000:01:31  Established
     10.1.1.4         65522      telnet     000:00:46  Established
     10.1.1.4         65524      telnet     000:00:44  Established
     10.1.1.131       4060       as-file    000:00:04  Established
     10.1.1.131       4062       as-file    000:00:15  Established
     10.1.1.131       4063       telnet     000:01:13  Established
     10.1.1.131       4064       telnet     000:01:13  Established
```

Figure 250. AS/400 TCP/IP connections: M15 system verification

The LAN-attached clients also have autostart 5250 sessions for the M01 system. Issuing the `NETSTAT *CNN` command on the M01 system shows the established connections (Figure 251).



```
                        Work with TCP/IP Connection Status
                                                              System:   M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.2         4468       telnet     000:00:07  Established
     10.1.1.3         3878       telnet     000:00:07  Established
     10.1.1.3         3879       telnet     000:00:07  Established
     10.1.1.4         65521      telnet     000:10:13  Established
     10.1.1.4         65523      telnet     000:10:10  Established
```

Figure 251. AS/400 TCP/IP connections: M01 system verification

9.3.2.6 Summary

This scenario shows a network of two AS/400 systems and four IBM Network Station clients. One of the AS/400 systems (M15) is a boot server, and is set up to supply IP addresses to the IBM Network Station clients. There are both V1R3 and V2R1 hardware clients environment, so both levels of the IBM Network Station Manager (V1R3 and V2R1) are installed on the system.

Only the BOOTP method is used among the IBM Network Station clients and all are successful in booting and logging on to the M15 (server) system. All clients are successful in getting 5250 sessions established. Through the IBM Network Station Managers, different autostart values can be made for each individual Network Station user.

9.3.3 Scenario 6: V1R3 and V2R1 clients using DHCP

This scenario is similar to 9.3.2, “Scenario 5: V1R3 and V2R1 clients using BOOTP only” on page 261. In some environments, DHCP may be used instead of BOOTP. This scenario shows the same LAN and twinaxial-attached IBM Network Stations. Because there is a mixture of both V1R3 and V2R1 hardware models in the network, both Network Station Manager code levels are required in this scenario.

9.3.3.1 Scenario overview

This scenario shows an AS/400 system (M15) running V4R3M0 of OS/400. The AS/400 system supports one of each of the following models of Network Station:

- **Network Station Series 100:** Token-Ring attached
- **Network Station Series 300:** Twinaxial attached
- **Network Station Series 1000:** Token-Ring attached
- **Network Station Series 2800:** Token-Ring attached

The Model 2800 is supported only under the V2R1 Network Station Manager code. The remaining three models are currently supported under the V1R3 Network Station Manager code. Because not all of the models are supported under the same IBM Network Station Manager level, it will be necessary for both code levels (V1R3 and V2R1) to coexist on the server system (M15).

9.3.3.2 Scenario Network configuration

Figure 252 shows the network topology of the AS/400 systems and the attached Network Station clients. An internal LAN exists for the Token-Ring attached Network Station models, and a different network addressing scheme is used for the twinaxial subnet.

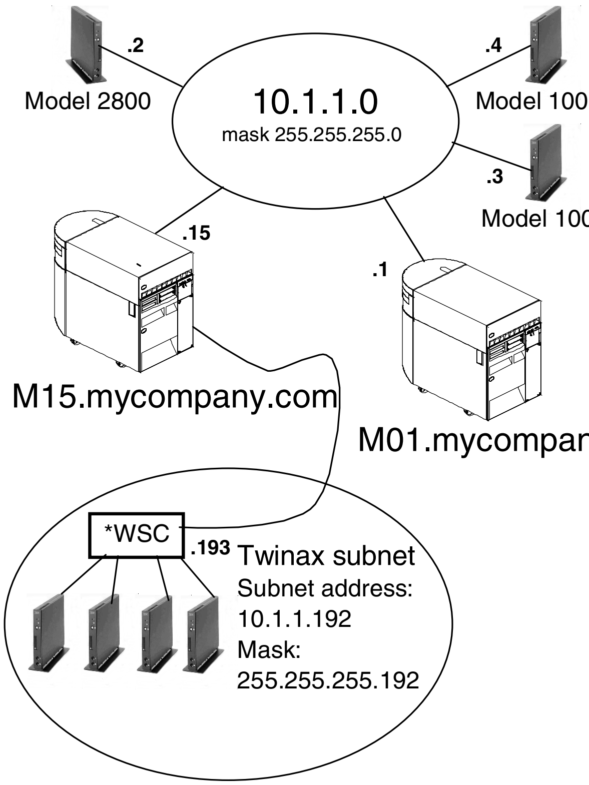
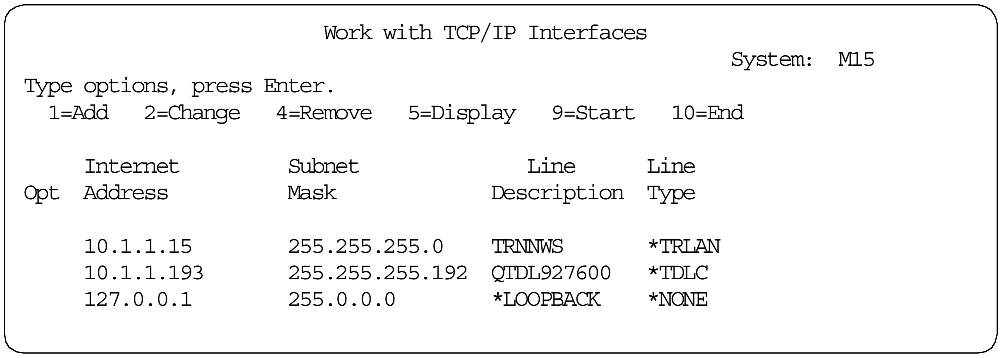


Figure 252. TCP/IP network topology

The IP interfaces defined for this scenario are shown in Figure 253. The twinaxial network is a subnet of the main network 10.1.1.0.



```
                          Work with TCP/IP Interfaces
                                                           System:  M15
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet           Line        Line
Opt  Address          Mask             Description Type

     10.1.1.15        255.255.255.0    TRNNWS      *TRLAN
     10.1.1.193       255.255.255.192  QTDL927600  *TDLC
     127.0.0.1        255.0.0.0        *LOOPBACK   *NONE
```

Figure 253. AS/400 Work with TCP/IP Interfaces screen

The twinaxial subnet range is from 10.1.1.192 to 10.1.1.255. This gives the subnet 61 available addresses.

9.3.3.3 Network Station configuration

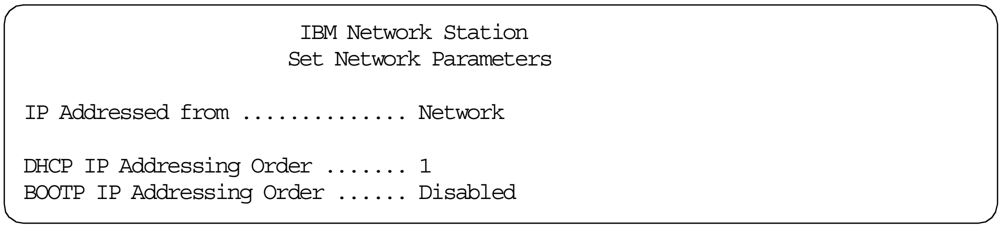
There are four IBM Network Stations used in this scenario. All models are using the DHCP method for obtaining their IP address.

Table 43 shows some of the IBM Network Station hardware specifications. The models shown are the ones that are used in this scenario.

Table 43. IBM Network Station specifications: Scenario 6

Network Station Model	Boot monitor version	Total DRAM memory	IP address
100	v3.0.7.6	16 MB	10.1.1.2
341 - Twinax	v3.0.7.2	32 MB	10.1.1.194
1000	v3.0.8.8	64 MB	10.1.1.3
2800	H2082090	64 MB	10.1.1.4

The configuration for all the models is contained both on the Network Station and on the AS/400 system. The only configuration needed on the Network Station is in the Network Parameters. An example of the V1R3 clients configuration is shown in Figure 254.

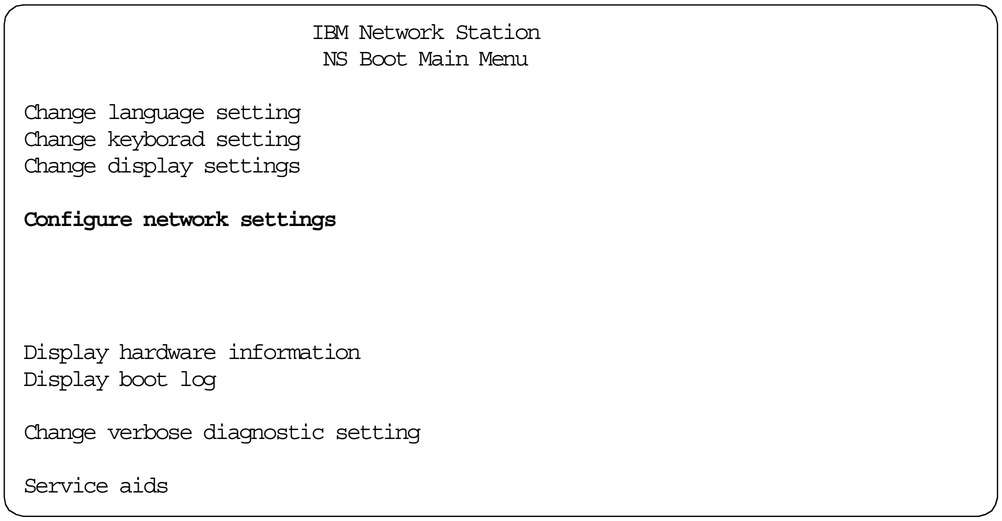


```
                         IBM Network Station
                       Set Network Parameters

IP Addressed from ............. Network

DHCP IP Addressing Order ....... 1
BOOTP IP Addressing Order ...... Disabled
```

Figure 254. IBM Network Station: Network parameters for Models 100, 341, and 1000

The remaining configuration screens on the V1R3 Network Station do not need to be set.

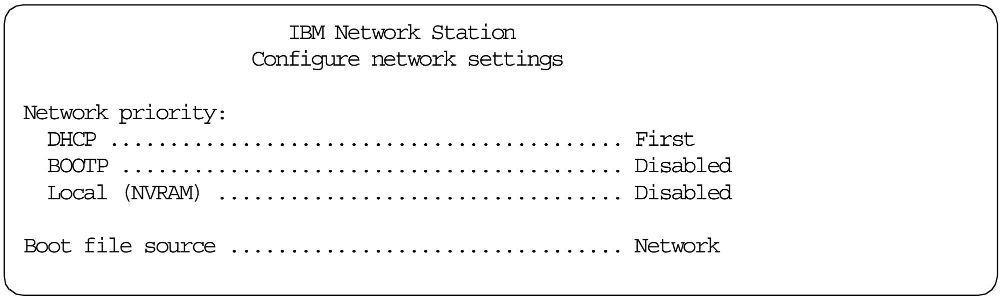
The configuration for the Model 2800 is set in only one screen. The main menu is shown in Figure 255. To configure this station for DHCP, select **Configure network settings** on this main menu.



```
                         IBM Network Station
                         NS Boot Main Menu

Change language setting
Change keyborad setting
Change display settings

Configure network settings




Display hardware information
Display boot log

Change verbose diagnostic setting

Service aids
```

Figure 255. IBM Network Station: Main menu for Model 2800

The next screen that is presented is the Configure network settings screen (Figure 256). Although the entire screen is not shown here, you can see the important fields.

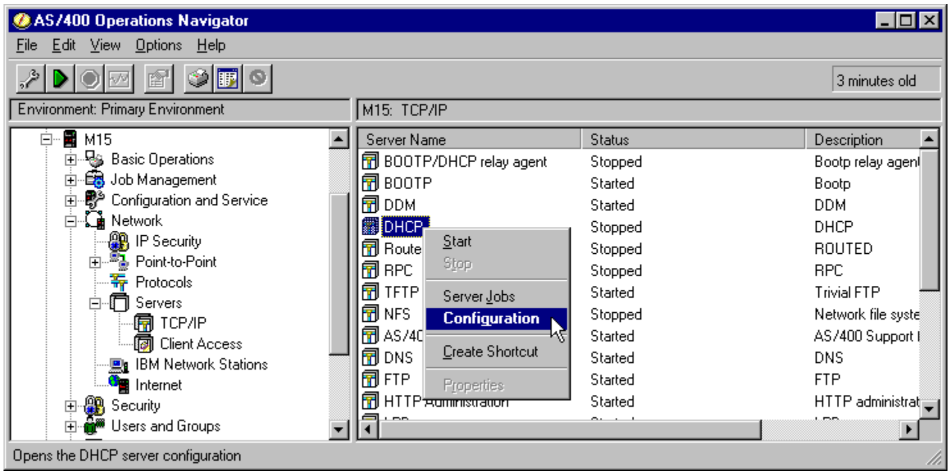


```
                       IBM Network Station
                   Configure network settings

Network priority:
  DHCP ......................................... First
  BOOTP ........................................ Disabled
  Local (NVRAM) ................................ Disabled

Boot file source ............................... Network
```

Figure 256. IBM Network Station: Configure network settings screen

Once this screen is completed, press Enter. You are returned to the NS Boot Main Menu as shown in Figure 255.

The remaining configuration for these DHCP clients is contained in the DHCP server properties. You can access this server in Operations Navigator. When you are in Operations Navigator, double-click **Network->Servers->TCP/IP**. A list of the TCP/IP servers is shown on the right-hand side of the display. Left-click the **DHCP** server. A similar display appears as shown in Figure 257 on page 274.



Server Name	Status	Description
BOOTP/DHCP relay agent	Stopped	Bootp relay agent
BOOTP	Started	Bootp
DDM	Started	DDM
DHCP	Stopped	DHCP
Route	Stopped	ROUTED
RPC	Stopped	RPC
TFTP	Started	Trivial FTP
NFS	Stopped	Network file syste
AS/40	Started	AS/400 Support I
DNS	Started	DNS
FTP	Started	FTP
HTTP Administration	Started	HTTP administrat

Opens the DHCP server configuration

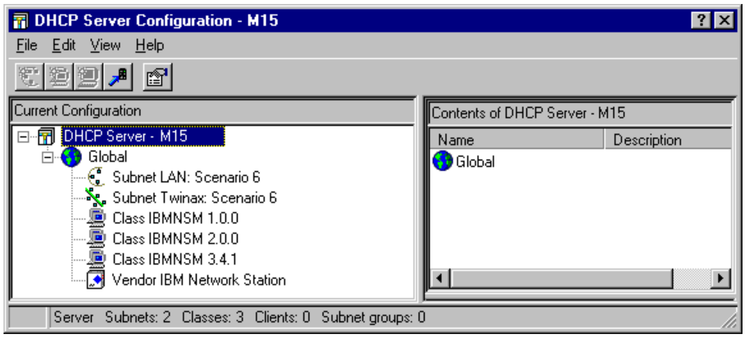
Figure 257. AS/400 Operations Navigator: DHCP server

Note

The configuration of DHCP on the AS/400 system, is beyond the scope of this redbook. More detailed information can be found in *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, and *IBM Network Station Manager Installation and Use*, SC41-0664.

In this scenario, we add a Model 2800 Network Station to an existing DHCP configuration.

Select **Configuration** as shown in Figure 257. Then, the configured subnets and classes for the DHCP server are shown (Figure 258).



Name	Description
Global	

Server Subnets: 2 Classes: 3 Clients: 0 Subnet groups: 0

Figure 258. AS/400 Operations Navigator: DHCP configuration

9.3.3.4 AS/400 requirements

For this scenario, there are two subnets already defined within DHCP. The first subnet is for the LAN-attached devices, and the second one is for the twinaxial-attached devices.

With the addition of the V2R1 Network Station hardware model, the V2R1 IBM Network Station Manger code needs to be installed on the AS/400 system. After this step, the V2R1 Setup Wizard needs to be run. This wizard ensures the correct setup of the V2R1 hardware clients and that the correct servers are started on the AS/400 server system.

The V2R1 Setup Wizard is discussed in detail in Chapter 4, “Installation and server setup” on page 83. For the addition of Model 2800 in this scenario, we cover a few Setup Wizard screens in this section.

Attention

Before running the V2R1 Setup Wizard, ensure that the V1R3 Network Station Login Server is ended. To do this, issue the AS/400 command:

```
CALL QYTC/QYTCUSVR ('ENDTCPSVR ')
```

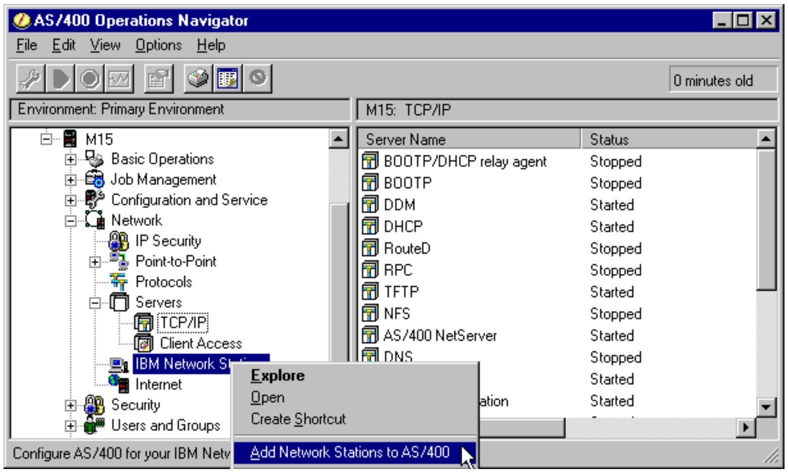
If this is not done, the Setup Wizard will not start the V2R1 Network Station Login Server. This can be corrected by manually ending the V1R3 server (as shown above) and then manually starting the V2R1 server with the following AS/400 command:

```
CALL QYTCV2/QYTCUSVR ('STRTCPSVR ')
```

Also be aware that the V2R1 Setup Wizard will end all of your HTTP instances. At the time this redbook was written a PTF was not yet available for this problem. To ensure correct operation of the IBM Setup Wizard, ensure that you end all of the HTTP instances running on your system. The AS/400 command is:

```
ENDTCPSVR *HTTP
```

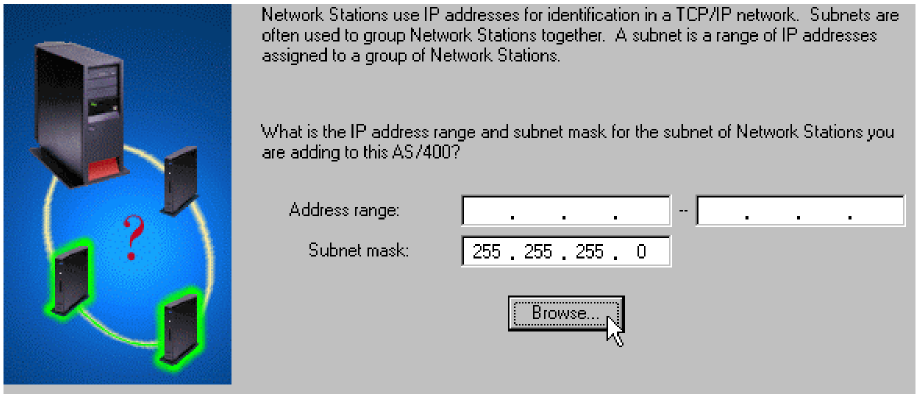
The Model 2800 will be added to our existing 10.1.1.0 LAN. To start the Setup Wizard, right-click **IBM Network Stations**, as shown in Figure 259. Select **Add Network Stations to AS/400**.



Server Name	Status
BOOTP/DHCP relay agent	Stopped
BOOTP	Stopped
DDM	Started
DHCP	Started
RouteD	Stopped
RPC	Stopped
TFTP	Started
NFS	Stopped
AS/400 NetServer	Started
DNS	Stopped
	Started
ation	Started

Figure 259. AS/400 Operations Navigator: Starting Network Station Wizard

Figure 260 on page 276 shows one of the initial screens seen in the Wizard. Click the **Browse** button to see what available IP address ranges are available on your system.



Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

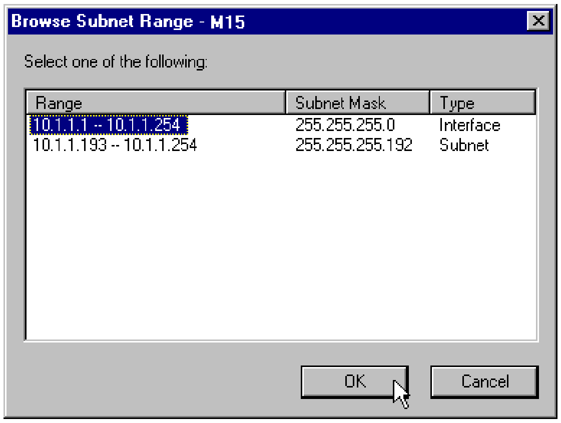
What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

Address range: . . . -- . . .

Subnet mask: 255 . 255 . 255 . 0

Figure 260. AS/400 Setup Wizard: Browsing IP address range

The existing IP ranges are shown in Figure 261. The first range listed is for the LAN-attached devices, and the second range listed is for the twinaxial-attached devices. Select he first address range, and click **OK**.



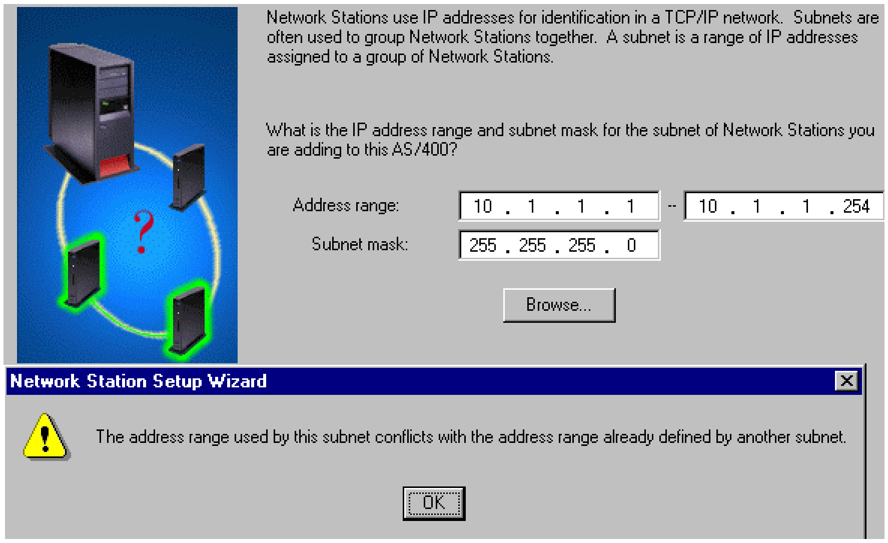
Browse Subnet Range - M15

Select one of the following:

Range	Subnet Mask	Type
10.1.1.1 -- 10.1.1.254	255.255.255.0	Interface
10.1.1.193 -- 10.1.1.254	255.255.255.192	Subnet

Figure 261. AS/400 Setup Wizard: Selecting IP address range

Selecting the 10.1.1.1 to 10.1.1.254 range results in an error message as shown in Figure 262. Click **OK** to return to the previous display.



Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

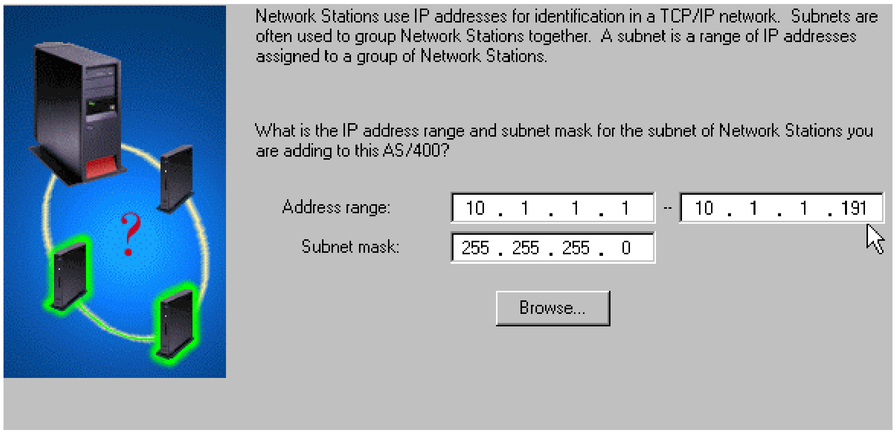
Address range: 10 . 1 . 1 . 1 -- 10 . 1 . 1 . 254

Subnet mask: 255 . 255 . 255 . 0

The address range used by this subnet conflicts with the address range already defined by another subnet.

Figure 262. AS/400 Setup Wizard: Error message when choosing subnet range

For this scenario, we select a range of addresses that does not include the twinaxial subnet. We manually enter this range as shown in Figure 263. After this range is entered, click **Next**.



Network Stations use IP addresses for identification in a TCP/IP network. Subnets are often used to group Network Stations together. A subnet is a range of IP addresses assigned to a group of Network Stations.

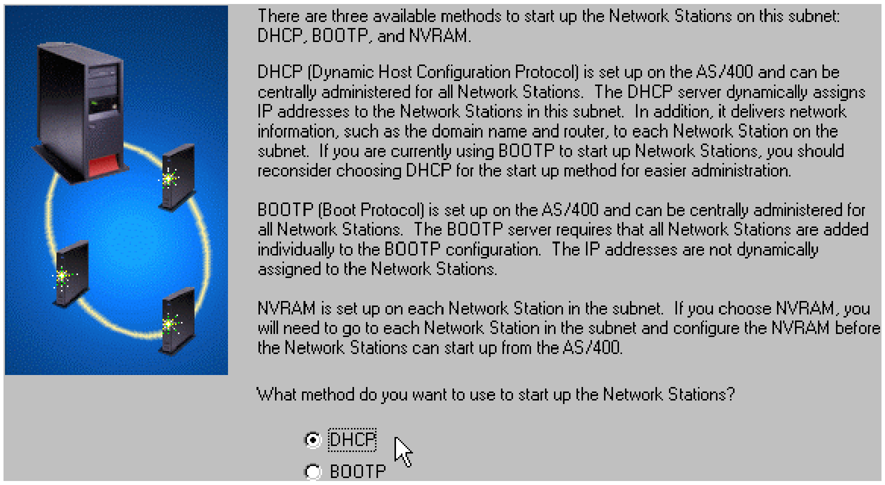
What is the IP address range and subnet mask for the subnet of Network Stations you are adding to this AS/400?

Address range: 10 . 1 . 1 . 1 -- 10 . 1 . 1 . 191

Subnet mask: 255 . 255 . 255 . 0

Figure 263. AS/400 Setup Wizard: Defining an IP address range

The next display in the Setup Wizard asks you to select a boot method. We chose to use the DHCP method of booting for the Model 2800. On the Setup Wizard display (Figure 264 on page 278), the DHCP method is chosen.


There are three available methods to start up the Network Stations on this subnet: DHCP, BOOTP, and NVRAM.

DHCP (Dynamic Host Configuration Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The DHCP server dynamically assigns IP addresses to the Network Stations in this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station on the subnet. If you are currently using BOOTP to start up Network Stations, you should reconsider choosing DHCP for the start up method for easier administration.

BOOTP (Boot Protocol) is set up on the AS/400 and can be centrally administered for all Network Stations. The BOOTP server requires that all Network Stations are added individually to the BOOTP configuration. The IP addresses are not dynamically assigned to the Network Stations.

NVRAM is set up on each Network Station in the subnet. If you choose NVRAM, you will need to go to each Network Station in the subnet and configure the NVRAM before the Network Stations can start up from the AS/400.

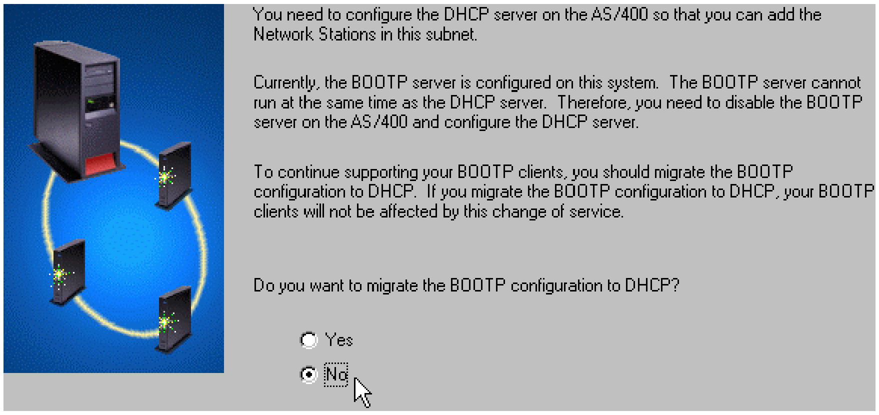
What method do you want to use to start up the Network Stations?

● DHCP

○ BOOTP

Figure 264. AS/400 Setup Wizard: Choosing a boot method

The next display asks you to select whether you want to migrate the BOOTP configuration. For this scenario, we do not migrate the BOOTP configuration. This selection is shown in Figure 265.


You need to configure the DHCP server on the AS/400 so that you can add the Network Stations in this subnet.

Currently, the BOOTP server is configured on this system. The BOOTP server cannot run at the same time as the DHCP server. Therefore, you need to disable the BOOTP server on the AS/400 and configure the DHCP server.

To continue supporting your BOOTP clients, you should migrate the BOOTP configuration to DHCP. If you migrate the BOOTP configuration to DHCP, your BOOTP clients will not be affected by this change of service.

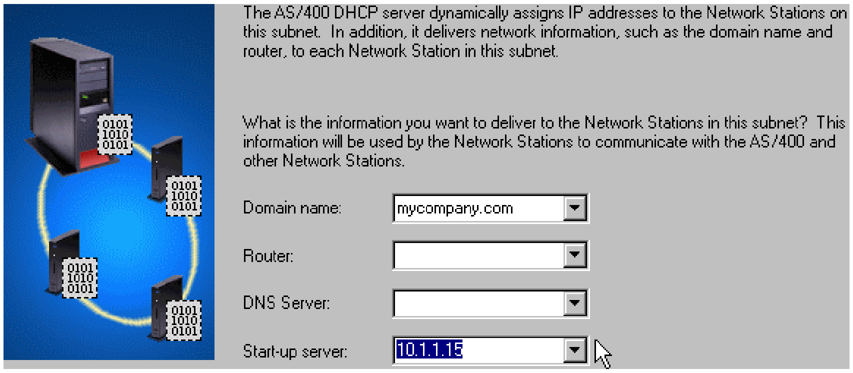
Do you want to migrate the BOOTP configuration to DHCP?

○ Yes

● No

Figure 265. AS/400 Setup Wizard: Choosing BOOTP migration

Further information in relation to DHCP is presented on the next display as shown in Figure 266. For this scenario, we only complete the Domain Name field and the Start-up server field.


The AS/400 DHCP server dynamically assigns IP addresses to the Network Stations on this subnet. In addition, it delivers network information, such as the domain name and router, to each Network Station in this subnet.

What is the information you want to deliver to the Network Stations in this subnet? This information will be used by the Network Stations to communicate with the AS/400 and other Network Stations.

Domain name: mycompany.com

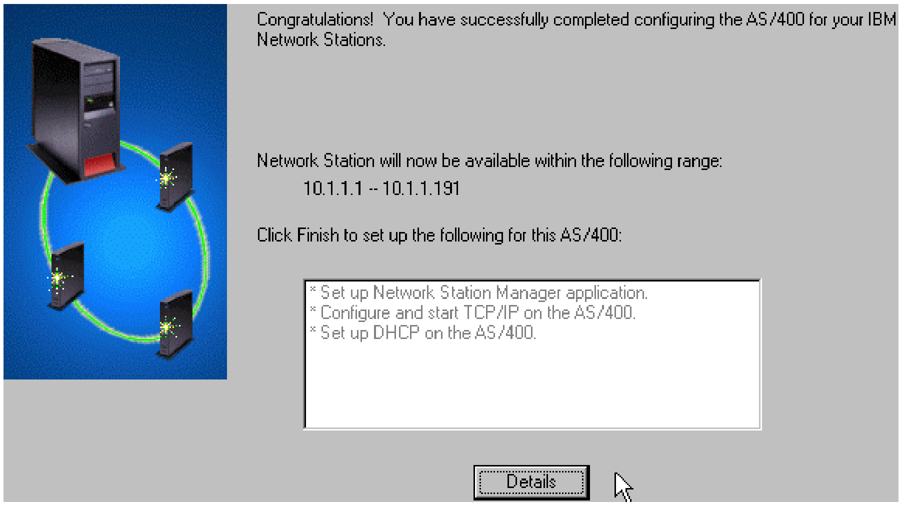
Router:

DNS Server:

Start-up server: 10.1.1.15

Figure 266. AS/400 Setup Wizard: Choosing DHCP options

The display shown in Figure 267 appears when the Network Station Wizard configuration has been completed. A list of tasks is presented. For further details on these tasks, click **Details**. If no details need to be reviewed at this time, click **Finish**.



Congratulations! You have successfully completed configuring the AS/400 for your IBM Network Stations.

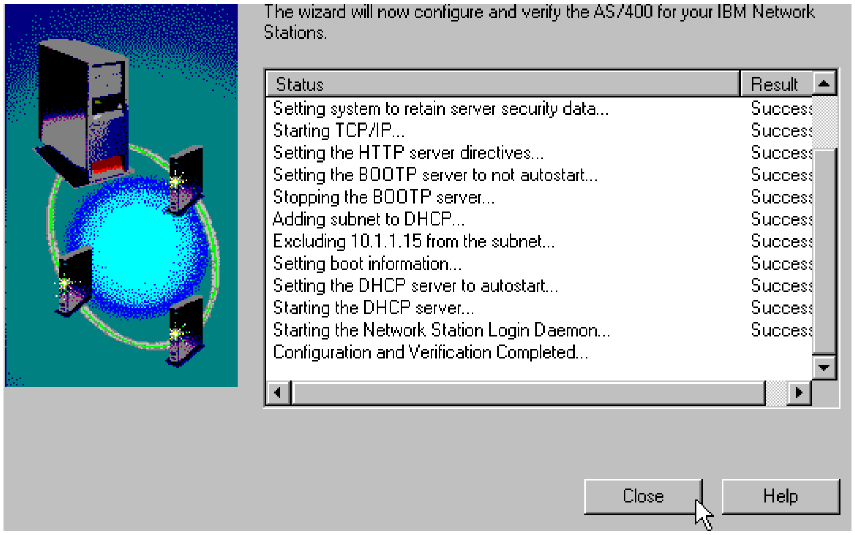
Network Station will now be available within the following range:
10.1.1.1 -- 10.1.1.191

Click Finish to set up the following for this AS/400:

- * Set up Network Station Manager application.
- * Configure and start TCP/IP on the AS/400.
- * Set up DHCP on the AS/400.

Figure 267. AS/400 Setup Wizard: Configuration completed

After clicking **Finish**, the Wizard takes a few moments to complete the tasks. As each task is completed, the display is refreshed automatically and the *Result* column is updated. You should check for any failed tasks and correct them. If all the tasks complete successfully, you see a display similar to the one shown in Figure 268.



The wizard will now configure and verify the AS/400 for your IBM Network Stations.

Status	Result
Setting system to retain server security data...	Success
Starting TCP/IP...	Success
Setting the HTTP server directives...	Success
Setting the BOOTP server to not autostart...	Success
Stopping the BOOTP server...	Success
Adding subnet to DHCP...	Success
Excluding 10.1.1.15 from the subnet...	Success
Setting boot information...	Success
Setting the DHCP server to autostart...	Success
Starting the DHCP server...	Success
Starting the Network Station Login Daemon...	Success
Configuration and Verification Completed...	

Figure 268. AS/400 Setup Wizard: Configuration and verification completed

Click **Close** to return to the main Operations Navigator session.

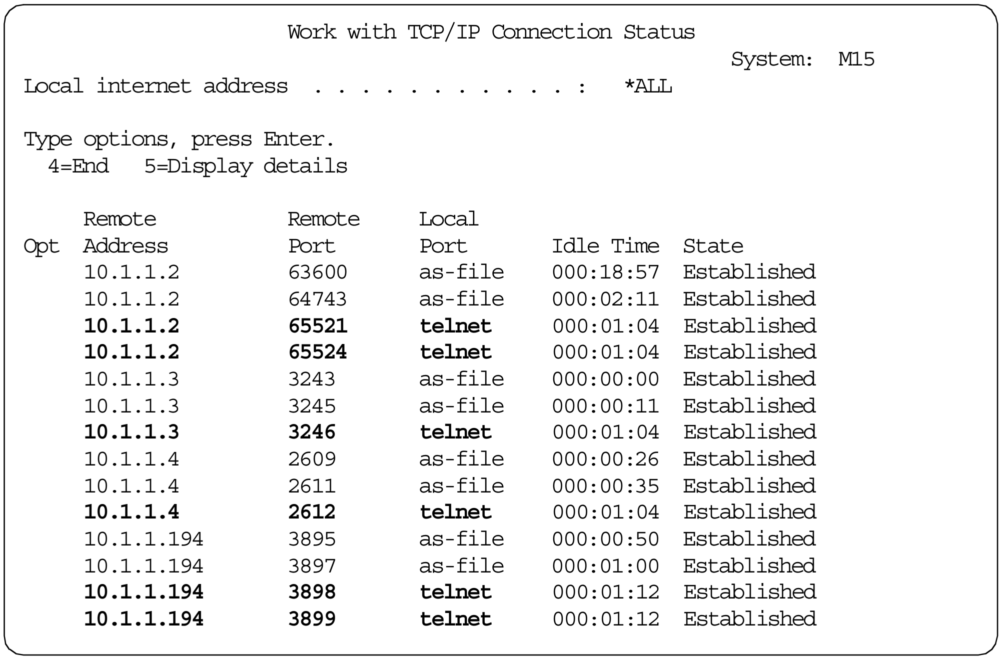
In this scenario, it is necessary to have the TFTP and DHCP servers started on the AS/400 server. After the boot-up process completes, a sign-on screen is present on all four client Network Stations. For each client user to sign on successfully, the Network Station Login Server needs to be started on port 256.

This Login Server is the V2R1 server, which supports both V1R3 and V2R1 clients. When the authentication of each user is completed, the appropriate autostart programs will be run on each client Network Station.

There are autostart 5250 sessions configured within the Network Station Managers. To access both of these managers, both the Admin and Default servers should be active on the AS/400 system. To verify this, issue the Work with Subsystem Jobs (WRKSBSJOB) command for the subsystem QHTTPSVR. The command would be `WRKSBSJOB SBS(QHTTPSVR)`. The resulting screen is shown in Figure 249 on page 269.

9.3.3.5 Connectivity verification

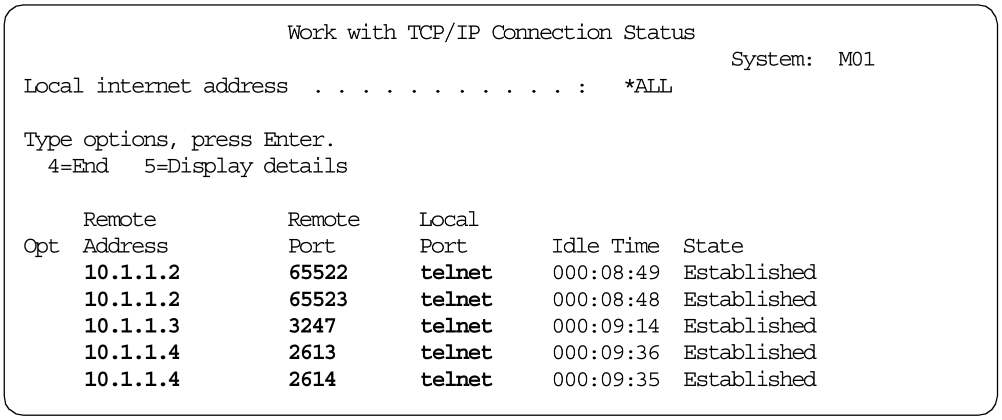
All four clients in this scenario have autostart 5250 sessions configured for the M15 system. To verify that these sessions are started, review the TCP/IP connection status screen on the M15 system by using the `NETSTAT *CNN` command. Figure 269 shows that the 10.1.1.194 (twinaxial client) has two established sessions, and each of the LAN clients have any number of autostarted sessions.



```
                       Work with TCP/IP Connection Status
                                                             System:  M15
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.2         63600      as-file    000:18:57  Established
     10.1.1.2         64743      as-file    000:02:11  Established
     10.1.1.2         65521      telnet     000:01:04  Established
     10.1.1.2         65524      telnet     000:01:04  Established
     10.1.1.3         3243       as-file    000:00:00  Established
     10.1.1.3         3245       as-file    000:00:11  Established
     10.1.1.3         3246       telnet     000:01:04  Established
     10.1.1.4         2609       as-file    000:00:26  Established
     10.1.1.4         2611       as-file    000:00:35  Established
     10.1.1.4         2612       telnet     000:01:04  Established
     10.1.1.194       3895       as-file    000:00:50  Established
     10.1.1.194       3897       as-file    000:01:00  Established
     10.1.1.194       3898       telnet     000:01:12  Established
     10.1.1.194       3899       telnet     000:01:12  Established
```

Figure 269. AS/400 TCP/IP connections: M15 system verification

The LAN-attached clients also have autostart 5250 sessions for the M01 system. Issuing the `NETSTAT *CNN` command on the M01 system shows the established connections (Figure 270).



```
                      Work with TCP/IP Connection Status
                                                                  System:  M01
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     10.1.1.2         65522      telnet     000:08:49  Established
     10.1.1.2         65523      telnet     000:08:48  Established
     10.1.1.3         3247       telnet     000:09:14  Established
     10.1.1.4         2613       telnet     000:09:36  Established
     10.1.1.4         2614       telnet     000:09:35  Established
```

Figure 270. AS/400 TCP/IP connections: M01 system verification

9.3.3.6 Summary

This scenario shows a network of two AS/400 systems and four IBM Network Station clients. One of the AS/400 systems (M15) is a boot server, which is set up to supply IP addresses to the IBM Network Station clients. There are both V1R3 and V2R1 hardware clients connected, so both levels of the IBM Network Station Manager (V1R3 and V2R1) are installed on the system.

Only the DHCP method is used among the IBM Network Station clients, and all are successful in booting and logging on to the M15 (server) system. All clients are successful in establishing 5250 sessions. Through the IBM Network Station Managers, different autostart values can be made for each individual Network Station user.

Chapter 10. Migration from V1R3 to V2R1 of NSM

This section is designed for those of you who are about to implement the newest Network Station Manager V2R1 software in your existing Network Station installation. It covers mainly the migration of the preference files and user data from previous NSM V1R3 level. Plus, it gives some hints about when you should not migrate or migrate partially due to certain circumstances. The term “migration” involves three steps that the Network Station Manager administrator should perform. In other words, migration from the NSM V1R3 to the NSM V2R1 can happen in three distinct phases:

- **Installation**: For more information about this phase, see Chapter 4, “Installation and server setup” on page 83.
- **Coexistence**: For more information about this phase and the factors that determine how long you stay in a V1R3 and V2R1 coexistence phase, see Chapter 9, “Coexistence of V1R3 and V2R1 IBM NSM” on page 211.
- **Migration**: At any point, you may decide to migrate one, some, or all your users to V2R1 of NSM.

This chapter focuses on migrating one, some, or all of your users to V2R1 of NSM.

Note: Appendix J, “Migration details” on page 645, offers you details behind the NSM migration broken down into the migration. It includes a breakdown of the system, group, user, and terminal preference levels.

10.1 Migration Utility overview

This part describes migration dependencies that take place when running the NSM V2R1 Migration Utility on a current NSM V1R3 installation. After running the Migration Utility, you can obtain a V2R1 environment in which you can use your both old Network Stations Model 300 and Model 1000 (Ethernet and Token-Ring), and new 2200 and 2800 hardware models.

Note: If you have Model 100 or Model 300 Twinax installed, you should retain your old NSM V1R3. Otherwise, they will be not supported.

We do not consider any network topology issues. We assume your present network configuration works fine and can support the additional demands placed on it by V2R1 of NSM (see Appendix I, “V2R1 memory requirements and network load” on page 643).

This section was written based on the exhaustive information found in Appendix J, “Migration details” on page 645, concerning the migration of the NSM V1R3 preferences and files.

Important note

It is assumed that the NSM V1R3 software is at its latest available version and the latest PTFs are applied. For Windows NT, you must have Service Pack (SP) 8. For the AS/400 system, you should apply the latest Group PTF SF99082).

10.1.1 Principles

A lot of work has been done to make the V2R1 Migration Utility relatively easy to use and useful. It gives the administrator a powerful tool to migrate V1R3 preferences at the following levels:

- System
- User
- Group
- Terminal

There are two types of migration:

- *NSM managed preferences migration*: The migration of preferences set up by the NSM V1R3 Graphical User Interface
- *User managed preferences ("backdoor files") migration*: The migration of all preferences not directly supported by the NSM V1R3 graphical user interface, or supported but set up manually apart from it.

10.1.2 Capabilities and performed functions

The Migration Utility performs the following functions:

- Carries out a conversion of V1R3 preferences files introduced in the V2R1 XML file format, encoded in UTF8. For more information about XML and UTF8, see 8.4, "Download profiles" on page 173.
- Carries out a conversion of "backdoor" entered preferences into the UTF8 coded configuration script ($USERBASEV2/profiles/migrate.scr).
- Changes the preferences for Netscape Communicator and NCi desktop.
- Converts both the MENUITEM and RUN commands found in NSM V1R3 to the appropriate items in NSM V2R1.
- Updates the paths due to the new directory structure.
- Removes an obsolete preferences and environment variables.

10.1.3 Migration paths

One of the most important files for the migration process is the file named preflist.nsm ($PRODBASEV2/nsm/defaults). It contains all the preferences that the Migration Utility transfers into version V2R1. For each of these preferences, the following information is included:

- Name
- Target category
- Type

All V1R3 configuration parameters are included in one of six groups:

- Hardware
- Desktop
- Navio
- 3270/5250 Emulators
- Startup
- Environment Variable

There are eight possible paths of migration:

- Migrate System
- Migrate User (user name)
- Migrate Group (group name)
- Migrate Terminal (nc-id)
- Migrate all Users
- Migrate all Groups
- Migrate all Terminals
- Migrate All

Table 44 shows a summary of migration paths.

Table 44. Migrations available to NSM administrator

Type of migration	Groups migrated
Migrate System	Hardware, Desktop, 3270/5250 Emulators, Navio, Startup, and Environment Variable
Migrate User (user name)	Hardware, Desktop, 3270/5250 Emulators, Navio, Startup, and Environment Variable
Migrate Group (group name)	Hardware, Desktop, 3270/5250 Emulators, Navio, Startup, and Environment Variable
Migrate Terminal (nc-id)	Hardware preferences are migrated
Migrate all Users	Hardware, Desktop, 3270/5250 Emulators, Navio, Startup, and Environment Variable for each valid user
Migrate all Groups	Hardware, Desktop, 3270/5250 Emulators, Navio, Startup, and Environment Variable for each valid group
Migrate all Terminals	Hardware preferences will be migrated for each valid NSM client
Migrate All	All of the above is migrated

10.1.4 Important files

The following sections briefly discuss all of the mentioned migration paths. They include information where all supported preferences will be appended (name of V2R1 target file) and what file they originated from (names of V1R3 origin files).

Note

The directory structure of the V1R3 terminal configuration files (origin files) is platform dependent. In the following section, it pertains to the OS/400 operating system. Be sure to make the appropriate substitution for your platform.

10.1.4.1 System-level migration path

Here are the original files for the three target files alluser.nsm, allncds.nsm, and migrate.scr, from which the data is migrated, presented in this section:

alluser.nsm

The target file for the system-level migration path is $USERBASEV2/profiles/allusers.nsm.

The origin files are:

- $USERBASE/SysDef/NCDwm/pref
- $USERBASE/SysDef/NS5250/pref
- $USERBASE/SysDef/NS3270/pref
- $USERBASE/SysDef/NAV/pref
- $USERBASE/SysDef/envvars.nsm
- $USERBASE/SysDef/NCDwm/startup.nsm

allncs.nsm

The target file is $USERBASEV2/profiles/allncs.nsm.

The origin file is $USERBASE/StationConfig/defaults.nsm.

migrate.scr

The target file is $USERBASEV2/profiles/migrate.scr.

The origin files are:

- $USERBASE/StationConfig/defaults.dft
- $USERBASE/SysDef/pref.dft
  - Supported preferences starting with “NAVIO”
  - Supported preferences starting with “NS5250*”
  - Supported preferences starting with “NS3270*”
  - Supported preferences starting with “NCDterm”
  - Supported preferences starting with “NSTerm”
  - Supported preferences starting with “mwm”

10.1.4.2 Group-level migration path

The original files for the two target files <group>.nsm and migrate.scr, from which the data is migrated, are listed in this section.

<group>.nsm

The target file for the group-level migration path is $USERBASEV2/profiles/groups/<group>.nsm.

The origin files are:

- $USERBASE/groups/<group>.nsg
- $USERBASE/groups/<group>/NCDwm/pref
- $USERBASE/groups/<group>/NS5250/pref
- $USERBASE/groups/<group>/NS3270/pref
- $USERBASE/groups/<group>/NAV/pref
- $USERBASE/groups/<group>/envvars.nsm
- $USERBASE/groups/<group>/startup.nsm

migrate.scr

The target file is $USERBASEV2/profiles/migrate.scr.

The origin file is $USERBASE/groups/<group>.grp.

10.1.4.3 User-level migration path

The original files for the two target files <user>.nsm and migrate.scr, from which the data is migrated, are presented in this section.

<user>.nsm

The target file for the user level-migration path is $USERBASEV2/profiles/users/<user>.nsm.

The origin files are:

- $USERBASE/users/<user>.nsg
- $USERBASE/users/<user>/NCDwm/pref
- $USERBASE/users/<user>/NS5250/pref
- $USERBASE/users/<user>/NS3270/pref
- $USERBASE/users/<user>/NAV/pref
- $USERBASE/users/<user>/envvars.nsm
- $USERBASE/users/<user>/startup.nsm

migrate.scr

The target file is $USERBASEV2/profiles/migrate.scr.

The origin file is $USERBASE/users/<user>.usr.

10.1.4.4 Terminal-level migration path

The original files for the two target files <nc-id>.nsm and migrate.scr, from which the data is migrated, are listed here.

<nc-id>.nsm

The target file for the terminal-level migration path is $USERBASEV2/profiles/ncs/<nc-id>.nsm.

The origin file is $USERBASE/StationConfig/<nc-id>.nst.

migrate.scr

The target file is $USERBASEV2/profiles/migrate.scr.

The origin file is $USERBASE/StationConfig/<nc-id>.trm.

10.1.4.5 Launch Bar migration

The V1R3 tags MENUITEM and RUN are handled differently during the migration by the Migration Utility. The tags are explained here:

- **MENUITEM**

  If the Migration Utility finds any V1R3 MENUITEM, tags at the end of the existing launchbar, a new folder named “Old Applications” will be created. If more than one MENUITEM exists, it will be added at the end of that same folder.

- **RUN**

  If the Migration Utility finds any V1R3 RUN tags, they are added to the “Startup” folder. Similarly all RUN commands are appended at the end of that folder.

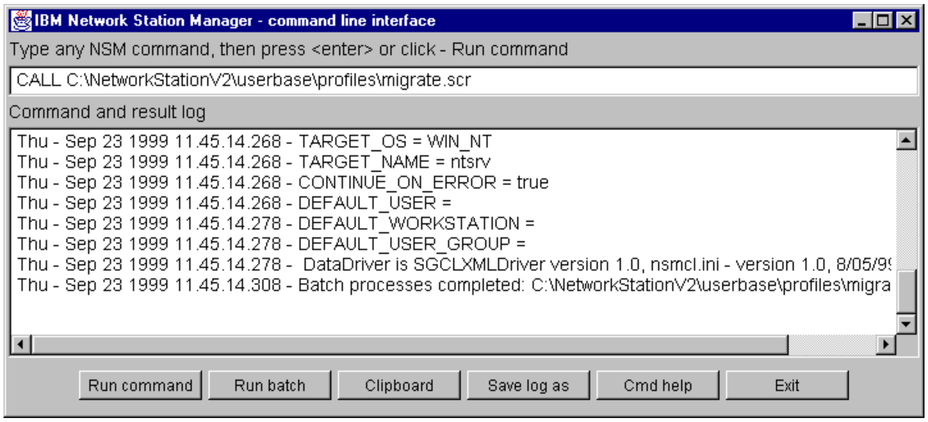
Note

If you are rerunning the Migration Utility, remember that both the Old Application and Startup folders will be cleared. Rerunning it on group level causes that mentioned folders for all users belonging to these groups will be cleared. Doing that on system level means that all Startup and Old Applications folders are cleared.

10.1.5 Migration of ‘backdoor’ preferences

A second important stage of migration is dealing with “backdoor” entered preferences. As mentioned earlier, they are “administrator-edited” preferences. You can find all preferences that can be moved to the new V2R1 in the migration script $USERBASEV2/profiles/migrate.scr. An NSM administrator can review it if they still want these preferences to migrate. If so, the next step is to use the NSM Command Line Utility. Section 8.5, “NSM Command Line Interface” on page 180, explains the process. Rerunning the Migration Utility always appends information to the existing migration script. This means that if you migrate in more than one step (user-level migration, groups-level migration), you do not have to run it each time the NSM Command Line Utility is run because all the work done so far is preserved.

Figure 271 shows an example of running the NSM Command Line Utility.



IBM Network Station Manager - command line interface

Type any NSM command, then press <enter> or click - Run command

CALL C:\NetworkStationV2\userbase\profiles\migrate.scr

Command and result log

```
Thu - Sep 23 1999 11.45.14.268 - TARGET_OS = WIN_NT
Thu - Sep 23 1999 11.45.14.268 - TARGET_NAME = ntsrv
Thu - Sep 23 1999 11.45.14.268 - CONTINUE_ON_ERROR = true
Thu - Sep 23 1999 11.45.14.268 - DEFAULT_USER =
Thu - Sep 23 1999 11.45.14.278 - DEFAULT_WORKSTATION =
Thu - Sep 23 1999 11.45.14.278 - DEFAULT_USER_GROUP =
Thu - Sep 23 1999 11.45.14.278 -  DataDriver is SGCLXMLDriver version 1.0, nsmcl.ini - version 1.0, 8/05/9
Thu - Sep 23 1999 11.45.14.308 - Batch processes completed: C:\NetworkStationV2\userbase\profiles\migra
```

Figure 271. Performing Command Line Utility against migration script

10.1.6 Tips and limitations

The following list describes the requirements necessary for NSM V2R1 Migration Utility to process backdoor files correctly:

- Each line in these backdoor files must end with either a Line Feed (LF) or Carriage Return - Line Feed (CR-LF). The CR character by itself at the end of a line is not supported.
- Migration Utility processes only SET commands. Other commands are ignored.
- The preferences name must be in lower case. Values of that preference, if the values represent a string, can be upper or lowercase. Here are examples:

```
set pref-mouse-arrangement=left-handed //lower case//
set unit-contact="John Smith" //any case//
```

- Comments are ignored.

Note

If comments appear in the same line as preference, they will be treated as a part of it.

- If the preference has no value, “nil” should be used.
- Accepted Boolean values are true or false.

10.1.7 Available parameters for the Migration Utility

Table 45 explains the meaning of each switch you can use in the Migration Utility. Switches are common for all platforms, including Windows NT, OS/400, and AIX.

Table 45. Migration Utility command line parameters

Parameter	Description
-A	This flag indicates that all preferences at all levels (system, users, groups, and terminals) will be migrated.
-S	This flag indicates that all system-level preferences will be migrated to Network Station Manager V2R1.
-U	This flag can be used to migrate a particular user or users. There is also an option to migrate all users by specifying an *ALL after the -U switch.
-G	This flag can be used to migrate a particular group or groups. There is also an option to migrate all groups by specifying an *ALL after the -G switch.
-T	This flag can be used to migrate a particular terminal or terminals. There is also an option to migrate all terminals by specifying an *ALL after the -T switch.
-C	This switch enables Power PC NVRAM clients automatic migration to the new NSM V2R1 file and directory naming convention. It can be used *only* in single server migration and with *both* NSM V1R3 and NSM V2R1 installed.
-P	This flag allows you to specify a path to directory where NSM V1R3 preference and configuration files are stored.

Here are examples of using parameters with Migration Utility:

- On Windows NT:

  ```
  nsmv2migr -S -G group1_5 group6_9 -U user1
  ```

  This command migrates system-level preferences, preference files for both group1_5 and group6_9 groups, and user preference files for user1.

- On the AS/400 system:

  ```
  CALL PGM(QYTCV2/QYTCMUMU) PARM('-S' '-G' *ALL '-T' 10.1.1.1)
  ```

  This command migrates system-level preferences, preference files for all V1R3 groups, and one terminal-level preference file for Network Station with the 10.1.1.1 IP address.

10.1.8 Error messages

Table 46 shows common messages you can encounter when running the Migration Utility.

Table 46. Messages generated while running the Migration Utility

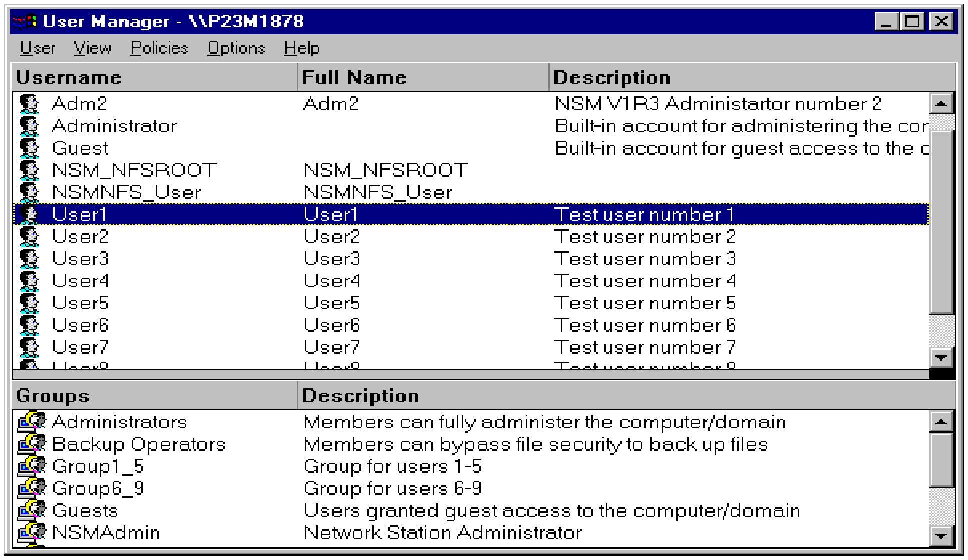
Message ID	Message text	Short explanation
NSM7007	Unable to access system settings.	Error in accessing (opening, reading) the NSM V2R1 system-level preference file.
NSM7008	Unable to access user settings.	Error in accessing (opening, reading) the NSM V2R1 user-level preference file.
NSM7009	Unable to update system settings.	Error in updating (writing) the NSM V2R1 system-level preference file.
NSM7010	Unable to update user settings.	Error in updating (writing) the NSM the V2R1 user-level preference file.
NSM7014	Unable to access workstation settings.	Error in accessing (opening, reading) the NSM V2R1 terminal-level preference file.
NSM7015	Unable to update workstation settings.	Error in updating (writing) the NSM V2R1 terminal-level preference file.
NSM7036	Unable to access group settings.	Error in accessing (opening, reading) the NSM V2R1 group-level preference file.
NSM7037	Unable to update group settings.	Error in updating (writing) the NSM V2R1 group-level preference file.
NSM7044	Unable to migrate file.	Error encountered that prevents the migration of a NSM V1R3 file. This may be due to problems reading the NSM V1R3 file or access or update problems with the NSM V2R1 preference file.
NSM7045	Unable to retrieve list of users.	Error retrieving the list of users to migrate (for migration of all preferences or all users).
NSM7049	Migration program did not complete successfully.	You should review previously logged messages to find a reason for this information.
NSM7050	Migration program completed successfully.	
NSM7052	Problem converting file to current CCSID.	Error in converting the contents of a file to CCSID (codepage) used by the job.
NSM7058	Unable to access required file &1.	A file required by Migration Utility cannot be accessed (opened, read).

Message ID	Message text	Short explanation
NSM7059	Unable to access script file &1.	Error in accessing or updating the migration command script file used to migrate backdoor files.
NSM7060	Setting &1 no longer supported.	A NSM V1R3 preference is no longer supported in NSM V2R1.
NSM7061	Value for setting &1 no longer supported.	A value for a NSM V1R3 preference is no longer supported in NSM V2R1.
NSM 7062	Parameter in application command no longer valid.	A parameter (or its value) on a NSM V1R3 startup command (RUN, MENUITEM) is no longer valid in NSM V2R1.
NSM7063	Unable to retrieve list of groups	Error retrieving the list of groups to migrate (for migration of all preferences or all groups).
NSM7064	Unable to retrieve list of workstations.	Error retrieving the list of workstations to migrate (for migration of all preferences or all workstations).
NSM7065	Not able to migrate setting &1.	A preference was found in a backdoor file that is valid, but is not supported by the IBM Network Station command line utility.
NSM7066	Migration command script created or updated.	Migration of backdoor files occurred so the migration command script was created or updated.
NSM7070	Object &1 not found.	You submitted a wrong parameter as an object name. It could be a wrong terminal, user, or group name.
NSM7071	Parameter &1 not valid.	You submitted a wrong parameter for the NSM Migration Utility. For a list of valid parameters, see Table 45 on page 289.

10.2 Migration utility examples

In our test lab, we set up two migration environments. One of them with a Windows NT Server 4.0 and a second for an AS/400 system. In both configurations, we migrate systems that consist of 12 users (three administrators and nine users) contained in the two groups.

For an example of the groups and users configured in our test lab, see Figure 272 on page 292.



Username	Full Name	Description
Adm2	Adm2	NSM V1R3 Administartor number 2
Administrator		Built-in account for administering the cor
Guest		Built-in account for guest access to the c
NSM_NFSROOT	NSM_NFSROOT	
NSMNFS_User	NSMNFS_User	
User1	User1	Test user number 1
User2	User2	Test user number 2
User3	User3	Test user number 3
User4	User4	Test user number 4
User5	User5	Test user number 5
User6	User6	Test user number 6
User7	User7	Test user number 7
User8	User8	Test user number 8

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Group1_5	Group for users 1-5
Group6_9	Group for users 6-9
Guests	Users granted guest access to the computer/domain
NSMAdmin	Network Station Administrator

Figure 272. Users and groups created for tests under Windows NT 4.0

10.2.1 Case 1: Windows NT 4.0 (single server migration)

First contact with migration appears already at the end of installation (if you choose Typical or Authentication Server Install). You are given the choice to automatically migrate. Although it is a convenient path, we do not choose it because it is an all-or-nothing method. We chose instead the Custom Install. In this case, the only way to run the Migration Utility is to run it as a standalone utility from a Windows NT prompt.

10.2.1.1 V1R3 environment

Our server installation consist of one IBM Netfinity 3000 server with Windows NT 4.0, Service Pack 5, and Network Station Manager V1R3 (3.08). The following lines show us a few examples of altered preferences in the V1R3 files by the NSM V1R3 GUI program (the markers x.x have been added for reference):

c:\Nstation\Userbase\SysDef\startup.nsm

```
VERSION   R3M0
SOURCE ${NSM_PROD_SYSDEFAULTS}/startup.nsm
SET TRACE ON
SET NSM_HTTP_PORT 80
SET JITC_ENABLED NO
SET RUNWM YES
MENUITEM "AS/400 ABC" ns5250 as01 a.7
RUN ns5250 as01 a.8
RUN ns5250 a.9
```

c:\Nstation\Userbase\SysDef\NAV\pref

```
Navio.proxyMode: 2
Navio.autoconfigUrl: w3.rchland.ibm.com/rch.proxy b.2
Navio*urlBar*directoryButton1.labelString: TRAX Poland
Navio.directoryButton1BUrl: www.trax.com.pl b.4
Navio*urlBar*directoryButton1.documentationString: TRAX Zielona Gora
Navio*urlBar*directoryButton2.labelString: IBM Rochester
Navio.directoryButton2BUrl: w3.rchland.ibm.com b.9
```

c:\Nstation\Userbase\groups\Group1_5\startup.nsm

```
VERSION R3M0
SOURCE ${NSM_ADMIN_SYSDEFAULTS}/startup.nsm
RUN ns5250 as01 -geometry -0+0 c.2
```

c:\Nstation\Userbase\groups\Group1_5\NCDwm\pref

```
mwm*useIconBox: False
mwm*iconPlacement: right bottom d.2
```

c:\Nstation\Prodbase\configs\9.5.92.60.trm

This file was edited manually by the NSM V1R3 administrator, who entered just one line in it. From this moment, this file can be called a “backdoor” terminal preference file for the 9.5.92.60 machine.

```
set unit-contact="Ryszard Pytko"
```

A further explanation of these lines is offered here.

Each V1R3 user has:

- One additional MENUITEM added for manually starting 5250 session - a.7
- One 5250 autostart session connected to `as01` - a.8
- One 5250 autostart session connection window - a.9
- Information about the proxy setting - b.2
- Two directory buttons under Navio pointing to two different URLs - b.4 and b.9

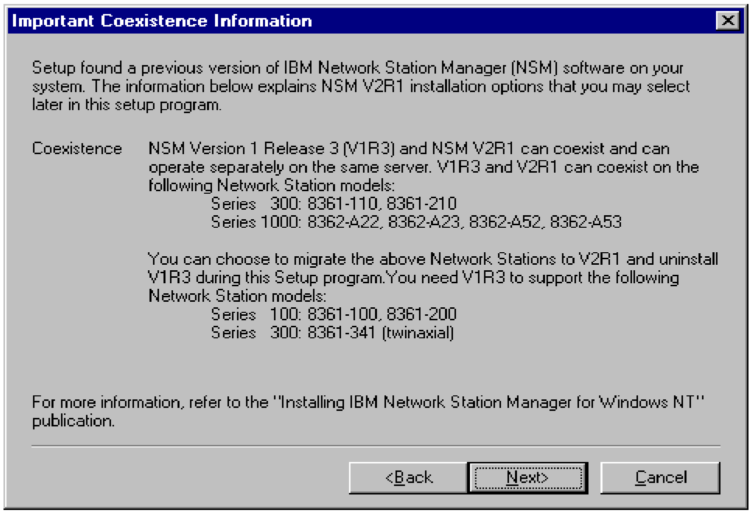
In addition, users belonging to group Group1_5 have:

- One additional 5250 autostart session placed in the upper-right corner of the window - c.2
- A preference that causes minimized window icons to be placed at the bottom-right corner of the window - d.2

10.2.1.2 V2R1 environment

This section contains Windows NT 4.0 displays during the installation and migration process. Since installation is not the main scope of this chapter, we provide just few examples for clarity.

The first message (just informational) related with migration and coexistence appears in a few seconds after starting the installation program (Figure 273 on page 294).



Important Coexistence Information

Setup found a previous version of IBM Network Station Manager (NSM) software on your system. The information below explains NSM V2R1 installation options that you may select later in this setup program.

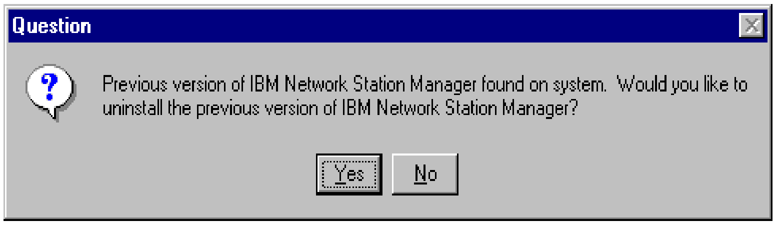
Coexistence NSM Version 1 Release 3 (V1R3) and NSM V2R1 can coexist and can operate separately on the same server. V1R3 and V2R1 can coexist on the following Network Station models:
Series 300: 8361-110, 8361-210
Series 1000: 8362-A22, 8362-A23, 8362-A52, 8362-A53

You can choose to migrate the above Network Stations to V2R1 and uninstall V1R3 during this Setup program.You need V1R3 to support the following Network Station models:
Series 100: 8361-100, 8361-200
Series 300: 8361-341 (twinaxial)

For more information, refer to the "Installing IBM Network Station Manager for Windows NT" publication.

Figure 273. Coexistence information displayed at the beginning of the installation process

Next, the program asks you whether you want to un-install the previous V1R3 version (Figure 274). Remember that if you choose *Yes*, the IBM Network Station Manager will only uninstall the code, *not* your user data. We chose *No* to have greater control over the migration of our user preferences.



Question

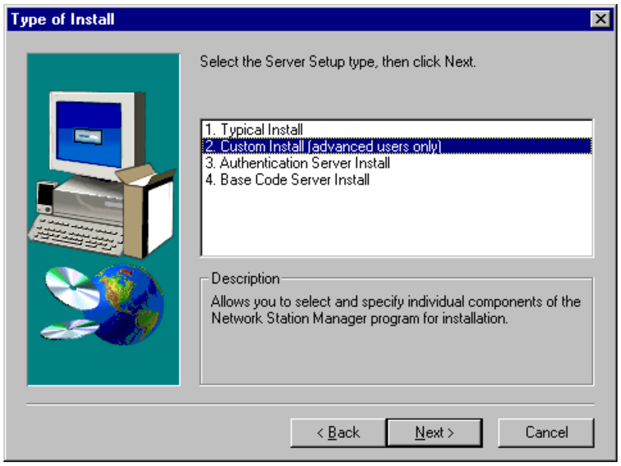
Previous version of IBM Network Station Manager found on system. Would you like to uninstall the previous version of IBM Network Station Manager?

Figure 274. Deinstallation prompt

Important note

If you choose Yes, it will be not possible to use -C switch with the nsmv2migr.exe program. This switch causes all NVRAM machines Series 1000 (8362-all models) and Series 300 (8361-110, 8362-210) to boot to the newly installed V2R1 Network Station Manager. For this switch to work correctly, *both* versions V1R3 and V2R1 *must* be installed on the same server.

Then, you must choose the type of installation as shown in Figure 275.



Type of Install

Select the Server Setup type, then click Next.

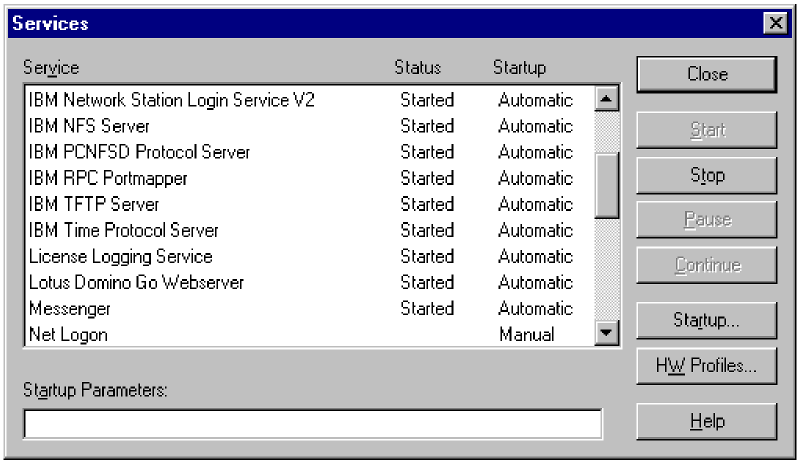
1. Typical Install
2. Custom Install (advanced users only)
3. Authentication Server Install
4. Base Code Server Install

Description

Allows you to select and specify individual components of the Network Station Manager program for installation.

Figure 275. Type of installation

After choosing the components to install, the procedure begins. In our test lab equipped with IBM Netfinity 3000 PC Server, PII 350 MHz, 128 MB RAM, 4.3 GB UltraSCSI disk, it took about 20 minutes (5 minutes to install from the CD-ROM and 15 minutes to set up permissions). As we checked after installation, the NetworkStationV2 directory includes more than 11,000 files in more than 1,000 directories. After a successful installation, the service window should look like the example in Figure 276.



Services

Service	Status	Startup
IBM Network Station Login Service V2	Started	Automatic
IBM NFS Server	Started	Automatic
IBM PCNFSD Protocol Server	Started	Automatic
IBM RPC Portmapper	Started	Automatic
IBM TFTP Server	Started	Automatic
IBM Time Protocol Server	Started	Automatic
License Logging Service	Started	Automatic
Lotus Domino Go Webserver	Started	Automatic
Messenger	Started	Automatic
Net Logon		Manual

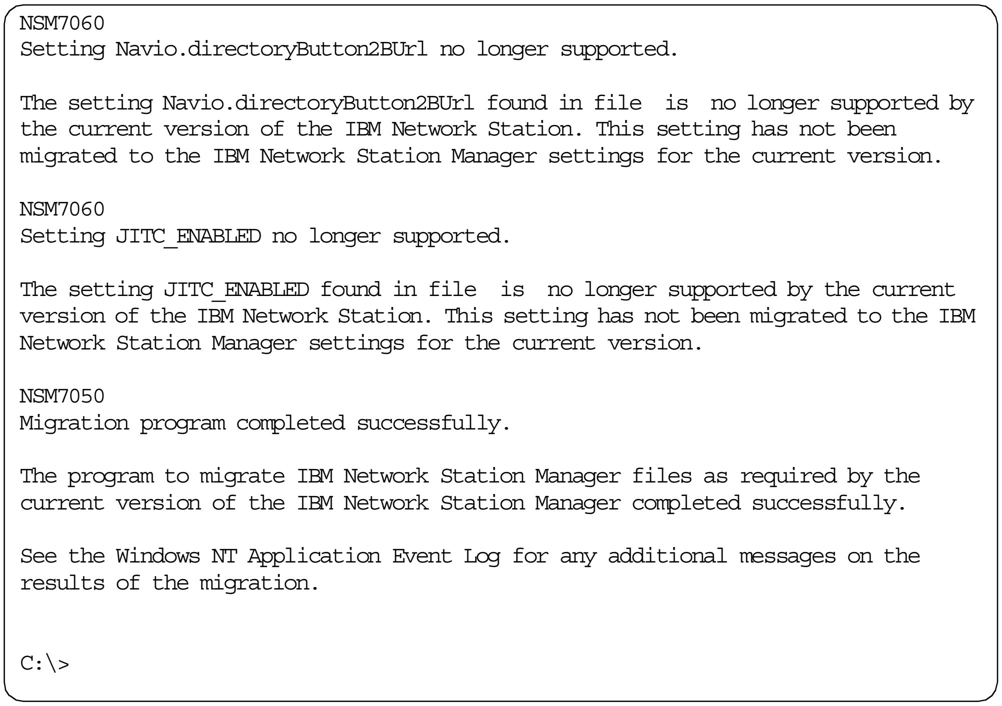
Startup Parameters:

Figure 276. Services window after installing NSM V2R1 and rebooting the Windows NT Server

At this point, you can use your old Network Stations in both environments. You can perform migration now since it is a non-disruptive process. We choose the “migrate all” method, which is activated by following command from a Windows NT command line prompt:

```
nsmv2migr.exe -A
```

In a minute, a command prompt appears as shown in Figure 277 on page 296.



```
NSM7060
Setting Navio.directoryButton2BUrl no longer supported.

The setting Navio.directoryButton2BUrl found in file  is  no longer supported by
the current version of the IBM Network Station. This setting has not been
migrated to the IBM Network Station Manager settings for the current version.

NSM7060
Setting JITC_ENABLED no longer supported.

The setting JITC_ENABLED found in file  is  no longer supported by the current
version of the IBM Network Station. This setting has not been migrated to the IBM
Network Station Manager settings for the current version.

NSM7050
Migration program completed successfully.

The program to migrate IBM Network Station Manager files as required by the
current version of the IBM Network Station Manager completed successfully.

See the Windows NT Application Event Log for any additional messages on the
results of the migration.


C:\>
```

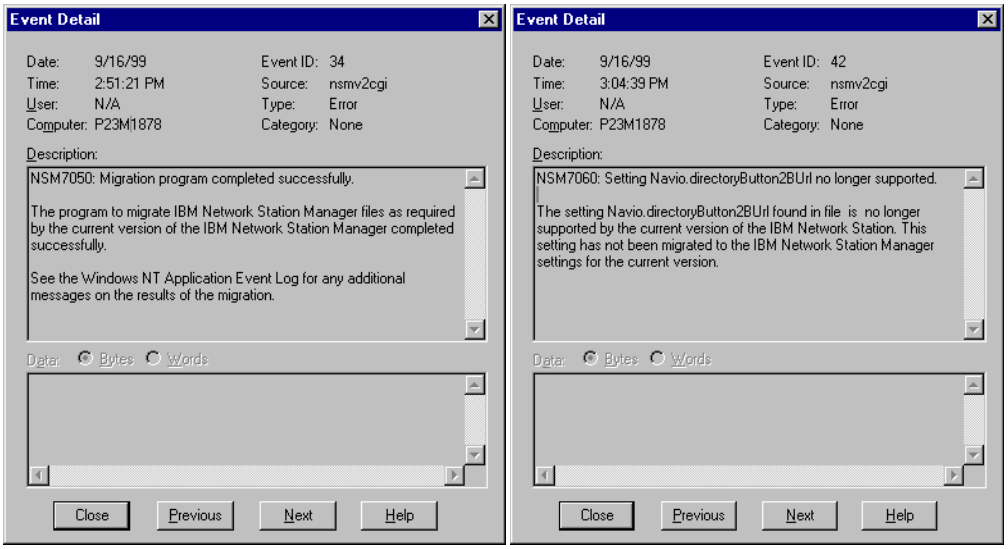
Figure 277. Prompt window after running the nsmv2migr.exe program

Tip

You can redirect the output of a migration program to a file to easily review it by using the greater than symbol (>), for example:

```
nsmv2migr -A > migr_log.log
```

Every activity that occurs while nsmv2migr.exe is running is also logged in the Event Viewer under the Application section. Figure 278 through Figure 280 on page 298 provide a few examples of such messages.



Event Detail

Date: 9/16/99 Event ID: 34
Time: 2:51:21 PM Source: nsmv2cgi
User: N/A Type: Error
Computer: P23M1878 Category: None

Description:

NSM7050: Migration program completed successfully.

The program to migrate IBM Network Station Manager files as required by the current version of the IBM Network Station Manager completed successfully.

See the Windows NT Application Event Log for any additional messages on the results of the migration.

Event Detail

Date: 9/16/99 Event ID: 42
Time: 3:04:39 PM Source: nsmv2cgi
User: N/A Type: Error
Computer: P23M1878 Category: None

Description:

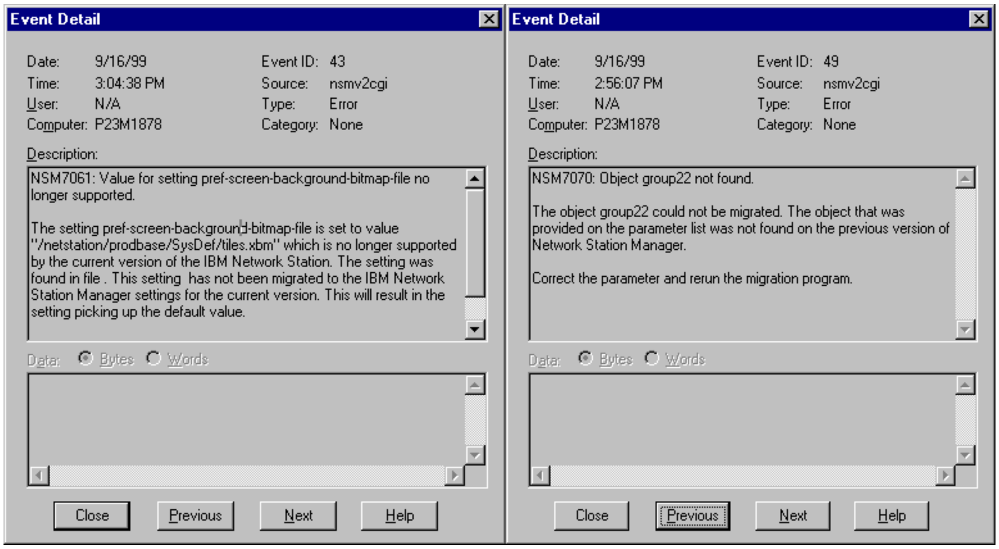
NSM7060: Setting Navio.directoryButton2BUrl no longer supported.

The setting Navio.directoryButton2BUrl found in file is no longer supported by the current version of the IBM Network Station. This setting has not been migrated to the IBM Network Station Manager settings for the current version.

Figure 278. Messages from the Event Viewer

On the right display in Figure 278, there is an example of what message is logged when a previously supported preference is no longer valid. In this case, it is the directory button from the NSM V1R3 Navio Web browser. The following examples show different messages:

- NSM7061: Value for setting <preference-name> no longer supported.
- NSM7070: Object group22 not found.
- NSM7071: Parameter *ALL not valid.



Event Detail

Date: 9/16/99 Event ID: 43
Time: 3:04:38 PM Source: nsmv2cgi
User: N/A Type: Error
Computer: P23M1878 Category: None

Description:

NSM7061: Value for setting pref-screen-background-bitmap-file no longer supported.

The setting pref-screen-background-bitmap-file is set to value "/netstation/prodbase/SysDef/tiles.xbm" which is no longer supported by the current version of the IBM Network Station. The setting was found in file . This setting has not been migrated to the IBM Network Station Manager settings for the current version. This will result in the setting picking up the default value.

Event Detail

Date: 9/16/99 Event ID: 49
Time: 2:56:07 PM Source: nsmv2cgi
User: N/A Type: Error
Computer: P23M1878 Category: None

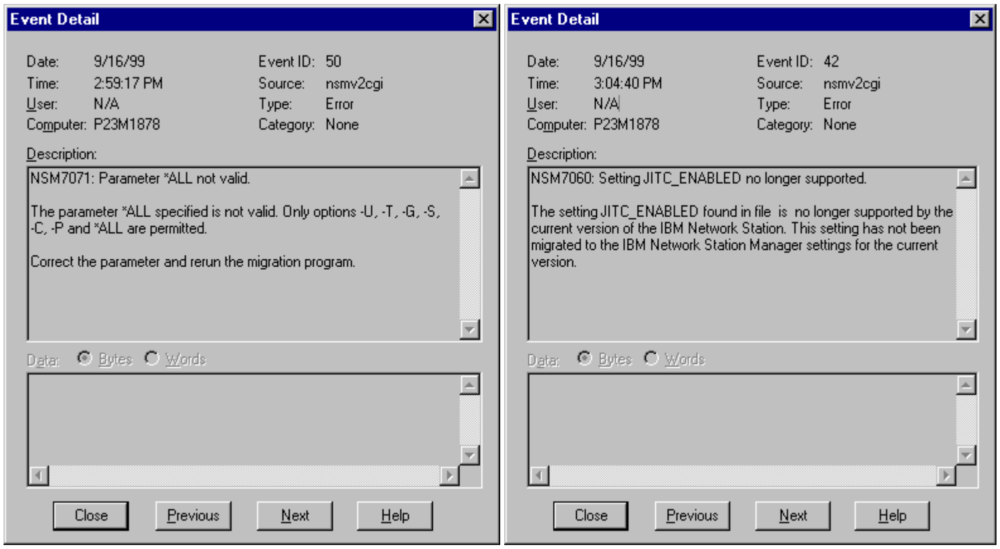
Description:

NSM7070: Object group22 not found.

The object group22 could not be migrated. The object that was provided on the parameter list was not found on the previous version of Network Station Manager.

Correct the parameter and rerun the migration program.

Figure 279. Messages from the Event Viewer



Date: 9/16/99 Event ID: 50
Time: 2:59:17 PM Source: nsmv2cgi
User: N/A Type: Error
Computer: P23M1878 Category: None

Description:

NSM7071: Parameter *ALL not valid.

The parameter *ALL specified is not valid. Only options -U, -T, -G, -S, -C, -P and *ALL are permitted.

Correct the parameter and rerun the migration program.

Date: 9/16/99 Event ID: 42
Time: 3:04:40 PM Source: nsmv2cgi
User: N/A Type: Error
Computer: P23M1878 Category: None

Description:

NSM7060: Setting JITC_ENABLED no longer supported.

The setting JITC_ENABLED found in file is no longer supported by the current version of the IBM Network Station. This setting has not been migrated to the IBM Network Station Manager settings for the current version.

Figure 280. Messages from the Event Viewer

Explanation

Message NSM7071 may be a little confusing. *ALL is permitted, but only in conjunction with -U, -G, -T, for example:

```
nsmv2migr -U *ALL
```

The migration ends successfully.

Important

Verifying preferences in the NSM V2R1 files, we discovered that supported preferences from the NSM V1R3 defaults.nsm were not migrated to the NSM V2R1 allncs.nsm.

If you had your bookmark file and address-book file are in the old V1R3 Navio browser, the Migration Utility rename them respectively to v1r3_bm.htm and v1r3_ab.htm. They are saved in the $USERBASE2/home/<user name>/.netscape directory. If you want to use them in V2R1 Netscape Communicator, you have to import them manually. Each user should perform the following procedure.

To import a bookmarks file, follow these steps:

1. Start Network Station's Netscape Communicator browser.
2. From the main menu, select **Communicator->Bookmarks->Edit Bookmarks**.
3. From the main menu of the Bookmarks window, select **File->Import**.
4. Select the **v1r3_bm.htm** file. Click **Open**.

To import an address file, complete these tasks:

1. Start Network Station's Netscape Communicator browser.
2. From the main menu, select **Communicator->Address Book**.

3. From the main menu of the Address Book, select **File->Import**.
4. Select an import format, and select **Next**.
5. Select the **v1r3_ab.htm** file. Click **Open**.

Note

The Migration Utility copies the contents of user's home directory into the new NSM V2R1 directory structure.

This note must be further explained as a home directory. Its content is very important for each user. In practice, there are two home directories on the Windows NT 4.0 Authentication Server for *each* user:

- **/userbase/home/<user name>/**

  The user's "true" home directory. Pressing ALT+S under the Navio browser, the directory is presented to the user by default as:

  ```
  /netstation/homebase/users/<user name>/*.*
  ```

  Its primary goal is to store anything that belongs to <user name>, plus, for example, browser's bookmarks.

- **/userbase/users/<user name>/**

  The second directory to where <user name> can write.

Important note for Windows NT users

User files from the /$USERBASE/home/<user name>/ directory are not migrated to the new NSM V2R1 /$USERBASEV2/home/<user name>/ home directory.

Users files from the /$USERBASE/users/<user name>/ directory are. It means that there is additional, manual work to do by the NSM administrator. There are two ways to migrate the required files from the /$USERBASE/home/<user name>/ directory:

- Move the files from the /$USERBASE/home/<user name>/ directory to the /$USERBASE/users/<user name>/. Then, run Migration Utility.
- Move the files from the /$USERBASE/home/<user name>/ directory to the /$USERBASEV2/home/<user name>/ directory in NSM V2R1.

This work must be done manually and on a per-user basis.

However, this is not the case in the NSM V1R3 AS/400 environment where user files are, by default, saved in the /QIBM/UserData/NetworkStation/users/<user name>/ directory. All of its content is migrated to the NSM V2R1 /QIBM/UserData/NetworkStationV2/home/<user name>/ directory.

Because we are using NVRAM in this case, we manually change our settings in the Network Stations boot menu with respect to the new directory path. We strongly suggest that you do it manually for a few clients to check whether their preferences were migrated correctly. Then, you can use "client migration switch" with Migration Utility `nsmv2migr.exe -C` to perform automatic migration for the rest of your clients.

Note

Extensive information pertaining especially installing and configuring DHCP can be found in *Installing IBM Network Station Manager for Windows NT V2R1*, SC41-0668.

We modify the boot parameters on both our Model 2800 (x86) and Model 1000 (IBM PPC) Network Stations and then reboot them. Since we installed NSM V2R1 with Service Pack 1 a new boot code to our NS Model 2800 was applied, so it booted twice. There is no new boot code for the PPC model at Service Pack 1, so it stayed with code number 3.0.8.8, which it received from NSM V1R3 Service Pack 8.

Both Network Computers started successfully, and after login using different user IDs, they act as they should. Figure 282 shows that all applications started and were placed as we expected. It is very important that both types of the Network Station start in the expected manner. Supported preferences were moved correctly. Preferences that were not supported were disregarded without causing any malfunction of the components with which they are concerned.

Now a few words about `nsmv2migr.exe -C` since it is not well documented. All the Migration Utility is doing is recognizing the operating system environment and writing it to the file named nvram.mig, which is located in the same directory where the V1R3 kernel files are. For Windows NT 4.0, this file contains just five characters “WinNT”. To use this file, your boot monitor has to be at its latest level (Network Station Manager V1R3 with Service Pack 8). The latest boot monitor has been hardcoded to look up the nvram.mig file before loading the kernel. If it finds it, then the boot monitor changes to the new directory paths on-the-fly, causing the Network Computer to boot from the new V2R1 Network Station Manager.

Tip

If you want to return to the previous state (before running `nsmv2migr.exe -C`) simply delete the nvram.mig file and change the Network Computer settings using the Boot Utility for the previous values.

Now we have to check what happened with our backdoor terminal preference file. While running the Migration Utility program, the message shown in Figure 281 appeared in the Windows NT 4.0 prompt.

```
NSM7066
Migration command script created or updated.

The migration command script C:\NetworkStationV2/userbase/profiles/migrate.scr
has been created or updated. This script contains commands that contain the
settings from the user edited settings files from the previous version of the
IBM Network Station Manager. To update the settings for the current version with
the settings contained in the script, the script must be processed by the IBM
Network Station Manager Command Line utility.
```

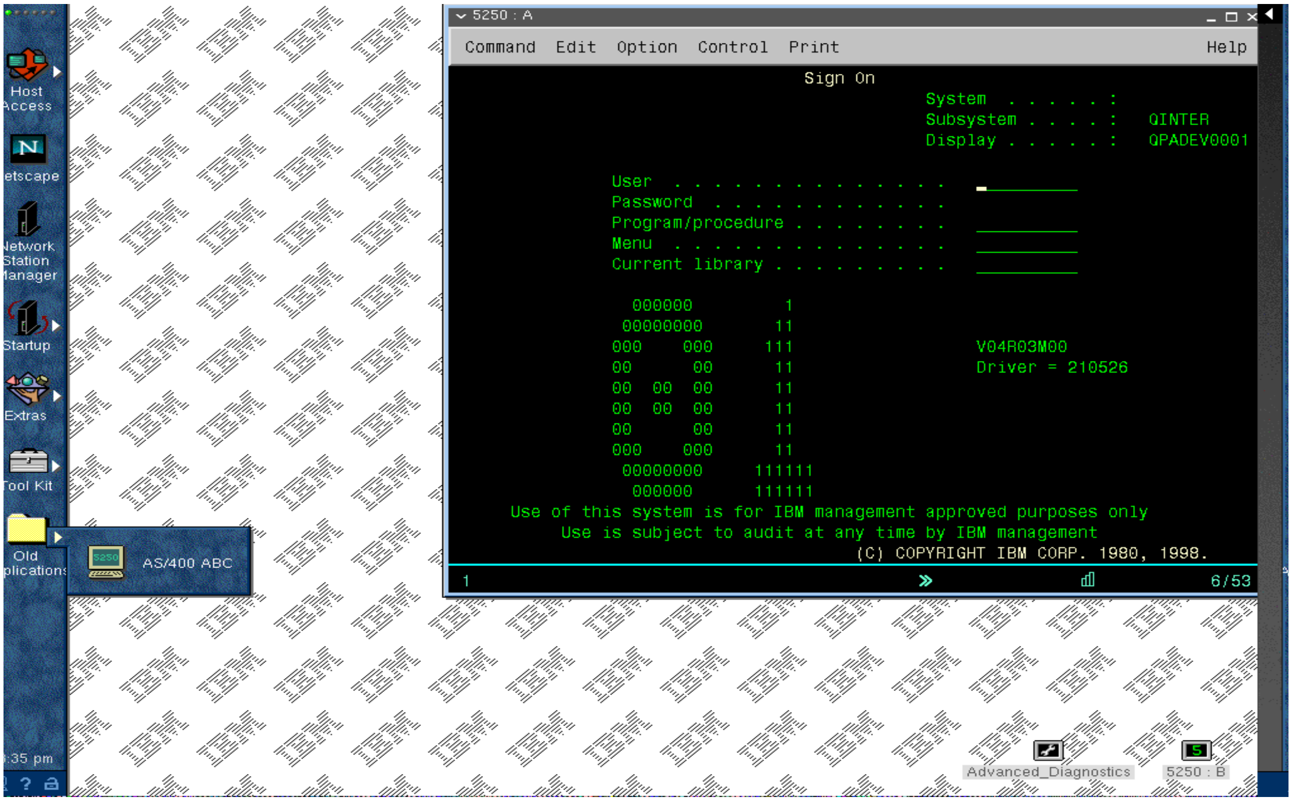
Figure 281. Informational message that backdoor preference file was found and processed

If we open it, we see the following statement generated by the NSM V2R1 Migration Utility program line:

```
INSERT IBMNSM/WORKSTATION/9.5.92.60/WORKSTATION/unit-contact/Ryszard
PytkoCOMMIT
```

As you can see, the manually entered line `set unit-contact="Ryszard Pytko` has been converted to a comprehensible Command Line Utility format. The spaces before and after the configuration value are not mandatory.

Finally, we start new the hardware (Model 2800, Token-Ring) and log on with the same <user name> as we used to do. The result is exactly the same as we had before (Figure 282).



```
                                   Sign On
                                          System  . . . . . :
                                          Subsystem . . . . :   QINTER
                                          Display . . . . . :   QPADEV0001

               User  . . . . . . . . . . . . . .      _
               Password  . . . . . . . . . . . .
               Program/procedure . . . . . . . .      __________
               Menu  . . . . . . . . . . . . . .      __________
               Current library . . . . . . . . .      __________

                 000000         1
                00000000       11
               000     000     111               V04R03M00
               00       00      11               Driver = 210526
               00  00   00      11
               00  00   00      11
               00       00      11
               000     000      11
                00000000      111111
                 000000       111111
          Use of this system is for IBM management approved purposes only
               Use is subject to audit at any time by IBM management
                                        (C) COPYRIGHT IBM CORP. 1980, 1998.
 1                                          »                 6/53
```

Figure 282. System Network Station Model 2800 and Model 1000

10.2.2 Case 2: AS/400 system environment

In the AS/400 system environment, there is no possibility to run the Migration Utility during the installation or configuration process. For testing purposes, we prepare identical settings in V1R3 NSM as shown in the previous section for Windows NT 4.0.

To start the AS/400 System Migration Utility, you have to be logged on to the AS/400 system, on any terminal screen, as a user with *SECOFR (Security Officer user class) specified in its user profile. More specifically, it can be any user with *ALLOBJ special authority. We do it using eNetwork Personal Communication Program Version 4.2 for Windows 95 and Windows NT. After signing on, type a command in the AS/400 prompt. Due to migrating all V1R3 preferences, we type the following command:

```
CALL PGM(QYTCV2/QYTCMUMU) PARM('-A')
```

When this program ends, you should enter a few more commands to see or print its results:

- `DSPJOBLOG OUTPUT(*PRINT)`

  The Display Job Log display shows you the commands processed by the job and the messages returned from running those commands.

- `DSPJOB OPTION(*SPLF)`

  Select this option to display information about the job's spooled input or output files.

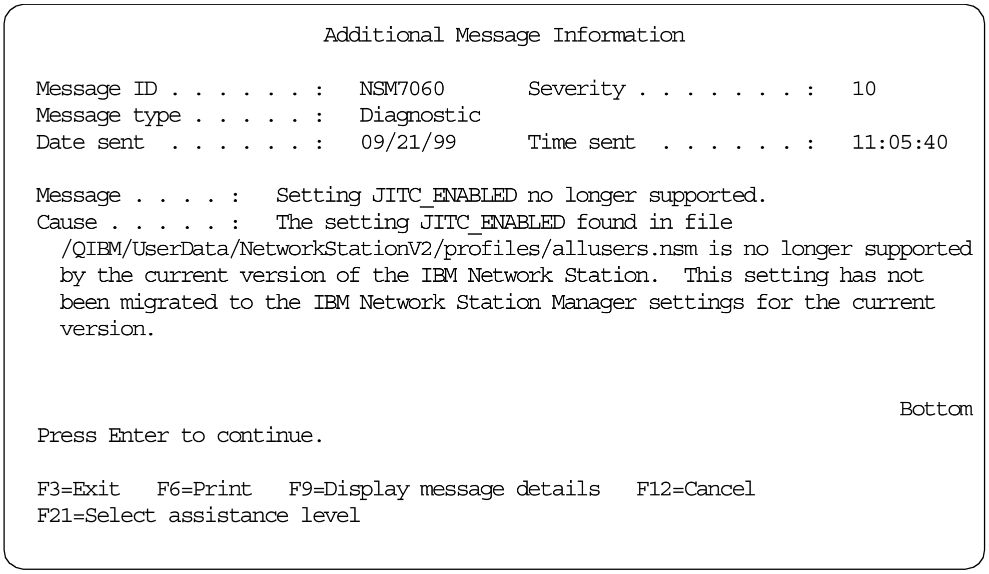
If you want to print your job log, type the following command:

```
WRKOUTQ QEZJOBLOG
```

Press F18, which moves you to the end of this output queue. At the last entry, select the following options in order:

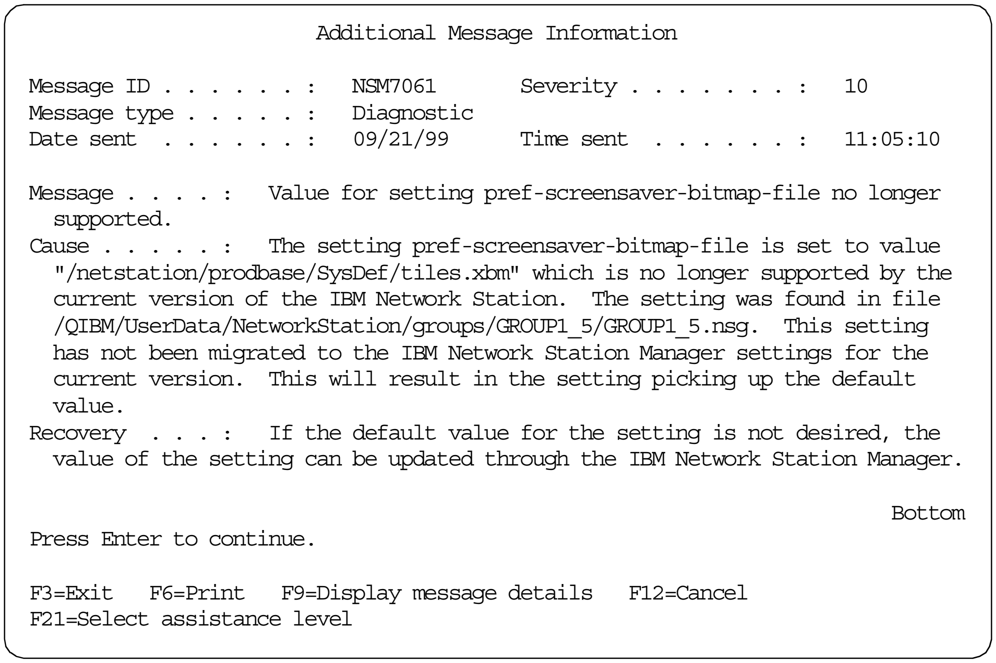
1. Option **9**, Work with printing status
2. Option **2**, Change status; press F4
3. Option **1**, Select
4. A proper printer

Figure 283 and Figure 284 show examples of AS/400 messages you can see during migration.



```
                         Additional Message Information

 Message ID . . . . . . :   NSM7060       Severity . . . . . . . :   10
 Message type . . . . . :   Diagnostic
 Date sent  . . . . . . :   09/21/99      Time sent  . . . . . . :   11:05:40

 Message . . . . :   Setting JITC_ENABLED no longer supported.
 Cause . . . . . :   The setting JITC_ENABLED found in file
   /QIBM/UserData/NetworkStationV2/profiles/allusers.nsm is no longer supported
   by the current version of the IBM Network Station.  This setting has not
   been migrated to the IBM Network Station Manager settings for the current
   version.


                                                                        Bottom
 Press Enter to continue.

 F3=Exit   F6=Print   F9=Display message details   F12=Cancel
 F21=Select assistance level
```

Figure 283. Message logged when preference no longer supported



```
                         Additional Message Information

 Message ID . . . . . . :   NSM7061       Severity . . . . . . . :   10
 Message type . . . . . :   Diagnostic
 Date sent  . . . . . . :   09/21/99      Time sent  . . . . . . :   11:05:10

 Message . . . . :   Value for setting pref-screensaver-bitmap-file no longer
   supported.
 Cause . . . . . :   The setting pref-screensaver-bitmap-file is set to value
   "/netstation/prodbase/SysDef/tiles.xbm" which is no longer supported by the
   current version of the IBM Network Station.  The setting was found in file
   /QIBM/UserData/NetworkStation/groups/GROUP1_5/GROUP1_5.nsg.  This setting
   has not been migrated to the IBM Network Station Manager settings for the
   current version.  This will result in the setting picking up the default
   value.
 Recovery  . . . :   If the default value for the setting is not desired, the
   value of the setting can be updated through the IBM Network Station Manager.

                                                                        Bottom
 Press Enter to continue.

 F3=Exit   F6=Print   F9=Display message details   F12=Cancel
 F21=Select assistance level
```

Figure 284. Message logged when value no longer supported

As with 10.2.1, “Case 1: Windows NT 4.0 (single server migration)” on page 292, we did not encounter any problems with the Migration Utility. All preferences from NSM V1R3 were transferred successfully to NSM V2R1.

10.3 Tips and recommendations

The Migration Utility enclosed in the Network Station is a relatively easy-to-use and efficient tool. It lets you migrate all preferences set up by NSM V1R3 and supported by NSM V2R1. A desirable feature of NSM V2R1 is that you can make a smooth transition from NSM V1R3 to NSM V2R1 through the coexistence stage.

After installing your new software and migrating preferences to NSM V2R1 (at this point, your NSM V1R3 still works normally unless you deleted it), you should carefully consider your memory and network potential bottleneck. If you intend to use new hardware (2200 and 2800), you must use the new NSM V2R1.

Important note

According to IBM Software Announcement 299-259, support for Model 1000 will be provided with Service Pack 2, which was expected in mid November 1999. For the Model 300 (Ethernet and Token-Ring), support should be provided in the first quarter 2000.

The choice between single server or dual server migration should be made individually based on actual and desired hardware configuration. In dual server migration, a case -P switch used with the Migration Utility lets you specify a previous preference files directory. You must remember (Windows NT, dual server migration) to create users and appropriate groups before running the Migration Utility.

Typically dual server migration is used when you want to set up quite a new, much more powerful server (frequently done in a Windows NT Server 4.0 environment). In other cases (OS/400, AIX), usually the single server migration procedure is applied.

Chapter 11. Java environment

This chapter discusses the Java environment that NSM V2R1 brings to Network Station and the capabilities it provides. Before we introduce the NSM V2R1 Java environment, we set the scene by giving a brief overview of the NSM V1R3 Java environment.

11.1 NSM V1R3 Java environment

NSM V1R3 included only a single Java Virtual Machine (JVM). It was based on JDK 1.1.4. The browser included in NSM V1R3, NC Navigator 3.0, did not include its own JVM. This single JVM was used whenever the Network Station executed a Java application or a Java applet, regardless of how the applet was invoked. See Figure 285 for an overview of the NSM V1R3 Java environment.

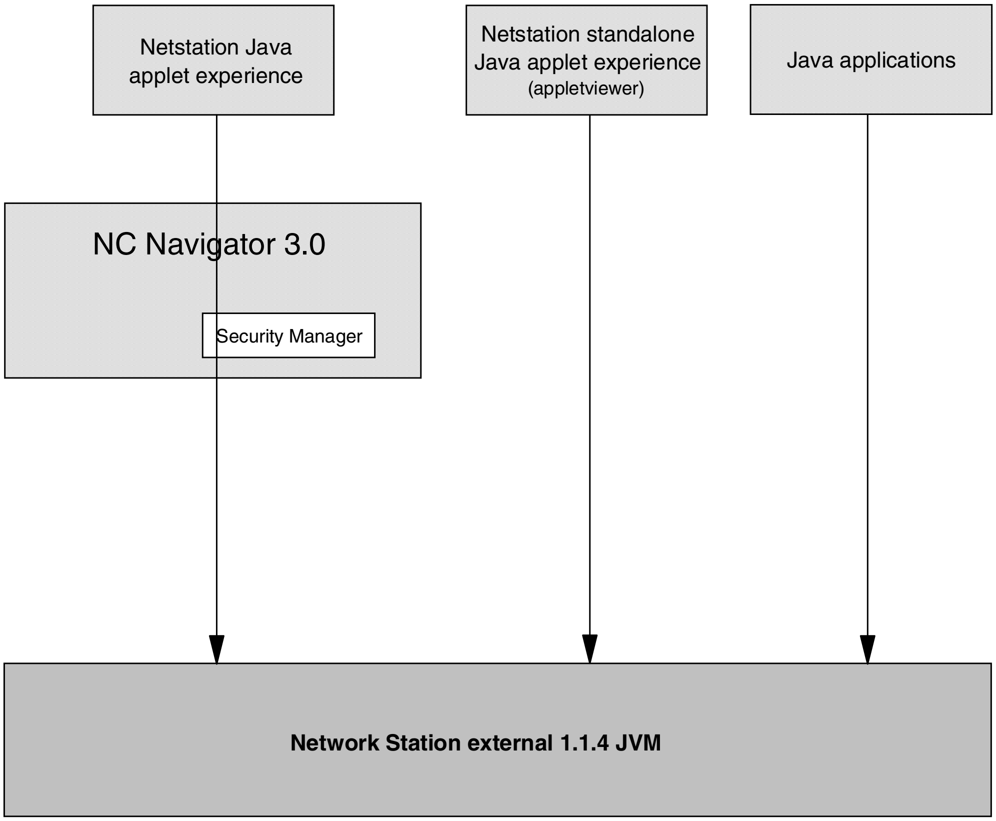

Netstation Java applet experience
Netstation standalone Java applet experience (appletviewer)
Java applications
NC Navigator 3.0
Security Manager
Network Station external 1.1.4 JVM

Figure 285. NSM V1R3 Java environment overview

To distinguish between the different ways to run Java applets and applications, we introduce a new term, the *experience*. This is not a generic Java term. We just use it here for our own purposes. In the case where the browser launches the Java applet through the APPLET HTML tag, we call it the *Netstation Java applet experience*. If the applet is launched outside of the browser, running in the appletviewer, we call it the *Netstation standalone Java applet experience*. In the case where the Network Station runs a Java *application*, we simply call it *Java applications*. In the last two cases, the NC Navigator 3.0 browser is not involved at all.

The operating system in V1R3 caused the Java environment to have some limitations. The most apparent was that only one invocation of the Java Virtual Machine could be run at a time, it was not possible to run multiple JVMs in parallel. This led to the fact that only one Java application could run at a time. However, it was possible to run multiple Java applets since they all ran within that single JVM. It was not possible to run both a Java application and one or more Java applets at the same time. It was either one Java application or one or more Java applets.

These limitations have now been overcome with the introduction of the NSM V2R1 Java environment.

11.2 NSM V2R1 Java environment

NSM V2R1 introduces a *significantly* more capable Java environment than NSM V1R3, so now the annoying limitations of V1R3 are now gone. Figure 286 shows an overview of the NSM V2R1 Java environment.

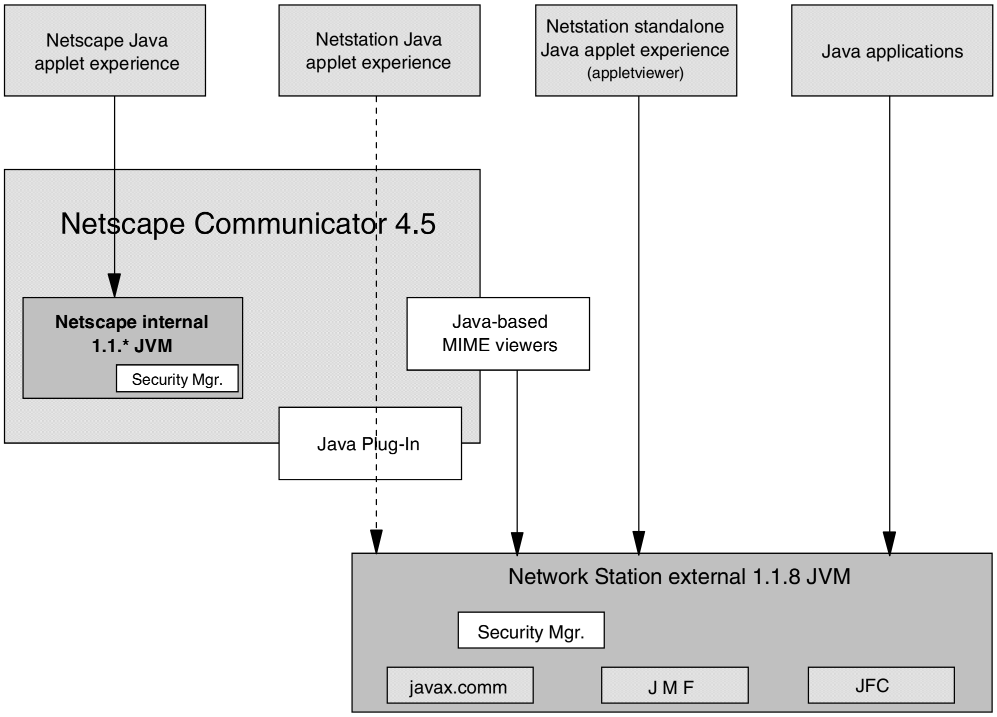

Netscape Java applet experience
Netstation Java applet experience
Netstation standalone Java applet experience (appletviewer)
Java applications
Netscape Communicator 4.5
Netscape internal 1.1.* JVM
Security Mgr.
Java-based MIME viewers
Java Plug-In
Network Station external 1.1.8 JVM
Security Mgr.
javax.comm
J M F
JFC

Figure 286. NSM V2R1 Java environment

The browser included in NSM V2R1, Netscape Communicator 4.5, comes with its own internal JVM, which is the same JVM found in Netscape Communicator 4.5 on any other platform. This internal JVM is based on JDK 1.1 and provides full compatibility with Netscape Communicator 4.5 on other platforms. When Java applets are launched from the APPLET HTML tag and run in this internal JVM, we call it the *Netscape Java applet experience*. This is the default behavior for applets launched from Web pages visited by the browser.

In addition to the Netscape internal JVM, there is also an external JVM (as in NSM V1R3). This JVM is significantly upgraded and is now the IBM enhanced JVM, based on JDK 1.1.8, with some additional features and bug fixes.

Netscape Communicator 4.5 also supports the Sun Microsystems Java Plug-In technique that allows the browser to select in which JVM applets should run. The browser supports both the Sun Microsystems' proposed HTML tags for selecting the external JVM. In addition to this, NSM now also has a setting that enables the selection of which JVM to use. In 12.3.2, "Configuring generic settings through NSM" on page 337, we describe how to use the NSM setting for selecting between the two JVMs. If the Java Plug-In capability is used to redirect applets to the external JVM, we call it the *Netstation Java applet experience*. While this in some cases may impact the compatibility, it provides additional features and enhancements coming from the external JVM higher JDK level and added features.

The browser now also has the ability to map MIME types to external helper applications. When these are written in Java, they *always* run in the IBM enhanced external JVM, never in Netscape's internal JVM. For more information on how to configure Netscape MIME types, see 12.6, "Java-based MIME viewers" on page 357.

As in NSM V1R3, Java applets can also be launched outside of the browser and run in the appletviewer. We then call this the *Netstation standalone Java applet experience*. Applets launched outside of the browser *always* use the IBM enhanced external JVM, and the browser is not involved at all.

All applets that run in the IBM enhanced external JVM all run in the *same* instance of this JVM. This happens regardless if they are launched from the browser and redirected using the Java Plug-In or launched separately in the appletviewer.

Finally, Java *applications* always run in the IBM enhanced external JVM. We simply call this *Java applications*. Each application always runs in its own instance of the JVM. When multiple Java applications are to be run simultaneously, multiple JVM are (automatically) started to support them.

Table 47 on page 308 offers a short comparison between the functions provided by these two distinct JVM environments.

Table 47. JVM functional comparison

Java environment	Netscape Java applet experience	Netstation Java applet experience	Netstation standalone Java applet experience	Netstation Java experience
Function	-JDK 1.1.* -LiveConnect -HTTP authentication -HTTPS support -SOCKS support	-JDK 1.1.8 -javax.comm -JMF -JFC -Native extensions	-JDK 1.1.8 -javax.comm -JMF -JFC -Native extensions	-JDK 1.1.8 -javax.comm -JMF -JFC -Native extensions
Configuration	-ARCHIVE tags in HTML (limited by security) -Uses Netscape's CLASSPATH	-Applet environment CLASSPATH and settings	-Applet environment CLASSPATH and settings	-Individual application CLASSPATHs
Security	-Netscape's security model -Netscape capability APIs	-Java's security model	-Java's security model	-Java's security model
Other	-Netscape compatible		-Browser not needed -Requires less memory -Applets load faster	

Comments:

- In the Netstation standalone Java applet experience (appletviewer), the Netscape Communicator 4.5 browser is not involved. The applets run in the appletviewer and are configured through NSM (but still use an HTML page for their description). Since the browser is not needed, the Network Station can use less memory. If only a few applets are to be used, this may be a faster way of loading them, since the entire browser does not have to be loaded.
- As mentioned before, *all* applets that run in the IBM enhanced JVM all run in the *same* instance of this JVM. This means they all use the *same* CLASSPATH variable, regardless of how they are invoked. This classpath is, however, separated from the Netscape Communicator's classpath, which is used for applets running in its internal JVM. In addition to sharing the CLASSPATH variable, it also means that applets running in the IBM enhanced external JVM use the same settings for garbage collection, byte-code verification, memory configuration, etc.
- When applets run in the Netscape Communicator's internal JVM, they must conform to Netscape's security model. When applets run in the IBM enhanced external JVM, they must conform to the common Java security model. Both Java 1.1 and Java 2 security models are supported by this JVM.

11.2.1 New features in the NSM V2R1 Java environment

The NSM V2R1 Java environment brings a significantly more capable Java environment to the Network Station. Some of the most notable features are:

- **Support for multiple concurrent Java applications**
  The only-one-Java-application-at-a-time limitation is now gone. The NSM V2R1 operating system supports invocation of multiple JVM, running concurrently. Each JVM can run one Java application, which enables the Network Station to run multiple Java applications simultaneously. This also allows the Network Station to run both Java applications and one or more Java applets simultaneously. It even allows Netscape Communicator to run applets both in its internal JVM and in the IBM enhanced external JVM simultaneously.
- **Better compatibility with Netscape Communicator Java environment**
  Since NSM V2R1 Netscape Communicator 4.5 now includes "the real"

Netscape Communicator 4.5 JVM, full compatibility with applets running in Netscape on other platforms is provided.

- **Higher level of JDK**
  The IBM enhanced JVM is now at JDK 1.1.8 level (instead of 1.1.4).
- **Support for Java Communications Extensions, javax.comm**
  The javax.comm class library is used when Java applications communicate with the Network Station's serial and parallel ports.
- **Support for Java Media Framework (JMF)**
  The JMF class library is used for Java multi-media applications.
- **Support for Java Foundation Classes (JFC)**
  The JFC class library is used to write more "visually appealing" applications.
- **Complete JDK**
  The IBM enhanced 1.1.8 JVM is not only a Java Run-time Environment (JRE) but really a complete Java Developer's Kit (JDK). This means it includes the **javac** Java compiler so developers can actually compile Java applications *on* the Network Station.
- **Support for signed applets and JAR files**
  Signing is a technique used to grant a Java applet extended permissions. The NSM V2R1 Java environment supports both Netscape's signing technique (when the applets run in Netscape Communicator's internal JVM) and Java's common signing technique (when the applets run in the IBM enhanced external JVM).

11.2.2 Enhancements to the IBM enhanced JVM

The IBM enhanced JVM in NSM V2R1 includes some enhancements not found in Sun Microsystems' original Java 1.1.8 specification. Some of the most notable enhancements are:

- Memory management fixes and integration with the Network Station's operating system
- Euro currency support
- Enhanced security that supports the security model of Java 2 (Java 1.2) in addition to the Java 1.1 security model

Note

The NSM V2R1 Java environment does *not* include Java Just-In-Time Compiler (JITC) at this time.

11.3 Java glossary

For those not familiar with the Java language and all its acronyms, we compiled a short glossary, which may be useful before we continue.

11.3.1 Java Plug-In: Choosing JVM for the Netscape browser

To overcome the incompatibilities between different Java implementations in various browsers, that is Netscape Communicator and Internet Explorer, Sun Microsystems has developed the Java Plug-In module (formerly called the Java

Activator). This enables a Web browser to launch an external JVM instead of the shipped internal one whenever a Java applet is to be run. The selection between which JVM to use is done by adding special HTML tags in the HTML page that describes the applet. No modifications to the applets themselves are necessary. In addition to having a common JVM for different browsers, the Java Plug-In also enables the browsers to use an up-to-date JVM without modification to the browsers themselves.

The NSM V2R1 Java environment supports the Java Plug-In HTML tags for selecting which JVM the applets should run in. In addition, it also has a setting in NSM that can redirect *all* applets launched from the Web browser to the IBM enhanced external JVM, regardless of the HTML coding used to describe them.

The first option, using the HTML tags, makes it possible to redirect only certain Java applets to the IBM enhanced external JVM, while some still continue to run in the browser's internal JVM. While this increases flexibility, it also means that all Web pages used to launch applets, that is to run in the external JVM, must be modified.

The second option, using the NSM setting, means that all applets run in the IBM enhanced JVM and then no Web pages need to be modified.

Note

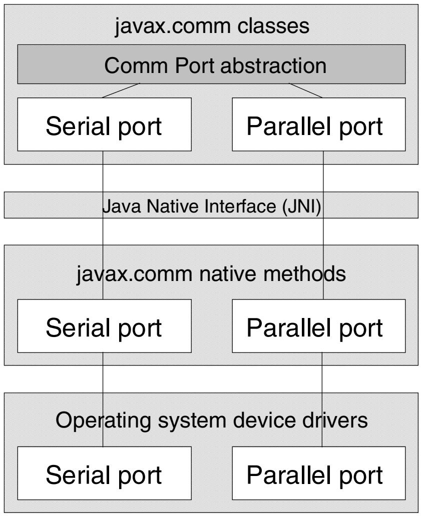
For more information on the Java Plug-In and a complete description of how to modify the HTML code, visit Sun Microsystems' Java Plug-In page at: `http://java.sun.com/products/plugin`

11.3.2 Javax.comm: Java Communications Extensions

The IBM enhanced JVM supports the javax.comm additions as proposed in Sun Microsystems' Java language specifications. This enables Java applets and applications to communicate with the Network Station's serial (RS-232) and parallel (IEEE 1284) ports, using the standard Java communications API. In addition to this, it can also be used to communicate with the internal Smart Card reader on the Network Station S1000. The serial and parallel ports are identified with the well-known PC names: COM1, COM2, LPT1, LPT2, LP0, LP1, TTYa, TTYb, and so on.

When using the javax.comm API, Java applications do not need to use the Java Native Interface (JNI) to communicate with the ports. This improves the compatibility and maintains the platform independence of the Java applications (JNI is one of the things that, if used, ties a Java application to a specific platform).

Figure 287 gives an overview of the javax.comm implementation.



Provides Java general I/O interface capabilities.
Provides Java APIs for specific device control.
Maps to Java Native Interfaces.

Provides specific device control function.
Maps Java to native device driver interfaces.

Implements native device driver.

Figure 287. javax.comm implementation

The javax.comm is supported by the IBM enhanced JVM only.

Note

For more information on the Java Communications Extensions, visit Sun Microsystems' Java Communications Extensions page at: `http://java.sun.com/products/javacomm`

11.3.3 Java Media Framework (JMF)

The Java Media Framework (JMF) is a class library used for developing multi-media applications in Java. As with the rest of the Java language, the JMF is platform independent.

NSM V2R1 includes the JMF 1.1., which was jointly developed by IBM and Sun Microsystems. It includes three versions: an all-Java version, a Windows version, and a Solaris version. The version included in NSM V2R1 is based on the all-Java version, with two native components ported from the Solaris version: the Cinepak video decoder and the xlib video blitter.

The JMF supports a wide range of audio and video protocols (including WAV, QuickTime, and AVI). It can receive the data both via the file system or via FTP, HTTP, or RTP (the Internet Real-Time Protocol, used for streaming audio and video). JMF 1.1 is a playback-only API (recording is only supported in JMF 2.0).

The JMF is supported by the IBM enhanced JVM only.

Note

For more information on the Java Media Framework, visit Sun Microsystems' Java Media Framework page at: `http://java.sun.com/products/java-media/jmf`

11.3.4 Java Foundation Classes (JFC)

Since its origin, Java has included a windowing toolkit called the Abstract Windowing Toolkit (AWT). Using this toolkit, programmers can create graphical user interfaces using windows, click buttons, menus, and so on.

The AWT is platform independent, which is the same of all Java languages. Due to the variations in graphics capabilities of different platforms, the AWT has had to implement only the lowest common denominator of the functions provided by all platforms. Therefore, the AWT has not supported, for example, the popular tree-list view that Windows 95/NT have (Windows Explorer for example). Also, Java applications written for the AWT toolkit have not had the same look and feel as other applications running natively on a particular platform. Therefore, Java applications have been considered somewhat ugly or dull, by some people.

To overcome these limitations, Sun Microsystems have developed a much more capable class library for developing graphical user interfaces, called the Java Foundation Classes (JFC). The JFC consists of the following parts:

- **Swing classes**: These classes include replacement classes for the AWT class library. The Swing classes also provide many more useful GUI components.
- **Accessibility API**: This API gives components a standard interface so they can be displayed to disabled users in an easily understood way.
- **Java 2D classes**: These classes provide Java with better fonts and drawing capabilities.
- **Drag-and-drop**: This feature lets programmers add the (these days almost vital) drag-and-drop features to their applications.

The JFC is supported by the IBM enhanced JVM only.

Note

For more information on the Java Foundation Classes, visit Sun Microsystems' Java Foundation Classes page at: `http://java.sun.com/products/jfc`

11.3.5 Internet Foundation Classes (IFC)

Before Sun Microsystems developed the Java Foundation Classes, Netscape developed their own class library that tried to accomplish the same thing. This was called the Internet Foundation Classes (IFC) and was incorporated into Netscape's internal JVM.

When developing the JFC, Sun Microsystems invited Netscape to take part of the project and Netscape did. This has led to the fact that the IFC is now discontinued and was more or less replaced by the JFC.

The IFC is supported by the Netscape Communicator's internal JVM only.

11.3.6 Internet Inter-ORB Protocol (IIOP)

The Internet Inter-ORB Protocol (IIOP) is an object-oriented transport protocol that allows distributed programs written in different programming languages to communicate with each other over the Internet. IIOP is an important part of the Common Object Request Broker Architecture (CORBA).

CORBA and IIOP are similar to the Distributed Component Object Model (DCOM) developed by Microsoft for the Windows platform.

The IIOP is supported by the Netscape Communicator's internal JVM only.

11.4 Java environment variables

The NSM V2R1 Java environment uses a number of environment variables for configuring the Java environment. If you issue a set command from the Advanced Diagnostics window, you see a list of all environment variables, several of which deal with Java. You do not need to change these, but for diagnostic purposes, they may provide you with valuable information. Some of these variables are:

- **CLASSPATH**: This environment variable specifies the path that the JVM will search for Java classes. By default it has the value of`/usr/local/java/J118/lib/classes.zip:.`

  Note: There is a dot after the colon.

- **JAVA_LEVEL**: This environment variable specifies which external JVM to use. The default value is `J118`, meaning the IBM enhanced 1.1.8 JVM is to be used. When IBM ships new JVMs (perhaps even beta level JVMs), they can simply be installed into the NSM directory structure and the JAVA_LEVEL environment variable be changed to reflect the new directory to activate the new JVM. This can be very useful for developers wanting to test their applications under different JVM levels. See also JAVA_HOME.

- **JAVA_HOME:** This is the actual path from where the external JVM is loaded. It expands its value from the `/usr/local/java/${JAVA_LEVEL}` into `/usr/local/java/J118`.

- **NETSCAPE_JAVA_ARGS**: The Netscape Communicator can use its own classpath, and the NETSCAPE_JAVA_ARGS environment variable specifies its value. The NETSCAPE_JAVA_ARGS variable *only* sets the classpath for Netscape's internal JVM. By default, it has the following value (split into multiple lines here for easier reading):

  ```
  /usr/local/netscape/java/classes/java40.jar:
  /usr/local/netscape/java/classes/jae40.jar:
  /usr/local/java/
  ```

11.5 Viewing output from Java applets and applications

Both Java applets and applications can write messages to the standard output, stdout. At the time of this writing, there was no Java console available in NSM V2R1 for Java applications or applets using the appletviewer. To view the stdout messages from a Java application or applet, execute the Java application or applet from the Advanced Diagnostics command line (see 11.8, "Using the Advanced Diagnostics shell to run Java" on page 327).

Java applets run from the browser have a Java console available. In the browser window, click **Communicator->Tools->Java Console**.

11.6 Configuring NSM to run a Java application example

In this section, we describe the steps necessary to get a simple Java application up and running. We perform these steps on a normal Windows NT 4.0 server (that also happened to be our Network Station boot server, running Network Station Manager V2R1). If you are using the AS/400 system or AIX as a server, these steps need to be modified to reflect the path names for those platforms.

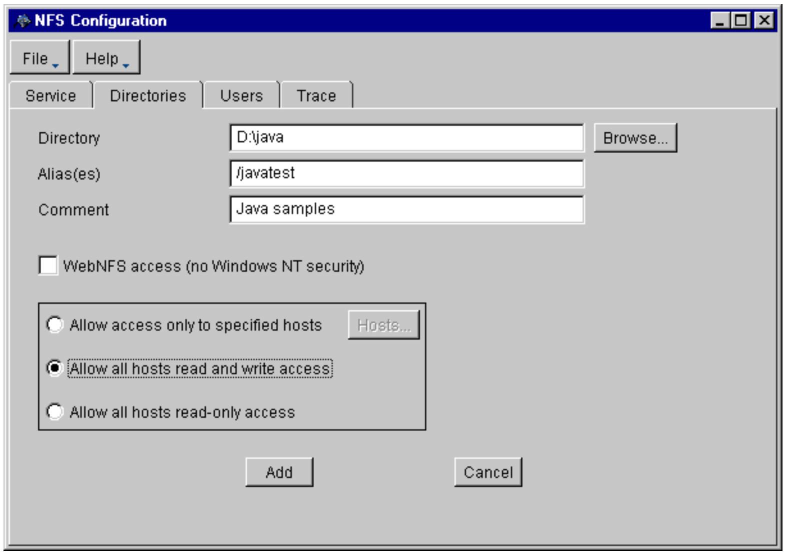
For demonstration purposes, we wrote a simple Java application that displays all the Java system properties in a window as well as prints them to the standard output. We call the application SysInfo. The source code for the application is shown here:

```
import java.awt.*;
import java.awt.event.*;
import java.util.*;

public class SysInfo extends Frame {
 public void paint(Graphics g) {}

 public SysInfo() {
   String property, value;
   TextArea ta = new TextArea(40,40);
   ta.setBackground(Color.white);
   ta.setEditable(false);
   add(ta, "Center");
   ta.append("Java application system property values:\n");
   System.out.println("Java application system property values (stdout):");
   Properties s = System.getProperties();
   Enumeration enum = s.propertyNames();
   while (enum.hasMoreElements()) {
     property = (String)enum.nextElement();
     value = s.getProperty(property);
     ta.append(property + " = " + value + "\n");
     System.out.println(property + " = " + value);
   }
 }

 public static void main(String[] args) {
   Frame f = new SysInfo();
   f.setTitle("SysInfo application");
   f.addWindowListener(
     new WindowAdapter() {
       public void windowClosing(WindowEvent e) {
         System.exit(0);
       }
     });
   f.setSize(400,200);
   f.setVisible(true);
 }
}
```

Note the following sequence of actions:

1. To separate our Java application from the rest of the NSM code, we created a new directory on our Windows NT 4.0 server. We named the directory `D:\java` to use for our Java samples. We also copied the Java class file, named SysInfo.class, to this directory.
2. To access this directory from the Network Station, it must be exported using a protocol that the Network Station can use. We chose NFS. Since our directory was on the same server on which we installed Network Station Manager and the eNetwork On-Demand Services (eNOD), we simply used the eNOD NFS

server to export the directory. To start the eNOD NFS Service Configuration, we clicked **Start->Programs->eNetwork OnDemand Server->NFS Server Configuration->Add**. The directories page appears (Figure 288).



Directory D:\java

Alias(es) /javatest

Comment Java samples

□ WebNFS access (no Windows NT security)

○ Allow access only to specified hosts

● Allow all hosts read and write access

○ Allow all hosts read-only access

Figure 288. eNOD NFS server configuration

The fields on the Directories page are explained here:

- **Directory**: This specifies which directory we want to export. We chose the D:\java directory.
- **Alias**: This specifies the NFS alias that the directory will be accessed as. We chose `/javatest/`.

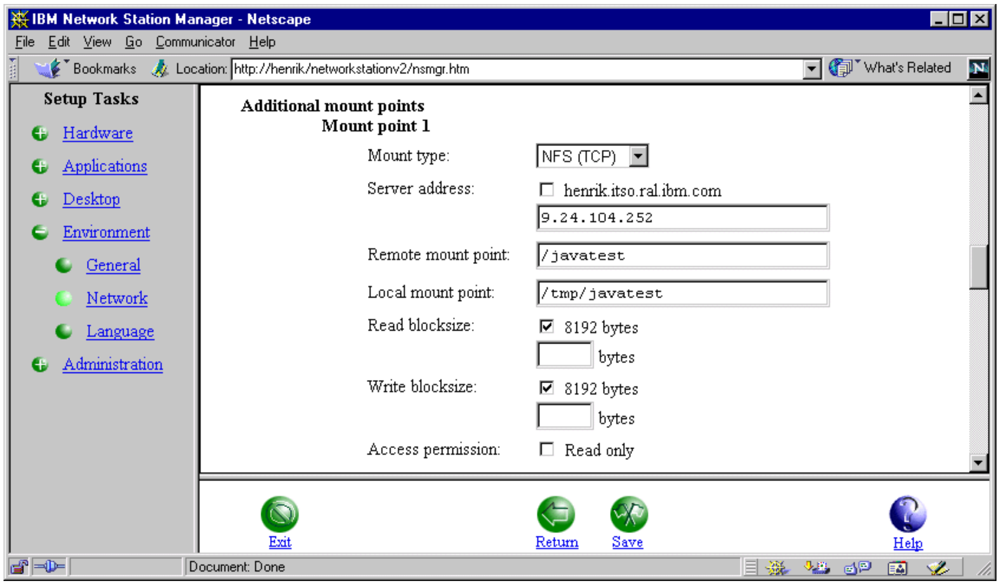
We also allowed clients both read and write access. However, since our Java application did not require write access, read access was enough.

Then, we clicked the **Add** button.

Once these changes were made, we selected **File->Save**. After they were saved, the NFS server needed to be restarted (this is done automatically).

Note: Make sure you don’t do this when users are online and accessing the server via NFS.

3. We wanted to automatically mount the directive which we just exported when a user logs on to the Network Station. To do this, we selected **Environment->Network panel** in NSM.



Additional mount points
Mount point 1

Mount type: NFS (TCP)

Server address: □ henrik.itso.ral.ibm.com
9.24.104.252

Remote mount point: /javatest

Local mount point: /tmp/javatest

Read blocksize: ☑ 8192 bytes
bytes

Write blocksize: ☑ 8192 bytes
bytes

Access permission: □ Read only

Figure 289. Configuring NSM to automount an NFS system

The fields shown in Figure 289 are explained here.

- **Mount Type**: The mount type depends on the server exporting the file system. Since we exported the file system from a Windows NT server, we chose the **NFS (TCP)** option.

Note

The IBM-supported platforms use the following protocols:

- **Windows NT 4**: UDP or TCP NFS
- **AIX**: UDP or TCP NFS
- **AS/400**: RFS

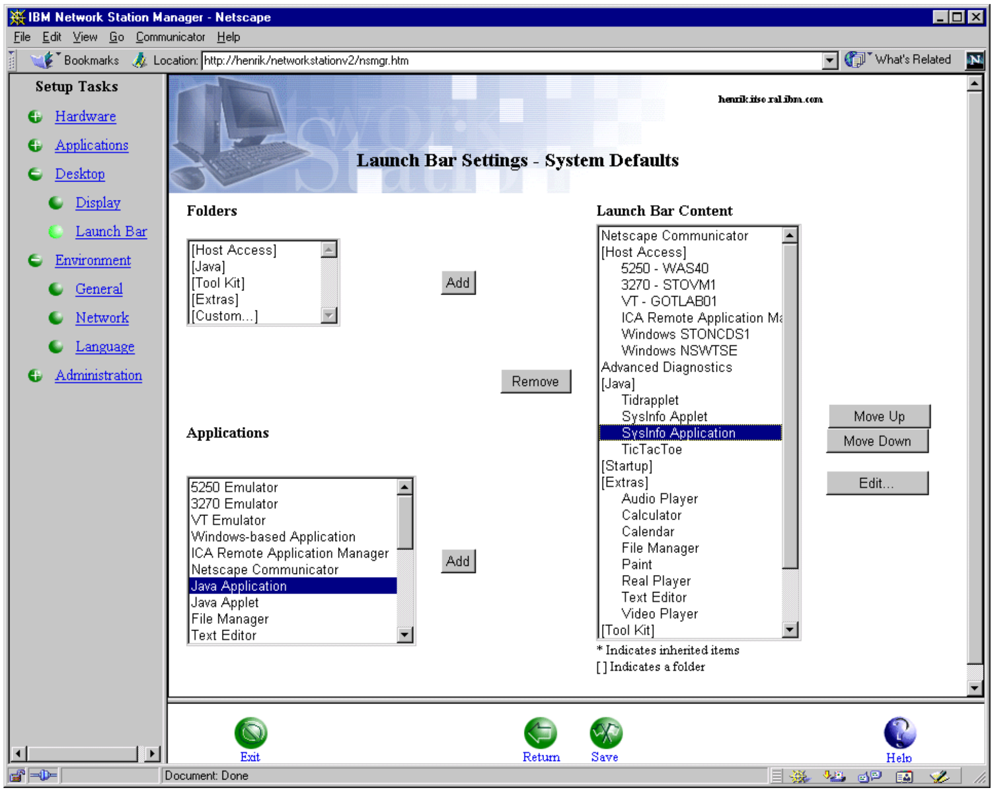
- **Server address**: Specify the IP address or the host name for the server exporting the file system. If it is the same server on which NSM is installed (as in our case), you can use the predefined name by selecting the box (we did not do this because we wanted to test the IP address option).
- **Remote mount point**: The remote mount point is the name (alias) the NFS server exports the file system as. In our example, we exported it as /javatest so we simply entered `/javatest` here.
- **Local mount point**: The local mount point is the name that the NFS file system will be known as *on* the Network Station. This name must *always begin* with /tmp, so we chose the name `/tmp/javatest`.
- **Read and Write block sizes**: The read and write block sizes are the number of bytes used for each read or write access to the file system. We simply chose the default value of 8192 bytes.

Tips

If you experience problems with the NFS file system (perhaps through routers and over WAN links), try reducing the read and write block sizes. Otherwise, use as large values as possible for maximum performance.

- **Access permission**: If the NFS file system is exported with write access permission but you, for security reasons, want to limit it to read-only access, you can do that by selecting this box.

4. The last step is to add and configure a button for our Java application to the NC Launch bar. To do this, we selected **Desktop->Launch Bar** in NSM. The page shown in Figure 290 appeared.



Launch Bar Settings - System Defaults

Folders

[Host Access]
[Java]
[Tool Kit]
[Extras]
[Custom...]

Applications

5250 Emulator
3270 Emulator
VT Emulator
Windows-based Application
ICA Remote Application Manager
Netscape Communicator
Java Application
Java Applet
File Manager
Text Editor

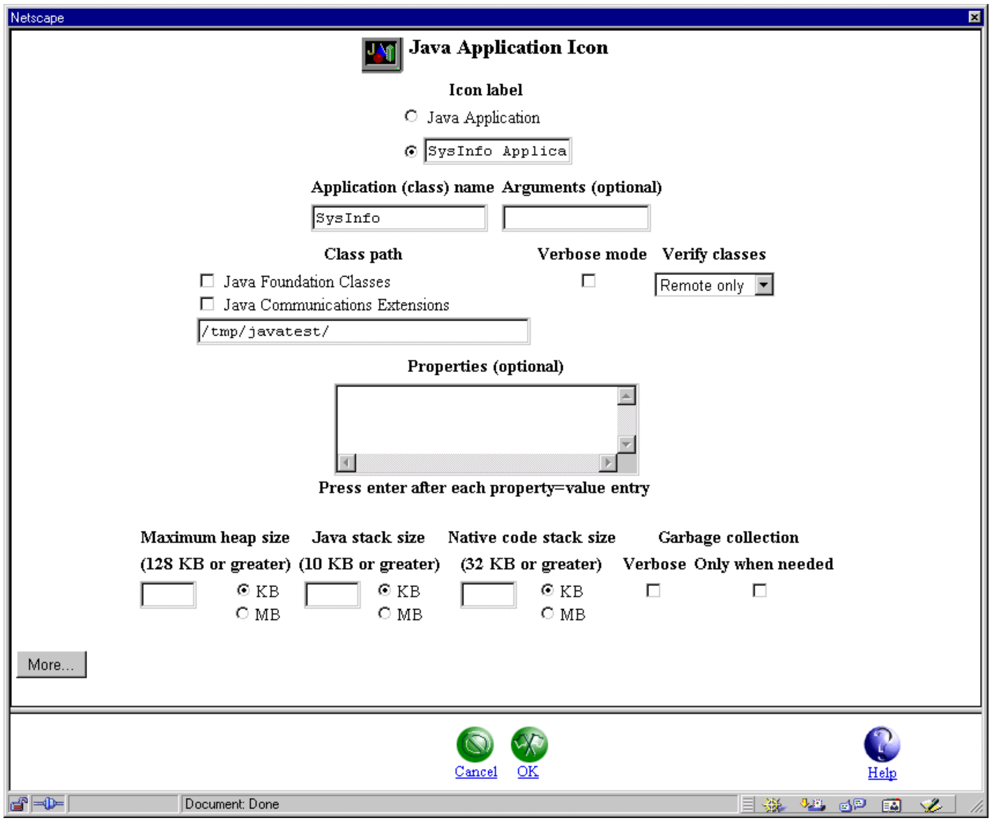
Launch Bar Content

Netscape Communicator
[Host Access]
5250 - WAS40
3270 - STOVM1
VT - GOTLAB01
ICA Remote Application Ma
Windows STONCDS1
Windows NSWTSE
Advanced Diagnostics
[Java]
Tidrapplet
SysInfo Applet
SysInfo Application
TicTacToe
[Startup]
[Extras]
Audio Player
Calculator
Calendar
File Manager
Paint
Real Player
Text Editor
Video Player
[Tool Kit]

* Indicates inherited items
[ ] Indicates a folder

Figure 290. Adding a Java application to the NC Desktop Launch Bar

Then, we selected **Java Application** (under Applications) and clicked the **Add** button. The window shown in Figure 291 on page 318 appeared.



Java Application Icon

Icon label

○ Java Application

● SysInfo Applica

Application (class) name: SysInfo

Arguments (optional):

Class path

□ Java Foundation Classes

□ Java Communications Extensions

/tmp/javatest/

Verbose mode □

Verify classes: Remote only

Properties (optional)

Press enter after each property=value entry

Maximum heap size (128 KB or greater): ● KB ○ MB

Java stack size (10 KB or greater): ● KB ○ MB

Native code stack size (32 KB or greater): ● KB ○ MB

Garbage collection: Verbose □ Only when needed □

Figure 291. Customizing the sample Java application icon

The fields shown in Figure 291 are explained here:

- **Icon label**: Click the second radio button, and enter the name for the button. We chose `SysInfo Application`.
- **Application (class) name**: This is the name of the Java application. It must *not* contain the .class extension. We simply entered `SysInfo`.
- **Arguments (optional)**: If you want to pass arguments to your Java application, you can specify them in the arguments field. Our simple application did not require any arguments, so we left this field blank.
- **Class path**: The class path options include:
  - **Java Foundation Classes**: If your Java application requires the Java Foundation Classes (JFC) class library (for example if you use the Swing package), you should mark this option to add its location to the classpath variable.
  - **Java Communications Extensions**: If your Java application requires the javax.comm class library, you should mark this option to add its location to the classpath variable.
  - **User classpath**: In this field, you *must* enter the path where your Java application's class files are located. If your application requires multiple paths, you can separate them with a colon (:) as with other Java class paths. This information is added to the CLASSPATH variable when your application is being run. We entered `/tmp/javatest`.

- **Verbose mode**: Checking this option causes Java to print a message to the diagnostic log each time a class file is loaded. This can be useful for debugging purposes.
- **Verify classes**: This option determines how the JVM should verify the byte code in the classes it loads. By verifying the byte code, the JVM can validate that the classes conform to the Java language specifications and do not contain viruses or other harmful code. The options are:
  - **All**: The byte-code verifier is run on all classes that are loaded, regardless of where they are located.
  - **Remote only**: The byte-code verifier is only run when classes are loaded from an untrusted location. This is the default value.
  - **None**: The byte-code verifier is never run.

> **Note**
>
> Verifying the byte code will impact the performance when loading the classes and somewhat increase the time it takes to load them.

- **Properties (optional)**: This input field allows you to define specific properties that your Java application can pick up and use, for example: `awt.button.color=green`.

  Make sure you press Enter after each of the properties you enter so there is only one property definition per line.
- **Memory settings**: These settings determine how much memory is allocated to the JVM running your Java application. Increasing the values allocates more memory to your Java application but also uses memory from the Network Station, limiting the number of other applications that can be run. The different memory options are:
  - **Maximum heap size**: This is the maximum amount of memory the JVM allocates to dynamically allocated objects and arrays. Valid values are 128 KB and above. The default value is 6 MB.
  - **Java stack size**: This is the maximum amount of memory allocated to the stack for each thread for running Java code. Valid values are 10 KB and above. The default value is 400 KB.
  - **Native code stack size**: This is the maximum amount of memory allocated to the stack for each thread for running native C or C++ code. Valid values are 32 to 128 KB. The default value is 128 KB.

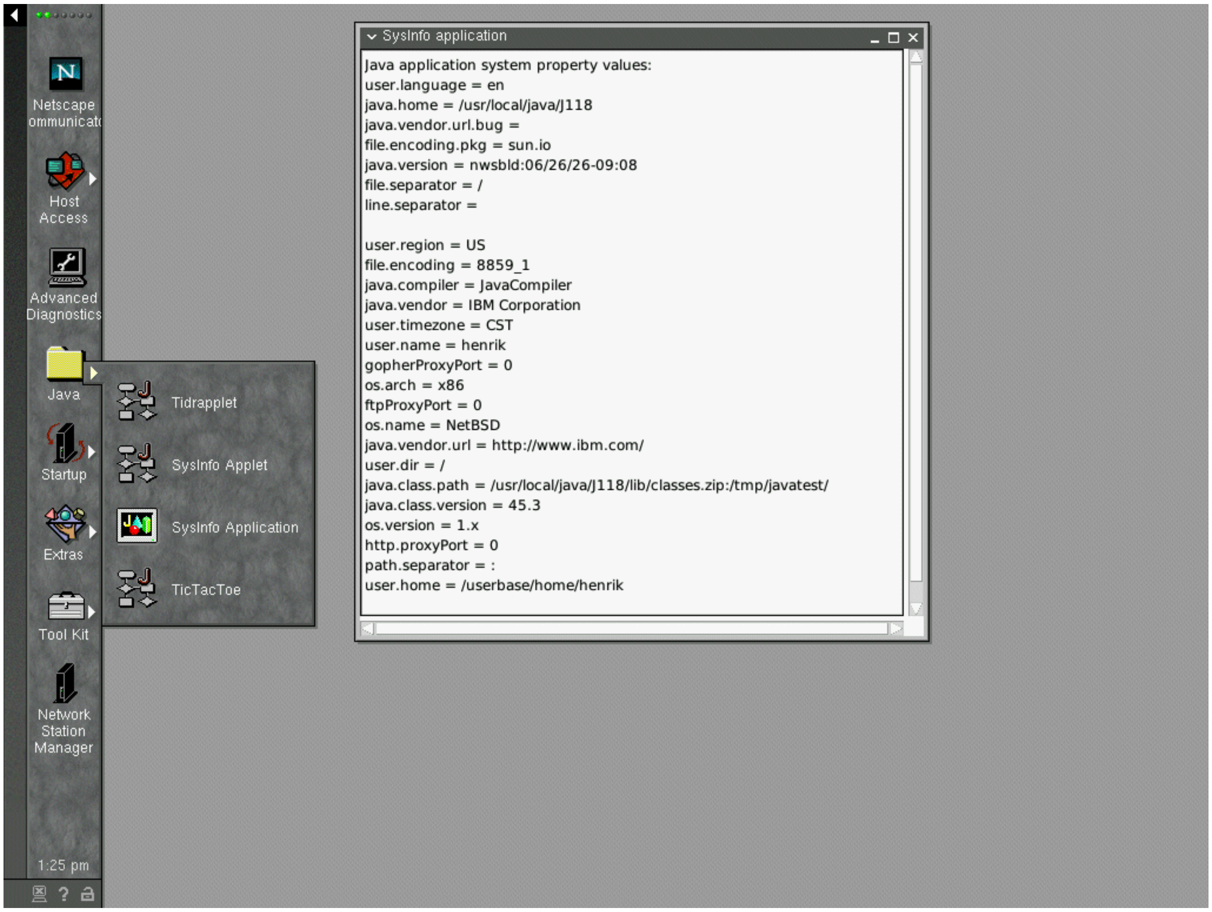
> **Note**
>
> - When specifying the amount of memory for each setting, make sure you also specify if it is MB or KB. For example, don’t specify a Java stack size of 512 MB, when you meant 512 KB.
> - If you experience out-of-memory conditions with your Java application, you can try to increase the amount of memory allocated to it. If you don’t know how much memory your application requires, you may have to experiment a little with these memory settings to get the optimum values for your Java application.

- **Garbage collection**: Garbage collection is Java’s process of reclaiming unused memory and relieving the programmers from that burden. By default, the system runs the garbage collector at unspecified intervals, even though memory may be available. While running, the garbage collector uses some CPU resources from the system and may impact the performance of the running Java applications. It may be desirable to only run the garbage collector when really necessary. The options are:
  - **Verbose**: Checking this item causes the garbage collector to print messages to the diagnostics log whenever it frees memory.
  - **Only when needed**: Checking this item causes the garbage collector to run only when the system is out of heap space.

5. We needed to place the Java application (SysInfo Application) button where we wanted it by using the Move Up and Move Down buttons. We preferred to put it in our Java folder.

11.6.1 Testing the Java application

When all settings were configured, we tested the application. The application displays all the Java system properties. Figure 292 shows that the JDK level is 1.1.8, and our classpath, /tmp/javatest, has been appended to the java.class.path system property variable. The Java application runs in the IBM enhanced 1.1.8 JVM as shown from the java.version property.



```
Java application system property values:
user.language = en
java.home = /usr/local/java/J118
java.vendor.url.bug =
file.encoding.pkg = sun.io
java.version = nwsbld:06/26/26-09:08
file.separator = /
line.separator =

user.region = US
file.encoding = 8859_1
java.compiler = JavaCompiler
java.vendor = IBM Corporation
user.timezone = CST
user.name = henrik
gopherProxyPort = 0
os.arch = x86
ftpProxyPort = 0
os.name = NetBSD
java.vendor.url = http://www.ibm.com/
user.dir = /
java.class.path = /usr/local/java/J118/lib/classes.zip:/tmp/javatest/
java.class.version = 45.3
os.version = 1.x
http.proxyPort = 0
path.separator = :
user.home = /userbase/home/henrik
```

Figure 292. SysInfo Java application

11.7 Configuring NSM to run a Java applet: Example

In NSM V2R1, there are really three different ways to launch and run Java applets, as described at the beginning of this chapter.

Two options involve launching the applets from the browser. This happens automatically whenever the browser detects the APPLET tag in the HTML code. We do not describe that here, except to remind you that the Network Station Netscape browser has, by default, Java disabled. See 12.3.4, “Configuration in the browser itself” on page 347, for more information.

Instead, we describe the steps necessary to get an applet up and running in the appletviewer, which enables it to run completely independent of the browser. This is what we call the *Netstation standalone Java applet experience*.

For demonstration purposes, we wrote a simple Java applet that displays a section of the Java system properties in a window as well as prints them to the standard output. We called the applet SysInfoApplet. The source code for the applet is shown in here:

```
import java.util.*;
import java.awt.*;
import java.applet.*;

public class SysInfoApplet extends Applet {
  public void init() {
    String[] properties = { "java.version",
          "java.vendor",
          "java.class.version",
          "os.name",
          "os.version",
          "os.arch" };
    String value = "";
    TextArea ta = new TextArea(40, 40);
    ta.setBackground(Color.white);
    ta.setEditable(false);
    setLayout(new BorderLayout());
    add(ta, "Center");
    ta.append("Java applet system property values:\n");
    System.out.println("Java applet system property values (stdout):");
    for (int i=0; i<6; i++) {
      value = System.getProperty(properties[i]);
      ta.append(properties[i] + " = " + value + "\n");
      System.out.println(properties[i] + " = " + value);
    }
  }
}
```

The corresponding HTML page that describes the applet is SysInfoApplet.html is shown in Figure 293 on page 322.

```
<html>
  <head>
    <title>SysInfo Applet</title>
    </head>
  <body>
      <h1>SysInfo Applet</h1>
      <hr>
      <applet code=SysInfoApplet.class width=400 height=200>
      </applet>
      <hr>
  </body>
</html>
```

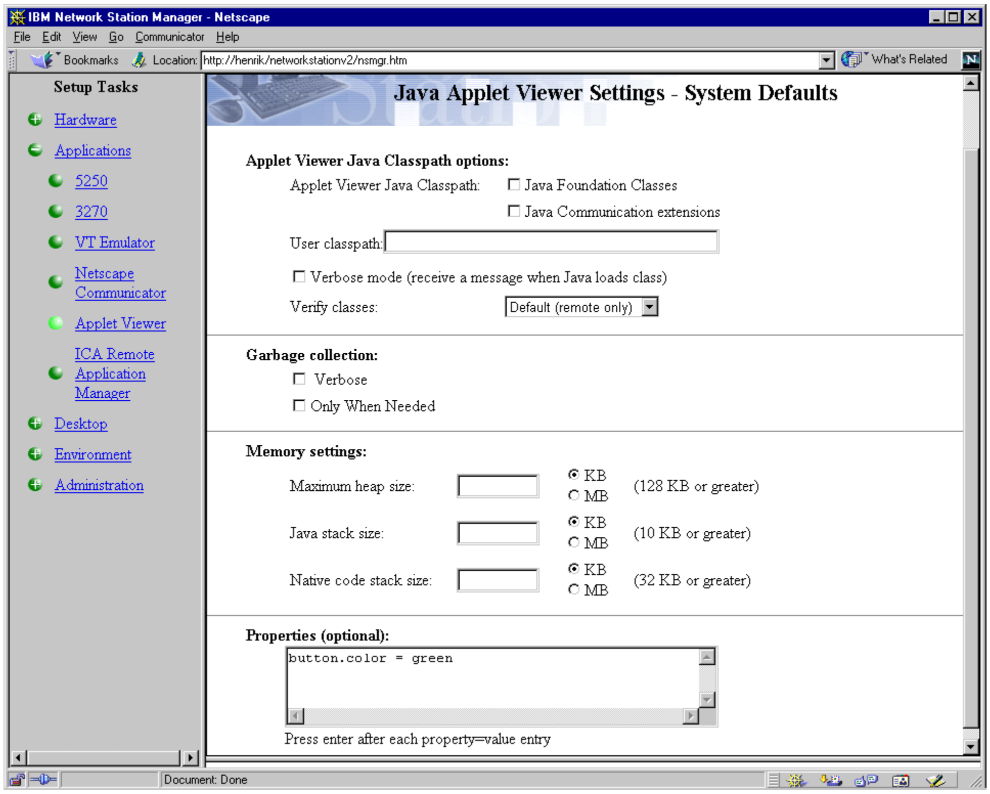
Figure 293. HTML page describing the sample applet

We placed the applet (.class file) and the corresponding HTML code on our Web server so it was accessible using the URL:

`http://henrik/applets/SysInfoApplet.html URL`

11.7.1 Configuring the Applet Viewer

You make generic settings that affect *all* applets running in the appletviewer by selecting **Applications->Applet viewer** in NSM (since they all run in the same instance of the IBM enhanced JVM). The page shown in Figure 294 appears.


IBM Network Station Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://henrik/networkstationv2/nsmgr.htm
What's Related
Setup Tasks
Hardware
Applications
5250
3270
VT Emulator
Netscape Communicator
Applet Viewer
ICA Remote Application Manager
Desktop
Environment
Administration
Document: Done

Java Applet Viewer Settings - System Defaults

Applet Viewer Java Classpath options:

Applet Viewer Java Classpath: □ Java Foundation Classes

□ Java Communication extensions

User classpath:

□ Verbose mode (receive a message when Java loads class)

Verify classes: Default (remote only)

Garbage collection:

□ Verbose

□ Only When Needed

Memory settings:

Maximum heap size:		● KB ○ MB	(128 KB or greater)
Java stack size:		● KB ○ MB	(10 KB or greater)
Native code stack size:		● KB ○ MB	(32 KB or greater)

Properties (optional):

```
button.color = green
```

Press enter after each property=value entry

Figure 294. Configuring generic appletviewer settings

Note the following fields:

- **Applet Viewer Java Classpath options**
  - **Java Foundation Classes**: If any of your Java applets require the Java Foundation Classes (JFC) class library (for example if you use the Swing package), you should select this option to add its location to the classpath variable.
  - **Java Communications extensions**: If any of your Java applets require the javax.comm class library you should select this option to add its location to the classpath variable.
  - **User classpath**: If any of your Java applets require additional Java classes, you should specify the path where they are located in this input field. If your application requires multiple paths, you can separate them with a colon (:) as with other Java classpaths. This may require you to export and mount directories as we described in the Java application example. The information in this field will be added to the CLASSPATH variable in the JVM where your applets run.
- **Verbose mode** (receive a message when Java loads class): Checking this option causes Java to print a message to the diagnostic log each time a class file is loaded. This can be useful for debugging purposes.
- **Verify classes**: This option determines how the JVM should verify the byte code in the classes it loads. By verifying the byte code, the JVM can validate that the classes conform to the Java language specifications and do not contain viruses or other harmful code. The options are:
  - **All**: The byte-code verifier is run on all classes that are loaded, regardless of where they are located.
  - **Default (Remote only)**: The byte-code verifier is only run when classes are loaded from an untrusted location. This is the default value.
  - **None**: The byte-code verifier is never run.

Note

Verifying the byte code will impact the performance when loading the classes and somewhat increase the time it takes to load them.

- **Garbage collection**: Garbage collection is Java’s process of reclaiming unused memory and relieving the programmers from that burden. By default, the system runs the garbage collector at unspecified intervals, even though memory may be available. While running, the garbage collector uses some CPU resources from the system and may impact the performance of the running Java applets. It may be desirable to only run the garbage collector when really necessary. The options are:
  - **Verbose**: Checking this item causes the garbage collector to print messages to the diagnostics log whenever it frees memory.
  - **Only when needed**: Checking this item causes the garbage collector to run only when the system is out of heap space.
- **Memory settings**
  These settings determine how much memory is allocated to the JVM running your Java applets. Increasing the values allocates more memory to the Java

applets. It also uses memory from the Network Station which limits the number of other applications that can be run. The different memory options are:

- **Maximum heap size**: This is the maximum amount of memory the JVM allocates to dynamically allocated objects and arrays. Valid values are 128 KB and above. The default value is 6 MB.
- **Java stack size**: This is the maximum amount of memory allocated to the stack for each thread for running Java code. Valid values are 10 KB and above. The default value is 400 KB.
- **Native code stack size**: This is the maximum amount of memory allocated to the stack for each thread for running native C or C++ code. Valid values are 32 to 128 KB. The default value is 128 KB.

Note

- When specifying the amount of memory for each setting, make sure you also specify if it is MB or KB. For example, don’t specify a Java stack size of 512 MB, when you meant 512 KB.
- If you experience out-of-memory conditions with your Java applets, you can try to increase the amount of memory allocated to the JVM. If you don’t know how much memory your applets require, you may have to experiment a little with these memory settings to get the optimum values for your Java applets.

- **Properties** (optional): This input field allows you to define specific properties that your Java applets can pick up and use, for example: `button.color=green`

Make sure you press Enter after each of the properties you enter so there is only one property definition per line.

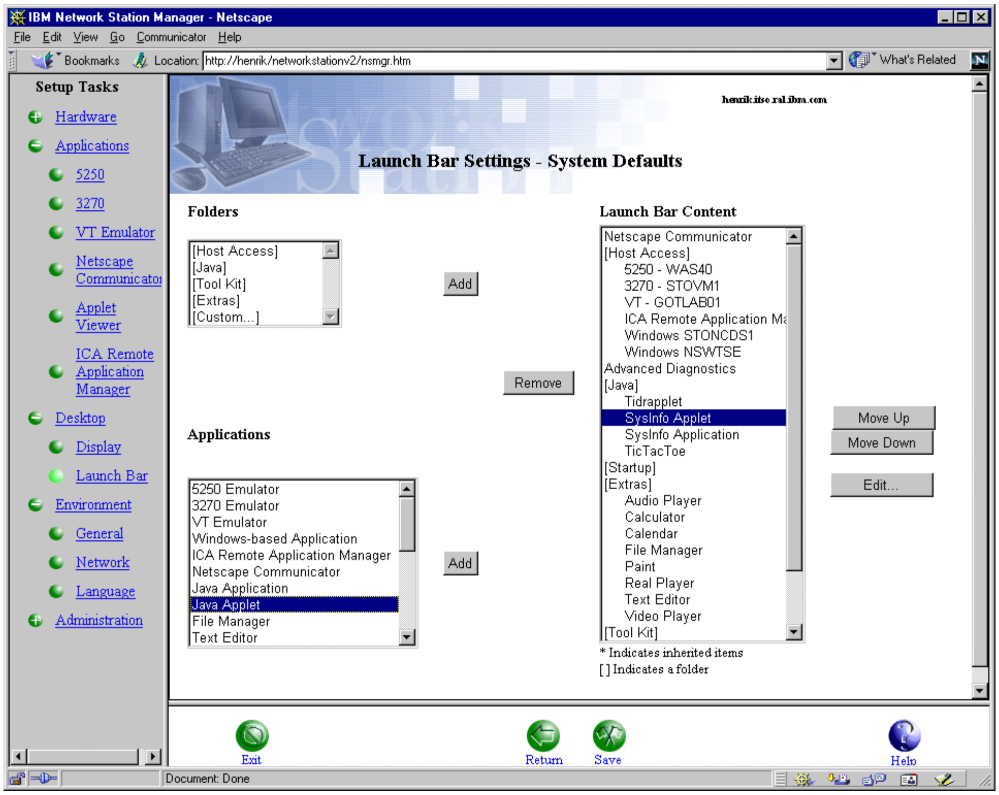
Remember

Since all Java applets running in the IBM enhanced JVM all run in the same JVM instance, all settings you make affect all applets.

11.7.2 Adding the Launch Bar icon

After configuring the generic appletviewer settings (which actually was not necessary for our simple applet), adding the Java applet to the Network Station was very easy.

To add a button for the Java applet on the Launch Bar, select **Desktop->Launch Bar** in NSM. Select **Java Applet** under applications. Then, click the **Add** button as shown in Figure 295.



Launch Bar Settings - System Defaults

Folders

[Host Access]
[Java]
[Tool Kit]
[Extras]
[Custom...]

Applications

5250 Emulator
3270 Emulator
VT Emulator
Windows-based Application
ICA Remote Application Manager
Netscape Communicator
Java Application
Java Applet
File Manager
Text Editor

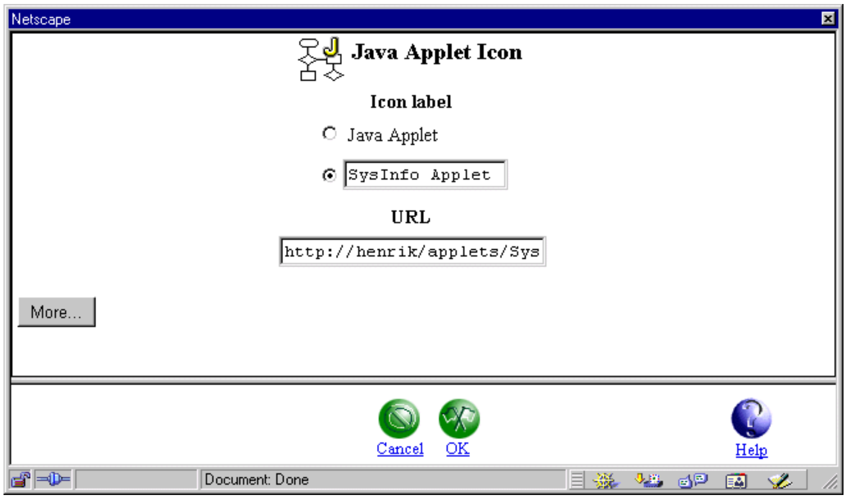
Launch Bar Content

Netscape Communicator
[Host Access]
5250 - WAS40
3270 - STOVM1
VT - GOTLAB01
ICA Remote Application Ma
Windows STONCDS1
Windows NSWTSE
Advanced Diagnostics
[Java]
Tidrapplet
SysInfo Applet
SysInfo Application
TicTacToe
[Startup]
[Extras]
Audio Player
Calculator
Calendar
File Manager
Paint
Real Player
Text Editor
Video Player
[Tool Kit]

* Indicates inherited items
[ ] Indicates a folder

Figure 295. Adding a Java applet to the NC Desktop Launch Bar

The display shown in Figure 296 appears.



Java Applet Icon

Icon label

○ Java Applet

● SysInfo Applet

URL

http://henrik/applets/Sys

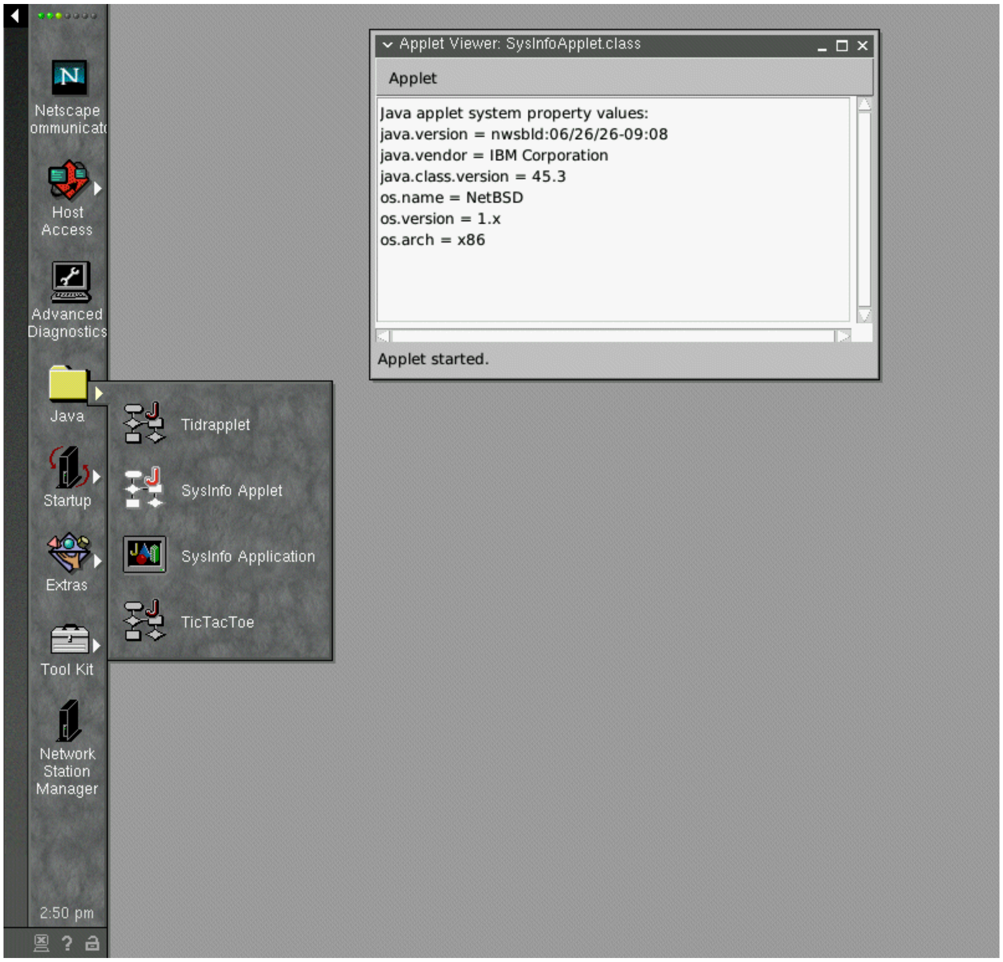
Figure 296. Customizing the sample Java applet icon

The fields shown in Figure 296 are explained here:

- **Icon label**: Select the second radio button, and enter the name for the button. Since we used our SysInfoApplet applet, it made sense to call the button `SysInfo Applet`.
- **URL**: This is the full URL for the HTML page that describes the applet. We used `http://henrik/applets/SysInfoApplet.html`.

11.7.3 Testing the Java applet

When all setting were configured, we tested the applet on the Network Station. This is shown in Figure 302.



```
Java applet system property values:
java.version = nwsbld:06/26/26-09:08
java.vendor = IBM Corporation
java.class.version = 45.3
os.name = NetBSD
os.version = 1.x
os.arch = x86
```

Applet started.

Figure 297. SysInfo applet

11.7.4 Loading applets using the HTTP protocol versus the file system

Java applications are always loaded via the file system (NFS or RFS). However, Java applets can be loaded either via the file system or via the HTTP protocol. The HTTP protocol is clearly the most common way of loading Java applets, since this is what is used when they are embedded in Web pages on the Internet.

In the previous example, when we ran the Java applet in the appletviewer, we used the HTTP protocol. That selection was made by specifying `http://` in the beginning of the applet URL (`http://henrik/applets/SysInfoApplet.html`).

If we wanted to load the applet using the file system instead, we would have to place the HTML file and the .class file in a directory that is exported via NFS or RFS and mounted by the Network Station (see the Java application example in 11.9, “JFC Swing 1.0.3 problem and its solution” on page 328). If we put the SysInfoApplet.html file and SysInfoApplet.class file in a directory that the Network Station could access as /tmp/javatest, we could have used the URL `/tmp/javatest/SysInfoApplet.html` the display in Figure 296 on page 325, instead of the `http://henrik/applets/SysInfoApplet.html`. The applet would then be loaded via the file system.

Now you probably wonder what the difference is between these two methods. Well, the visual appearance is the same. But, applets loaded via the file system are considered to come from a more secure place and, therefore, given extended permissions allowing them to do more than applets loaded via the HTTP protocol (which are considered coming from an insecure Internet site, an untrusted location) can do.

We do not go into the details of Java security here. For more information, refer to the Sun Microsystems' Java security FAQ at:
`http://java.sun.com/sfaq/index.html`

11.8 Using the Advanced Diagnostics shell to run Java

The Advanced Diagnostics shell can be useful for testing Java applications and applets and to try different parameters. This is much faster than making the changes to NSM and logging off and on to activate the changes.

We brought up the Advanced Diagnostics shell and tried running both our sample Java application and our sample Java applet from it.

The following commands started our SysInfo application:

```
$ cd /tmp/javatest
$ java SysInfo
```

If we had not changed the directory (cd command above) to where the application was located, we would have had to add its location to the classpath. This can be done in the Java command and would only be effective for that one command:

```
$ java -classpath /usr/local/java/J118/lib/classes.zip:/tmp/javatest:. SysInfo
```

Note: The default classpath is /usr/local/java/J118/lib/classes.zip. You can see this by using the echo $CLASSPATH command. Each directory is separated by a colon (:). The dot at the end specifies to search the current directory.

You could also export the CLASSPATH variable to change the classpath settings for your session:

```
$ export CLASSPATH=/usr/local/java/J118/lib/classes.zip:/tmp/javatest:.
```

To run the Java applet, we used:

```
$ appletviewer http://henrik/applets/SysInfoApplet.html
```

This loaded the applet using the HTTP protocol. To load it using the file system instead, we used the following command:

```
$ appletviewer /tmp/javatest/SysInfoApplet.html
```

When using the Advanced Diagnostics shell, the output written to the stdout is displayed directly in the shell window.

11.9 JFC Swing 1.0.3 problem and its solution

During tests with Java application on the Network Computer we encountered the following problem. First, we wrote a simple graphic application using VisualAge for Java Enterprise Edition version 2.1 (VAJava 2.0 EE + Enterprise Update 3/99). Originally, it should have been a simple calculator with a few additional “unnecessary” functions. We tested it on our Windows NT 4.0 workstation. All we had to do was to download and configure the JDK and JFC/Swing. We downloaded JDK 1.1.8 and JFC 1.1/Swing 1.0.3 from Sun’s Web page at:
`http://www.sun.com/`

To run our application, we typed the following command in the Windows NT prompt:

```
java -classpath
.;c:\jdk1.1.8\lib\classes.zip;c:\Swing-1.0.3\swingall.jar;d:\javatest
SimpleCalculator
```

Figure 298 shows the result as we expected.

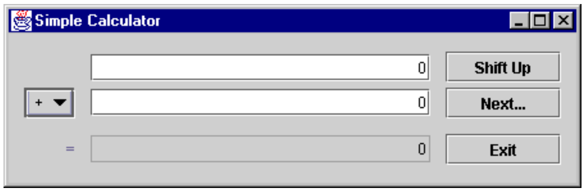


Figure 298. Java test application

We do not list the source code since it takes about 1200 lines. Figure 299 shows the test application during the coding stage.

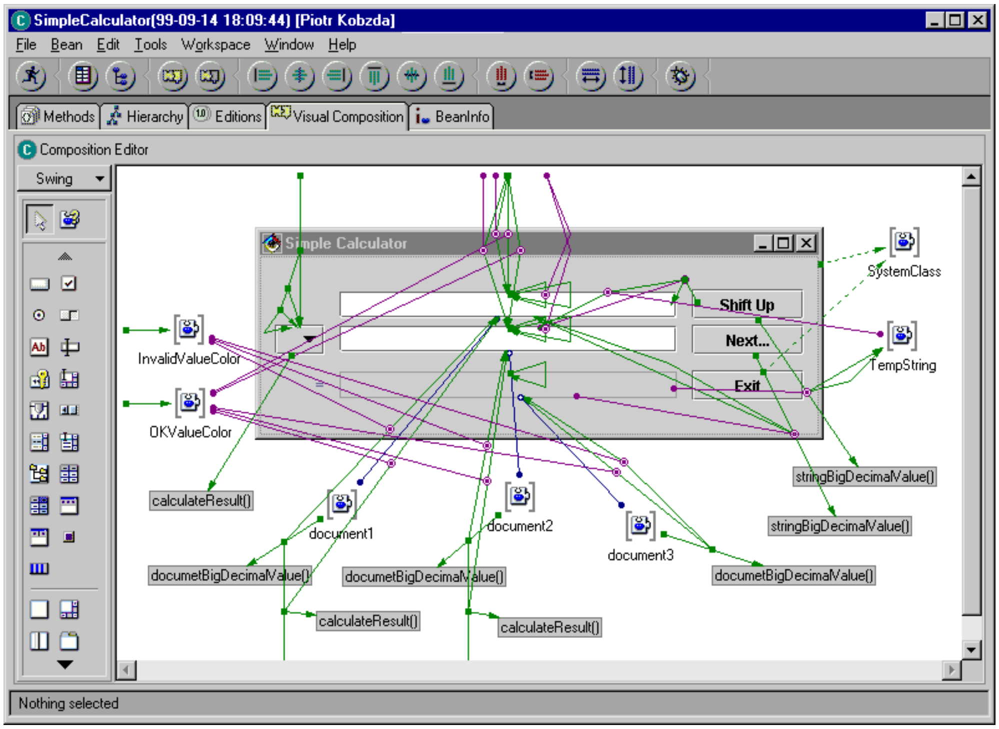
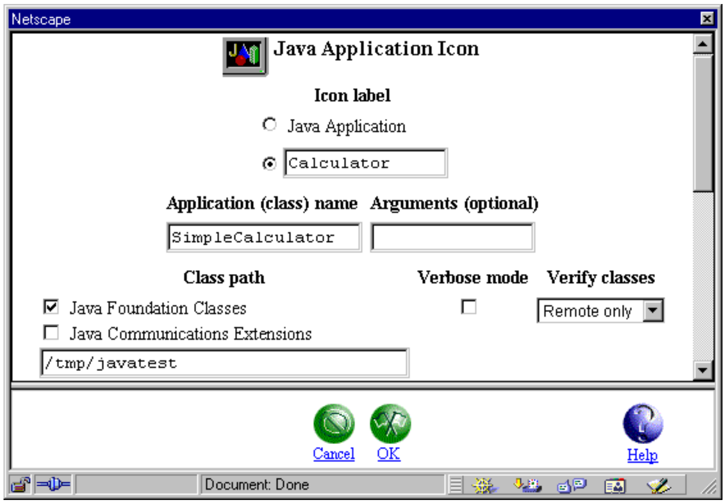


Figure 299. Building an application using IBM Visual Age for Java 2.1 EE

Next, we configured the NSM V2R1 to run this Java application from the Network Computer. We did this in the same way shown in 11.6, "Configuring NSM to run a Java application example" on page 314. The difference is shown in Figure 300. We selected the Java Foundation Classes since our application uses Swing classes for displaying its GUI components. After saving the configuration and rebooting the Network Computer, we tried to start our test application. We clicked on the icon and nothing happened. There was absolutely no result.



Java Application Icon

Icon label

○ Java Application

● Calculator

Application (class) name: SimpleCalculator

Arguments (optional):

Class path

☑ Java Foundation Classes

□ Java Communications Extensions

/tmp/javatest

Verbose mode □

Verify classes: Remote only

Figure 300. Setup window for the Java graphical application

Then, we started our investigation into the problem. We opened the Advanced Diagnostic window. Using the registry related tool `ncpkgget` (see 18.9, “Investigating the NC Registry” on page 600), we established that the following command was:

```
nsm_wrapper java -classpath
/usr/local/java/${JAVA_LEVEL}/lib/classes.zip:/usr/local/java/${JAVA_LEVEL}/li
b/swingall.jar:/tmp/javatest -verifyremote SimpleCalculator
```

This is equivalent to information found in the XML user profile:

```
<FIELD NAME="command">nsm_wrapper java -classpath
/usr/local/java/${JAVA_LEVEL}/lib/classes.zip:/usr/local/java/${JAVA_LEVEL}/li
b/swingall.jar:/tmp/javatest/ -verifyremote \
SimpleCalculator</FIELD>
```

Notice that the entire command is stored in two lines in the user XML preference profile (lines in UNIX are separated by LF character, which in turn has special meaning for the shell). To avoid skipping of the rest of the parameters, this LF character must be quoted with a backslash (\) character. In other words, if a newline character follows the backslash, the shell interprets this as a line continuation.

After running the command, we obtained the following error message:

```
Can’t find class SimpleCalculator.
```

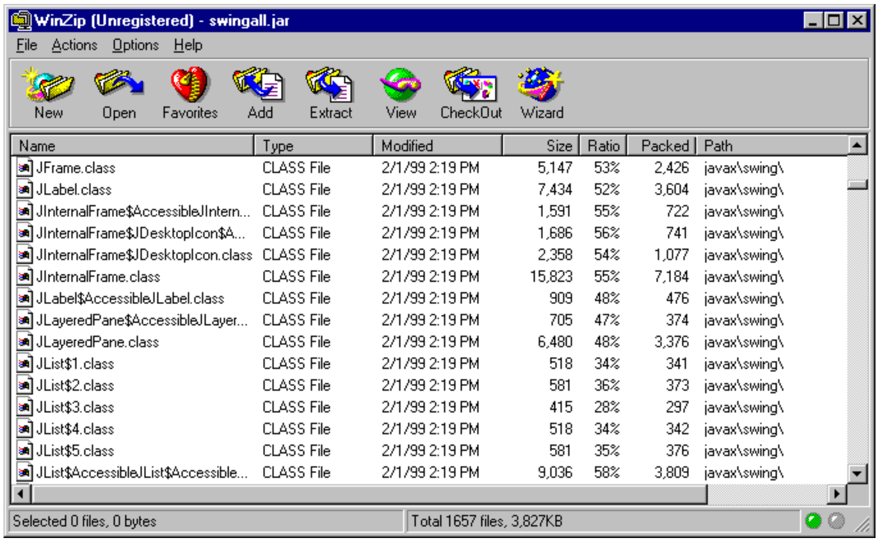
Having the source of that class, we issued the following command (compilation to bytecode):

```
nsm_wrapper javac -verbose -classpath
usr/local/java/${JAVA_LEVEL}/lib/classes.zip:/usr/local/java/${JAVA_LEVEL}/lib
/swingall.jar /tmp/javatest/SimpleCalculator.java
```

The following error messages appeared. The first message was the most meaningful:

```
/tmp/javatest/SimpleCalculator.java:5: Superclass com.sun.java.swing.JFrame of
class SimpleCalculator not found.
```

We realized that something was wrong with swingall.jar package. We opened this package using the WinZip application. The contents are shown in Figure 301.



Name	Type	Modified	Size	Ratio	Packed	Path
JFrame.class	CLASS File	2/1/99 2:19 PM	5,147	53%	2,426	javax\swing\
JLabel.class	CLASS File	2/1/99 2:19 PM	7,434	52%	3,604	javax\swing\
JInternalFrame$AccessibleJIntern...	CLASS File	2/1/99 2:19 PM	1,591	55%	722	javax\swing\
JInternalFrame$JDesktopIcon$A...	CLASS File	2/1/99 2:19 PM	1,686	56%	741	javax\swing\
JInternalFrame$JDesktopIcon.class	CLASS File	2/1/99 2:19 PM	2,358	54%	1,077	javax\swing\
JInternalFrame.class	CLASS File	2/1/99 2:19 PM	15,823	55%	7,184	javax\swing\
JLabel$AccessibleJLabel.class	CLASS File	2/1/99 2:19 PM	909	48%	476	javax\swing\
JLayeredPane$AccessibleJLayer...	CLASS File	2/1/99 2:19 PM	705	47%	374	javax\swing\
JLayeredPane.class	CLASS File	2/1/99 2:19 PM	6,480	48%	3,376	javax\swing\
JList$1.class	CLASS File	2/1/99 2:19 PM	518	34%	341	javax\swing\
JList$2.class	CLASS File	2/1/99 2:19 PM	581	36%	373	javax\swing\
JList$3.class	CLASS File	2/1/99 2:19 PM	415	28%	297	javax\swing\
JList$4.class	CLASS File	2/1/99 2:19 PM	518	34%	342	javax\swing\
JList$5.class	CLASS File	2/1/99 2:19 PM	581	35%	376	javax\swing\
JList$AccessibleJList$Accessible...	CLASS File	2/1/99 2:19 PM	9,036	58%	3,809	javax\swing\

Selected 0 files, 0 bytes

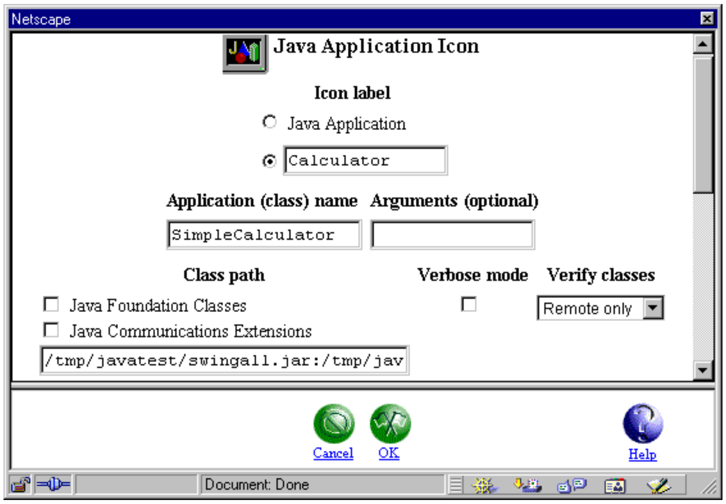
Total 1657 files, 3,827KB

Figure 301. Contents of NC swingall.jar package

For each class, the directory begins with javax\. This means that the swingall.jar package is at the JFC 1.1/Swing 1.1 level.

The conclusion from this example is that the Swing classes included in the NSM V2R1 cannot be used for Java applications written for JFC 1.1/Swing 1.0.3. The class names are the same. But, the fully qualified path names have changed, making these packages “incompatible”. If you want to use these classes, be sure that you produce the JFC 1.1/Swing 1.1 compatible code.

To start our Java application, we included the directory to Swing 1.0.3 package in the classpath. Then, we deselected the Java Foundation Classes box (Figure 302).



Java Application Icon

Icon label

○ Java Application

● Calculator

Application (class) name: SimpleCalculator

Arguments (optional):

Class path

☐ Java Foundation Classes

☐ Java Communications Extensions

/tmp/javatest/swingall.jar:/tmp/jav

Verbose mode ☐

Verify classes: Remote only

Document: Done

Figure 302. Setup window after changes

Chapter 12. Netscape Communicator 4.5

This chapter describes the new browser that is included in NSM V2R1. This browser is the UNIX version of the well-known Netscape Communicator 4.5 and is a significant step forward compared to the browser shipped in earlier releases of NSM.

This chapter deals mainly with non-Java issues. If you're interested in the Network Station Java environment, see Chapter 11, “Java environment” on page 305. This chapter discusses some browser-related Java issues.

Also, this chapter does not cover any e-mail or news groups-related issues. For information on that topic, go to Chapter 15, “Accessing Lotus Domino from the Network Station” on page 481.

Before we introduce the NSM V2R1 Netscape Communicator 4.5 browser, we just briefly describe the features of the earlier NC Navigator 3.0 browser.

AS/400 printing from Netscape

AS/400 customers printing from Netscape (parallel printing) require the following system PTF (appropriate for the system operating system level):

- V4R3 systems: 5769SS1-SF60984
- V4R4 systems: 5769SS1-SF60985

12.1 NC Navigator 3.0

The earlier NSM releases included a browser called NC Navigator 3.0 (also known as Navio), which was based on a sub-set of the UNIX version of the Netscape Navigator 3.0 code. NC Navigator included most of the features found in Netscape Navigator 3.0 on other platforms, such as:

- The ability to view HTML pages with frames, GIF or JPG images, animated GIFs, and so on
- Mail client with POP3 protocol support
- News client with NNTP protocol support
- JavaScript 1.1 support
- Java applet support
- SSL2 and SSL3 support, 40- or 128-bit encryption

Even though NC Navigator 3.0 was a capable browser, it lacked some important features to which users of Netscape Navigator or Microsoft Internet Explorer on other platforms were accustomed. Some of the most important features were:

- **No plug-in capability**: This rendered the NC Navigator incapable of running plug-ins, for example to view Adobe Acrobat documents (.pdf files).
- **No internal Java Virtual Machine**: When the NC Navigator 3.0 was to launch a Java applet it used the Network Station's JVM, which was external to the browser. Usually, this worked well. In some cases, it did not provide the level of compatibility required by some Java applets. Therefore, some applets that

ran fine in Netscape Navigator or Internet Explorer on, for example, the Win32 platform, did not run in NC Navigator.

12.2 Netscape Communicator 4.5

The NSM V2R1 Netscape Communicator 4.5 is a significant step forward compared to the NC Navigator 3.0. It adds a number of important features. For a comprehensive listing of the new functions in Netscape Communicator 4.5, visit the site at: `http://home.netscape.com/eng/mozilla/4.5/relnotes/windows-4.5.html`

Some of the features include:

- **IMAP4 mail support**: In addition to the POP3 protocol, the browser's mail client (Netscape Messenger) now also supports the IMAP4 protocol, which provides increased flexibility.
- **LDAP support**: The Netscape Communicator 4.5 browser includes Lightweight Directory Access Protocol (LDAP) client. LDAP is a protocol that bridges the gap between different and usually incompatible directory services. Information in such directories are usually names, phone numbers and e-mail addresses. Using the LDAP protocol, users can access and search these disparate directories over the Internet.
- **Smart Browsing**: Smart Browsing allows the browser to recommend related Web sites and information, and filters out Web pages containing inappropriate material. In addition to traditional URLs, Smart Browsing also lets the user pick common words to find the information. For example, the user can type the word `volvo` instead of `http://www.volvo.com`. This sub-function is called "Internet Keywords".
- **Enhanced support for bookmarks**: The user now has the ability to organize bookmarks into folders for easier access and a better overview.
- **Dynamic HTML (DHTML)**: The browser supports Dynamic HTML as defined by Netscape Navigator 4.5, including HTML positioning and layering, dynamic style sheet, and dynamic fonts.
- **PNG images support**: The browser also supports the PNG image format.
- **Audio support**: The browser supports audio clips, for example, when incorporated as background music on Web pages. Supported audio formats are AU, WAV, and AIFF. The audio files are played by an external helper application.
- **Video support**: In addition to audio support, the browser also supports QuickTime and AVI video formats. The video files are played by an external helper application.
- **RealAudio and RealVideo support**: NSM V2R1 also includes support for the common RealAudio and RealVideo multimedia file formats through an external RealPlayer (version 5) helper application. This player is automatically invoked when the browser detects the corresponding MIME types (.ra, .rm, and .ram).
- **PDF viewer**: To view the common Adobe Acrobat PDF file format, the browser now also includes a PDF viewer. This external viewer is automatically launched when the browser detects the corresponding MIME type (.pdf). It supports the Adobe Acrobat version 3.0 file format (PDF 1.2).

- **Support for user-configurable MIME types**: The browser now also supports user-configurable MIME types and accompanying helper applications. This feature could be used, for example, to launch a Java-based viewer for Microsoft Word documents when the browser detects a URL ending with the .doc extension.
- **Internal Netscape Java Virtual Machine (JVM)**: The browser includes the full Netscape internal JVM to provide full compatibility with Netscape on other platforms. The JVM included in Netscape Communicator 4.5 is based on JDK 1.1.
- **JavaScript 1.3 support**: The browser supports JavaScript 1.3. JavaScript is Netscape's scripting language for Web pages. It should not be confused with the Java language, which is completely different.
- **Netscape LiveConnect**: To enable communication back and forth between JavaScripts and Java applets, Netscape's LiveConnect is included. The LiveConnect feature only supports communication between JavaScript and Java applets that run in the browser's *internal* JVM.
- **Signed applets and signed JAR file**: The browser supports both signed applets and signed JAR files according to Netscape's security model.
- **HTML formatting of e-mail**: To provide rich contents in e-mail messages, Netscape Communicator 4.5 supports formatting e-mail messages using HTML.
- **Plug-in support**: Also added to this release is support for browser plug-ins. It should be noted that *only* plug-ins written in Java or for the Network Station's operating system can be used. This *excludes* plug-ins written for the Win32 platform.
- **Java Plug-In**: The NSM V2R1 Netscape Communicator 4.5 now supports Sun Microsystems' Java Plug-In technique via a plug-in module. The Java Plug-In capabilities are covered in more detail in 11.3.1, "Java Plug-In: Choosing JVM for the Netscape browser" on page 309, and 12.5, "Using the Java Plug-In feature" on page 356.
- **Ability to launch local Network Station applications**: The browser now has the ability to launch local Network Station applications, such as the ICA client, 5250 emulator, and so on, using special URL types. Using this feature, a Web-based desktop, "Web-top", interface can be built.

12.2.1 Functions not in NSM V2R1 Netscape Communicator 4.5

Even though the NSM V2R1 Netscape Communicator 4.5 browser is a very complete browser package, it lacks some features found in Netscape Communicator 4.5 on other platforms, for example, the Win32 platform. For most of these functions, it does not make sense to include a network computer's browser. The notable *missing* functions include:

- **Composer for editing web pages**: The Composer included in Netscape Communicator on other platforms is used to *create* Web pages. The Composer is included in NSM V2R1 Netscape Communicator, but it can not be used for creating or editing Web pages. However, it can still be used to create HTML-formatted e-mails to provide rich content.
- **Offline mode**: Netscape Communicator on other platforms has the ability to download Web pages and e-mail for local offline browsing. Since the Network

Station is always connected to the network and has no local storage, this function is not included.

- **Roaming user support**: Even though this feature is included in the code, it is disabled since it doesn't fit well into the Network Station environment, which provides roaming user support through NSM. NSM roaming user support includes all of the Network Station applications, not only the browser.
- **SmartUpdate**: SmartUpdate is Netscape's technique for enabling the enduser to easily download new versions of and enhancements to the Netscape Communicator browser. Since the Network Station does not have any local storage but rather downloads the correct version of the browser each time it is invoked, this function is not included.
- **What's related (Smart Browsing function)**: This function tells the browser to contact Netscape's site to retrieve sites related to the one the user is viewing. This creates a lot of traffic to Netscape's site and also sends URLs that the user is viewing to the Netscape site. The NSM V2R1 Netscape Communicator 4.5 browser code still supports this feature, but it has been disabled to reduce unnecessary network traffic.
- **TrueDoc font support**: TrueDoc is a platform independent font technology developed by Bitstream and incorporated into, for example, Netscape Communicator on the Windows platform. It is not included in the NSM V2R1 Netscape Communicator 4.5.
- **Java Just-In-Time Compiler (JITC)**: The NSM V2R1 Netscape Communicator 4.5 internal JVM does not include Netscape's Just-In-Time Compiler. That JITC is only available in the Windows version of Netscape Communicator.
- **Ability to execute Win32 plug-ins**: Only plug-ins written in Java or for the Network Station's operating system can be executed.
- **PalmPilot address book synchronization**: The ability to synchronize Netscape Communicator's address book with 3Com PalmPilot or IBM WorkPad devices is not included.
- **User profiles**: Netscape Communicator's ability to let users have different profiles, for example profiles for office (LAN) and home (modem) usage, is not included.
- **AOL Instant Messenger**: Support for AOL Instant Messenger, a chat system similar to the well-known ICQ system, is not included.

Apart from these functions, the NSM V2R1 Netscape Communicator 4.5 browser is compatible with Netscape Communicator 4.5 on other platforms. Any applications running under Netscape Communicator 4.5 on other platforms should also run on the Network Station.

12.2.2 Functions added to NSM V2R1 Netscape Communicator 4.5

The NSM V2R1 Netscape Communicator 4.5 also has a few added functions. The most notable are:

- Year 2000 compliancy for the internal JVM
- Euro currency support for the internal JVM
- Support for some Network Station-specific URL types used to launch local Network Station applications.

Note

The first time a user starts the browser, they must create the necessary files in the user's home directory. This may take a while, especially if the user's home directory is on a server that is behind a slow WAN connection. Be patient. After the files are created, the browser starts much faster.

12.3 Configuring the NSM V2R1 Netscape Communicator 4.5

This section describes how to configure the NSM V2R1 Netscape Communicator 4.5 browser. We describe both how to do basic configuration and also deal with more advanced topics.

12.3.1 Configuration overview

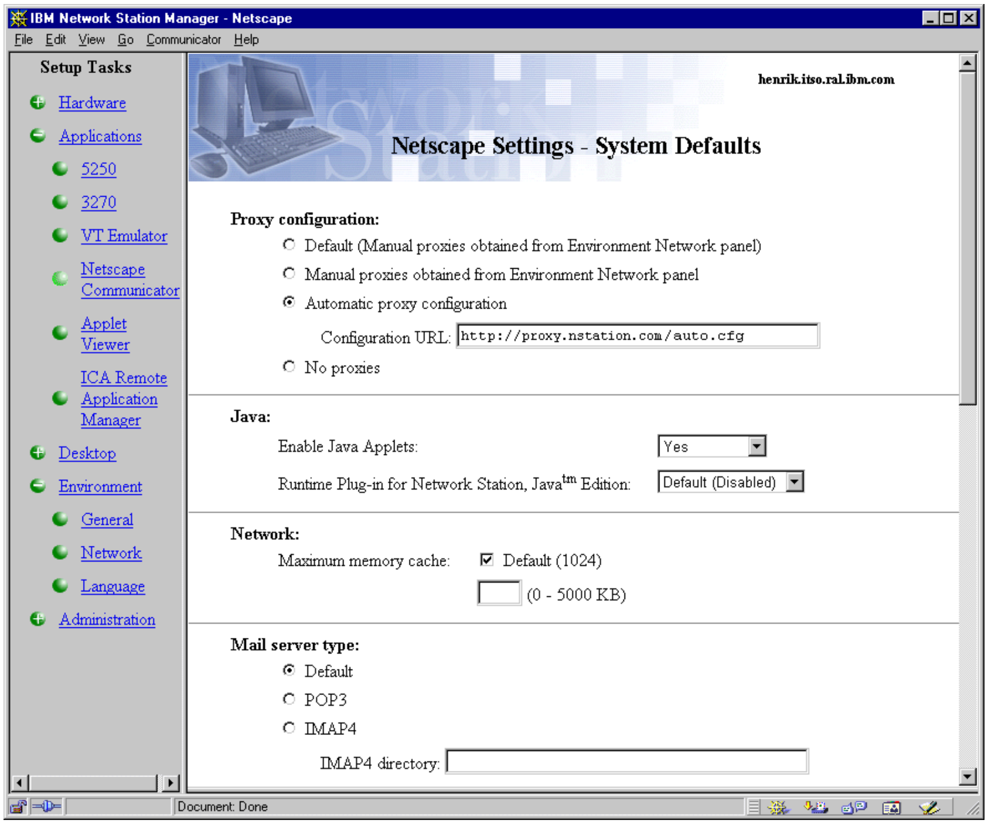
NSM V2R1 Netscape Communicator 4.5 retrieves its settings from four different origins:

- **IBM-shipped factory defaults**: These are the settings that IBM ships with the product. Examples are Java applets enabled or disabled and browser memory cache size. These settings are merely default values and are overridden by whatever changes an administrator or user makes using NSM or in the browser itself.
- **NSM-managed settings**: These settings are configured using the NSM Web (or command line) interface. The administrator can change settings for all users, while the end-user is only allowed to change a limited number of settings, affecting only them. Examples of settings made in NSM are proxy settings, home page, and so on.
- **End-user settings made in the browser**: These are settings that the end-user makes himself, using the browser's own dialogs. These dialogs are the same as Netscape Communicator on Windows or UNIX. Example of settings are e-mail address and so on.
- **Hand-edited configuration files (Advanced Customization)**: The preferred method of creating preferences for users is using NSM or NSMCL. However, but there may be situations where the setting needed is not available with these tools. In that case, there are JavaScript configuration files that can override all other values. They are usually used for advanced configuration or to lock certain settings. They cannot be changed by an end-user. Using this technique, it is possible to, for example, lock the proxy settings so an end-user cannot modify them.

All settings you make in point 2 or 3 above are stored in one or more of the NSM download profiles.

12.3.2 Configuring generic settings through NSM

To configure the Netscape Communicator settings in NSM, go to **Applications->Netscape Communicator**. The window shown in Figure 303 on page 338 is displayed.



Netscape Settings - System Defaults

Proxy configuration:

○ Default (Manual proxies obtained from Environment Network panel)

○ Manual proxies obtained from Environment Network panel

● Automatic proxy configuration

Configuration URL: `http://proxy.nstation.com/auto.cfg`

○ No proxies

Java:

Enable Java Applets: Yes

Runtime Plug-in for Network Station, Java^{tm} Edition: Default (Disabled)

Network:

Maximum memory cache: ☑ Default (1024)

(0 - 5000 KB)

Mail server type:

● Default

○ POP3

○ IMAP4

IMAP4 directory:

Figure 303. Configuring Netscape Communicator 4.5 generic settings

The sections shown in Figure 303 are explained here:

- **Proxy configuration**: Under this section, you can choose between three different proxy settings:
  - **Default/Manual**: The first two options, *Default (Manual proxies obtained from Environment Network panel)* and *Manual proxies obtained from Environment Network panel*, are identical. They tell the browser to use the proxy settings configured in the Environment->Network panel in NSM (see 12.3.2.1, “Configuring mail and proxy settings” on page 342).
  - **Automatic**: The third option, *Automatic proxy configuration*, allows you to configure the URL to an autoproxy. This enables the browser to automatically select different proxy servers for different protocols, as configured by the autoproxy URL.

    Note

    For a complete description of how to create an autoproxy configuration file, see the Netscape URL:

    `http://home.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html`

  - **No proxies**: If your system is not behind a firewall, or if your system is behind a firewall but you do not want your users to view Web pages outside the firewall, you would select the *No proxies* option.

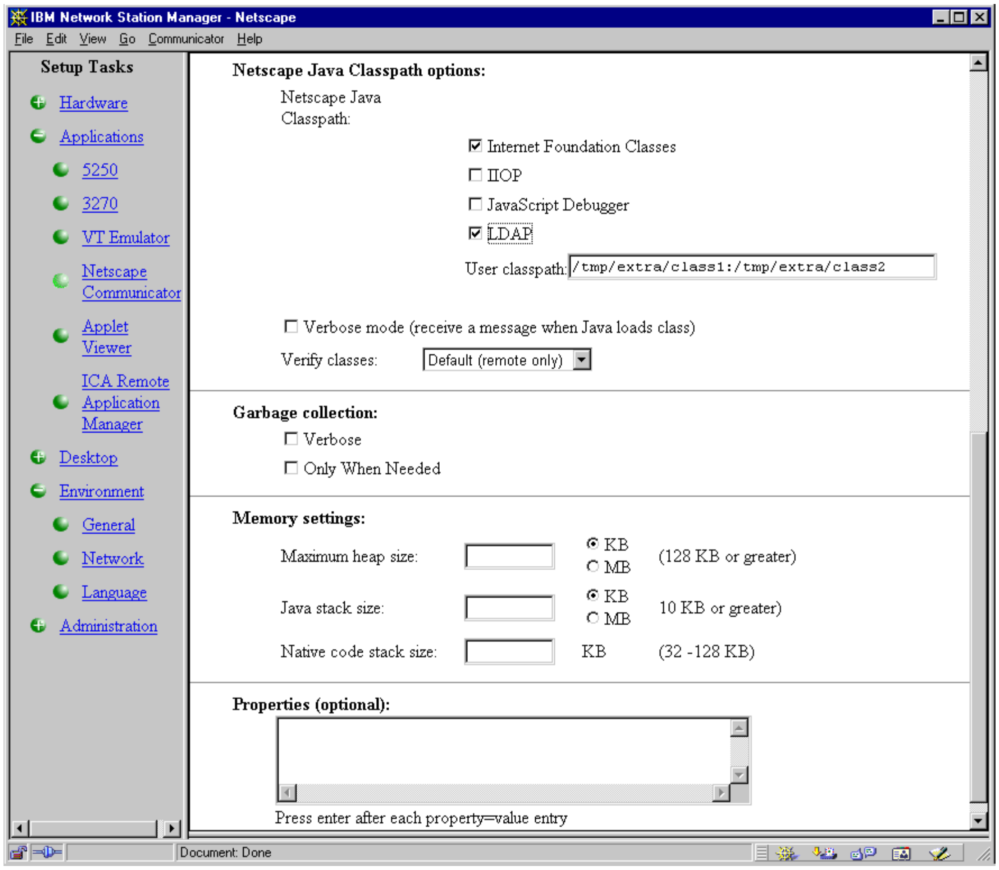
- **Java**: In this section, you need to set:
  - **Enable Java Applets**: This setting enables or disables the browser's Java applet support. If this option is set to disabled, the browser ignores all Java applets it encounters on Web pages. Enabling this option allows the browser to run Java applets. This requires more memory in the Network Station since it has to launch the JVM as well.

    Note

    By default, the Enable Java Applets setting is *disabled*, meaning the browser will *not* run Java applets. You must *enable* this setting to run Java applets from the browser.

  - **Runtime Plug-in for Network Station, Java Edition**: This setting enables or disables the Java Plug-In. If this setting is disabled, the Netscape Communicator's internal JVM will be used to run Java applets. If the setting is enabled, the IBM enhanced external JVM will be used to run Java applets. Then, *all* applets launched from the browser run in the IBM enhanced external JVM.
- **Network**: Here you can specify the amount of RAM that the browser will use for caching bitmaps and Web pages. A higher value can improve the performance and responsiveness of the browser, but also requires more memory in the Network Station. Unless you experience problems or poor performance, you can usually leave this value at its default of 1024 KB.
- **Mail server type**: Here you can specify the type of mail server you have. If you select Default, the browser uses the mail server type defined in the Environment->Network panel in NSM. For more information on how to configure the browser for e-mail usage, see Chapter 15, "Accessing Lotus Domino from the Network Station" on page 481.

Figure 304 on page 340 shows the setting for the Java environment.



Netscape Java Classpath options:

Netscape Java Classpath:

☑ Internet Foundation Classes
☐ IIOP
☐ JavaScript Debugger
☑ LDAP

User classpath: /tmp/extra/class1:/tmp/extra/class2

☐ Verbose mode (receive a message when Java loads class)

Verify classes: Default (remote only)

Garbage collection:

☐ Verbose
☐ Only When Needed

Memory settings:

Maximum heap size:		● KB ○ MB	(128 KB or greater)
Java stack size:		● KB ○ MB	10 KB or greater)
Native code stack size:		KB	(32 -128 KB)

Properties (optional):

Press enter after each property=value entry

Figure 304. Configuring Netscape Communicator 4.5 Java environment

- **Netscape Java Classpath options**: Using these settings you can change the classpath that the browser uses for locating Java classes. If you use Java applets that require any of these Java class libraries, you can select the corresponding kit to have its location automatically added to the browser's classpath. This enables the browser's internal JVM to find the class libraries. If you have other class libraries you can add the path to them in the input field. The path will be appended to the browser's classpath, enabling it to find your specific classes.
  - **Verbose mode (receive a message when Java loads class)**: Selecting this option causes Java to print a message to the diagnostic log each time a class file is loaded. This can be useful for debugging purposes. If the Java applets are run in the browser's internal JVM, the messages can be viewed by opening the browser's Java Console. This is done by selecting Communicator->Tools and clicking Java Console.
  - **Verify classes**: This option determines if and how the JVM should verify the byte code in the classes it loads. By verifying the byte code the JVM can validate that the classes conform to the Java language specifications and do not contain viruses or other harmful code. The options are:
    - **All**: The byte-code verifier is run on all classes that are loaded, regardless of where they are located.
    - **Remote only**: The byte-code verifier is only run when classes are loaded from an untrusted location. This is the default value.

- **None**: The byte-code verifier is never run.

Note

Verifying the byte code impacts the performance when loading the classes and somewhat increases the time it takes to load them.

- **Garbage collection**: Garbage collection is Java's process of reclaiming unused memory and relieving the programmers from that burden. By default, the system runs the garbage collector at unspecified intervals, even though memory may be available. While running, the garbage collector uses some CPU resources from the system and may impact the performance of the running Java applets. It may be desirable to only run the garbage collector when really necessary. The options are:
  - **Verbose**: Selecting this item causes the garbage collector to print messages to the diagnostics log whenever it frees memory.
  - **Only when needed**: Selecting this item causes the garbage collector to run only when the system is out of heap space.
- **Memory settings**: These settings determine the amount of memory allocated to the JVM. Increasing the values allocates more memory to the Java applets, but also uses memory from the Network Station, limiting the number of other applications that can be run. The different memory options are:
  - **Maximum heap size**: This is the maximum amount of memory the JVM allocates to dynamically allocated objects and arrays. Valid values are 128 KB and above. The default value is 6 MB.
  - **Java stack size**: This is the maximum amount of memory allocated to the stack for each thread for running Java code. Valid values are 10 KB and above. The default value is 400 KB.
  - **Native code stack size**: This is the maximum amount of memory allocated to the stack for each thread for running native C or C++ code. Valid values are 32 to 128 KB. The default value is 128 KB.

Note

- When specifying the amount of memory for each setting, make sure you also specify if it is MB or KB. For example, don't specify a Java stack size of 512 MB, when you meant 512 KB.
- If you experience out-of-memory conditions with your Java applets, you can try to increase the amount of memory allocated to the JVM. If you don't know how much memory your applets require, you may have to experiment a little with these memory settings to get the optimum values for your Java applets.

- **Properties (optional)**: This input field allows you to define specific properties that your Java applets can pick up and use, for example: `button.color=green`.

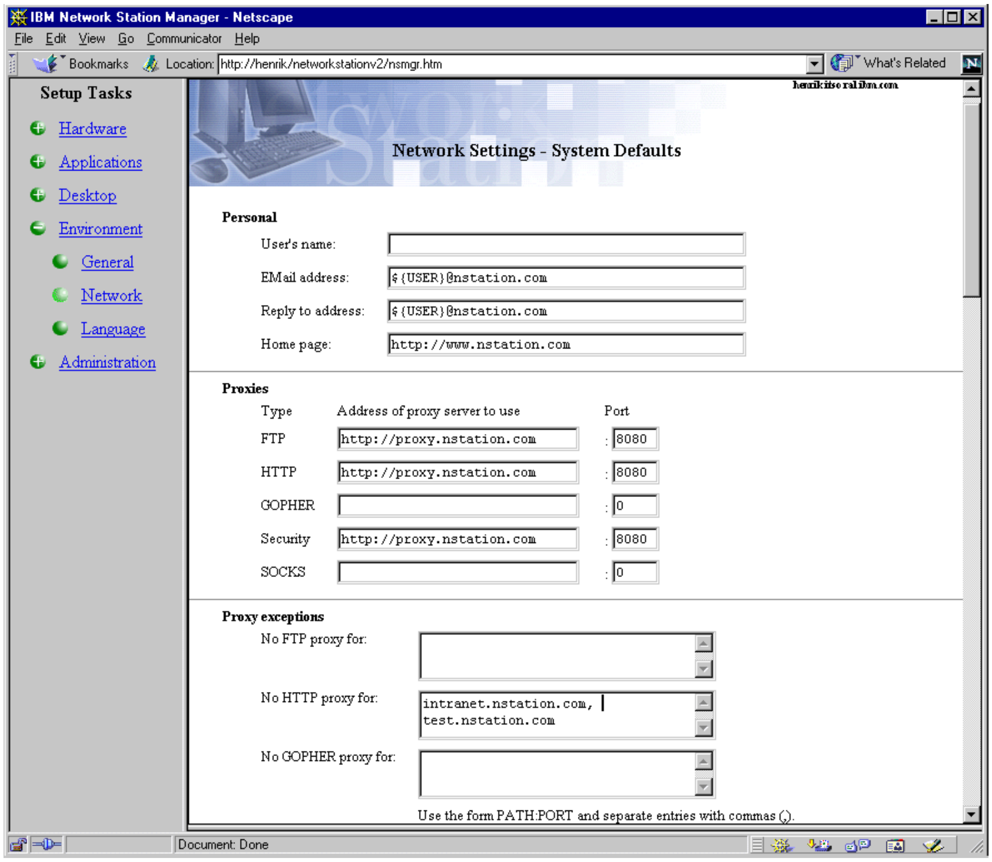
Make sure you press Enter after each of the properties you specify so there is only one property definition per line.

Note on Java configuration

All Java-related settings you make in NSM (classpath, memory settings etc.) only affect Java applets running in the browser's internal JVM. If you want to make the corresponding settings for Java applets that run in the IBM enhanced external JVM, select **Applications->Applet viewer** in NSM and make the changes there. Refer to the Chapter 11, "Java environment" on page 305, for information on this.

12.3.2.1 Configuring mail and proxy settings

You can configure mail and proxy settings on the Network panel by selecting **Environment->Network** in NSM as shown in Figure 305.



Network Settings - System Defaults

Personal

User's name:

EMail address: ${USER}@nstation.com

Reply to address: ${USER}@nstation.com

Home page: http://www.nstation.com

Proxies

Type	Address of proxy server to use	Port
FTP	http://proxy.nstation.com	8080
HTTP	http://proxy.nstation.com	8080
GOPHER		0
Security	http://proxy.nstation.com	8080
SOCKS		0

Proxy exceptions

No FTP proxy for:

No HTTP proxy for: intranet.nstation.com, test.nstation.com

No GOPHER proxy for:

Use the form PATH:PORT and separate entries with commas (,).

Figure 305. Configuring Environment->Network proxy settings

The sections in the display in Figure 305 are explained here:

- **Personal**: Here you can configure a user's user name, e-mail address, reply e-mail address, and browser home page.

Tips

If your Network Station login user ID is the same as the user name part of your e-mail address, you can use the ${USER} shortcut when defining the e-mail address, as shown above. The ${USER} then expands to the full user name, used when logging on.

For example, if your Network Station logon user ID was `hsjostrand` and your e-mail address was `hsjostrand@nstation.com`, you could use the ${USER} shortcut.

- **Proxy**: Define the proxy URLs and corresponding port numbers to use for the various protocols. If you are unsure of these values, your network administrator should be able to provide you with them.

Tip

We have, by experience, found that it's usually best to specify either a proxy server *or* a socks server, *not* both at the same time. If you specify proxy servers, leave the socks field blank, and vice versa.

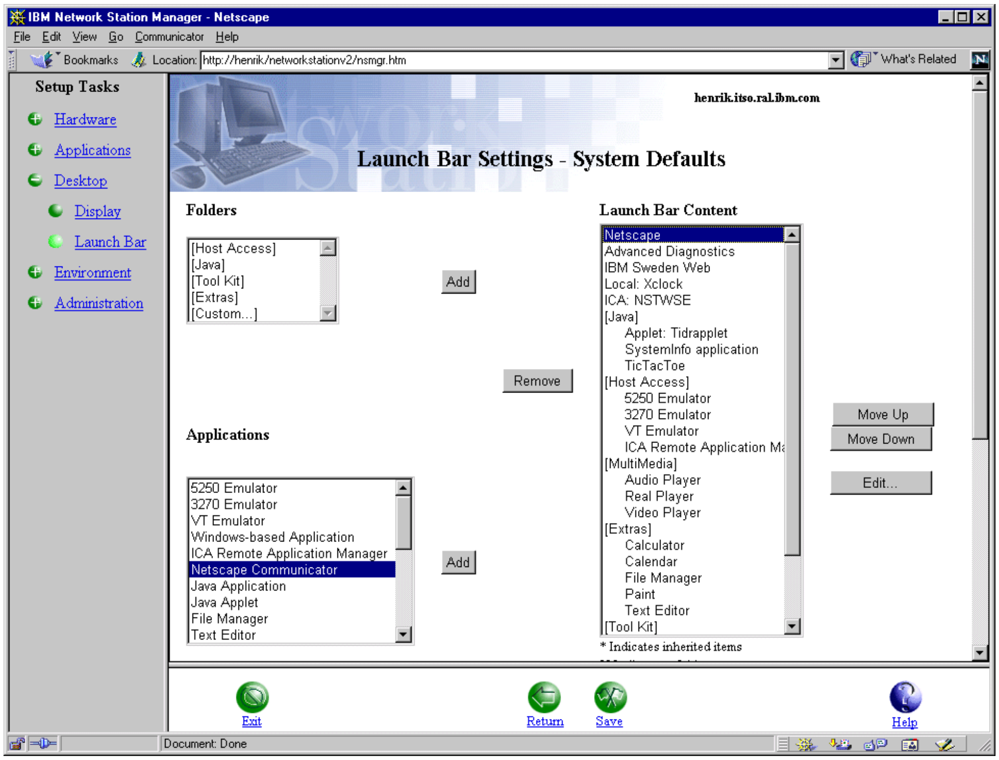
- **Proxy exceptions**: If you want to bypass the proxy servers for certain host names, you can define those addresses in the corresponding input fields. Normally, you bypass the proxy servers only if the host names you want to reach are inside your firewall.

Note

If (and only if) you set the proxy settings to *Default* or *Manual* in **Applications->Netscape Communicator** will the browser pick up the proxy settings defined in the **Environment->Network** panel in NSM.

12.3.3 Configuring the Netscape Communicator 4.5 Launch Bar icon: Startup values

On the **Desktop->Launch Bar** panel in NSM, you can add an icon for Netscape Communicator to the NC Desktop Launch Bar. Select **Netscape Communicator** from the Applications, and then click **Add** (Figure 306 on page 344).



Location: http://henrik/networkstationv2/nsmgr.htm

henrik.itso.ral.ibm.com

Launch Bar Settings - System Defaults

Folders

[Host Access]
[Java]
[Tool Kit]
[Extras]
[Custom...]

Applications

5250 Emulator
3270 Emulator
VT Emulator
Windows-based Application
ICA Remote Application Manager
Netscape Communicator
Java Application
Java Applet
File Manager
Text Editor

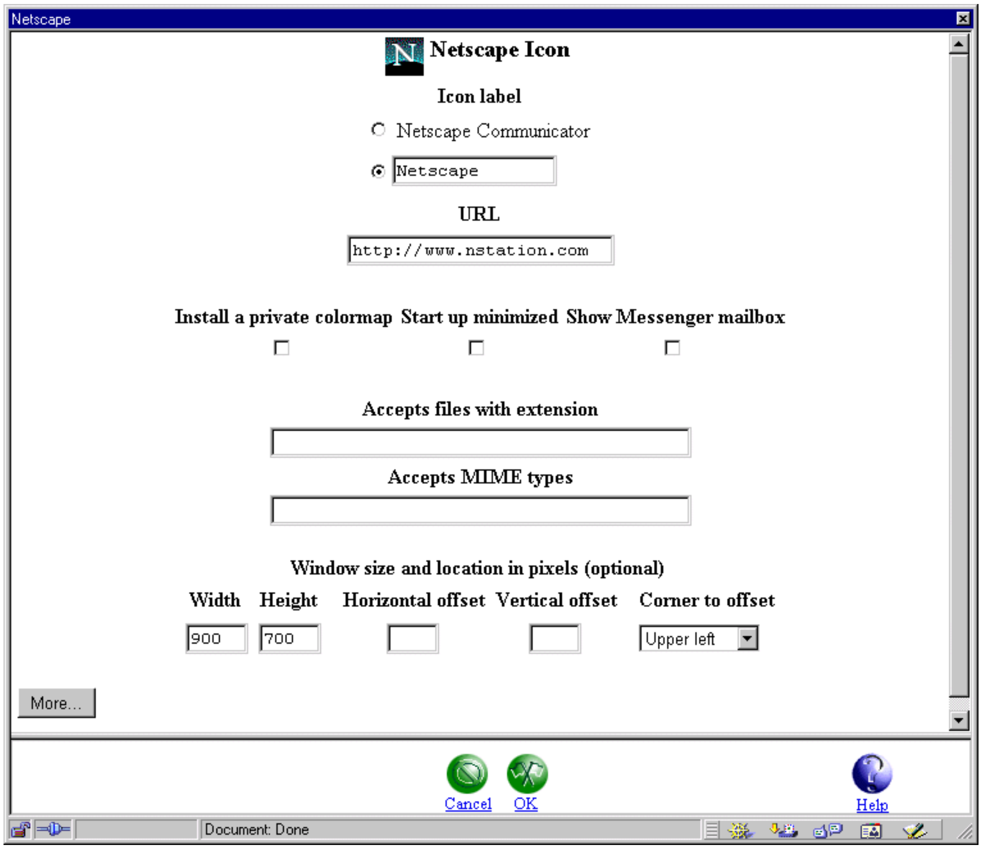
Launch Bar Content

Netscape
Advanced Diagnostics
IBM Sweden Web
Local: Xclock
ICA: NSTWSE
[Java]
    Applet: Tidrapplet
    SystemInfo application
    TicTacToe
[Host Access]
    5250 Emulator
    3270 Emulator
    VT Emulator
    ICA Remote Application Ma
[MultiMedia]
    Audio Player
    Real Player
    Video Player
[Extras]
    Calculator
    Calendar
    File Manager
    Paint
    Text Editor
[Tool Kit]

* Indicates inherited items

Figure 306. Adding an icon for Netscape to the NC Desktop Launch bar

The window shown in Figure 307 appears.



Netscape

Netscape Icon

Icon label

○ Netscape Communicator

● Netscape

URL

http://www.nstation.com

Install a private colormap	Start up minimized	Show Messenger mailbox
□	□	□

Accepts files with extension

Accepts MIME types

Window size and location in pixels (optional)

Width	Height	Horizontal offset	Vertical offset	Corner to offset
900	700			Upper left

Figure 307. Configuration settings for the Netscape Launch Bar icon

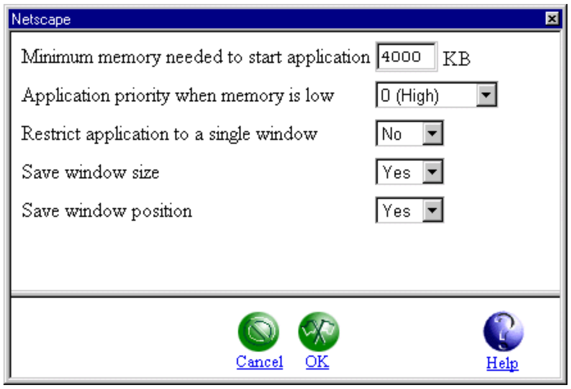
In the panel shown in Figure 307, you make settings that customize *this* particular invocation of the browser:

- **Icon label**: Select the second radio button and enter the name for the icon or simply select the first radio button to keep the default icon name Netscape Communicator.
- **URL**: This is the URL the browser should launch at startup. It does not affect the user's home page, which is reached by clicking the Home button in the browser.
- **Install a private color map**: If you experience color distortion on images displayed in the browser, you can try to select this box. This allows the browser to allocate more colors to itself than it normally does. Be aware, however, that this may affect other applications running in the Network Station. This option is usually not needed.
- **Start up minimized**: Usually the browser starts in a window on the screen. If, for some reason, you don't want to display the window immediately you can start the browser in minimized (iconized) mode instead, by selecting this box. This can be useful if you, for example, want to preload the browser when the user logs on.
- **Show Messenger mailbox**: Usually, when the browser is launched it starts the Navigator component, which enables you to view Web pages. If you want, you can start it with the Messenger component (the mail and news reader) instead by selecting this box. If you start it with the Messenger component, the

user can easily switch to the Navigator component later by selecting **Navigator** from the **Communicator** menu.

- **Accepts files with extension**: This is a comma-separated list of filename extensions that the Netscape Communicator understands. This is used to launch the browser from the NC Desktop when a user double-clicks on a file with an extension supported by the browser.
- **Accepts MIME types**: This is a comma-separated list of MIME types that Netscape Communicator understands. This is used to launch the browser from NC Desktop when a user double-clicks on a file that has a MIME type supported by the browser.
- **Window size and location in pixels (optional)**: These fields (Width, Height, Horizontal offset, and Vertical offset) allow you to specify the width and height of the browser's window and its starting position. The values should be specified in pixels. The Corner to offset parameter allows you to specify if the Horizontal and Vertical offsets should be counted from the upper left corner, upper right corner, lower left corner or lower right corner of the screen.

Clicking the More... button brings up another dialog, where you can specify the following parameters (Figure 308):



Minimum memory needed to start application 4000 KB
Application priority when memory is low 0 (High)
Restrict application to a single window No
Save window size Yes
Save window position Yes

Figure 308. More... settings

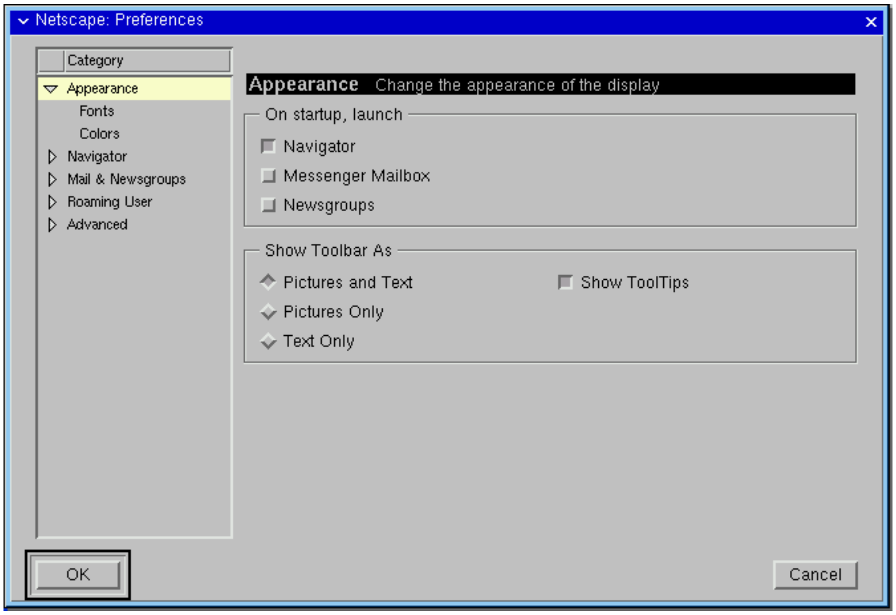
- **Minimum memory needed to start application:** This value defines the absolute minimum amount of memory that must be available in the Network Station to allow this application to start. It is specified in kilobytes (KB).
- **Application priority when memory is low**: If the Network Station is about to run out of memory, it needs to terminate one or more applications to allow the vital applications to continue to run. For this purpose, each application can be given a priority ranging from -1 (Critical) and 0 (High priority) to 10 (Low priority). When the Network Station needs to terminate applications, it starts with the least important applications, meaning those who have a higher value.
- **Restrict application to a single window**: If you want to deny an application the permission to open multiple windows, select **Yes** for this option. If you want to allow applications to open one or more windows, select **No**. This can be useful, for example, to deny the Netscape Communicator 4.5 browser to open new windows, which may clutter up the entire screen. Be careful with this setting since if additional windows cannot be opened, the application may not work as it should.

- **Save window size**: If you want the application to start with the same window size as it had when you last closed it, select **Yes** for this option. If you don't want this feature, select **No**.
- **Save window position**: If you want the application to start at the same position it had when you last closed it, select **Yes** for this option. If you don't want this feature, select **No**.

12.3.4 Configuration in the browser itself

In this section, we describe the settings that are made in the browser itself. These are usually modified by the end users themselves. The majority of these settings are identical to the settings found in Netscape Communicator 4.5 on any other platform. Instead of going through all of them here (when they can be found in Netscape's own documentation), we only cover the ones that differ and others that we found interesting and worth pointing out.

The configuration panels are accessed by choosing **Edit -> Preferences** in the browser. The configuration panels have a tree menu to the left where you select which category of settings you want to modify (Figure 309).



Appearance Change the appearance of the display

On startup, launch

☒ Navigator
☐ Messenger Mailbox
☐ Newsgroups

Show Toolbar As

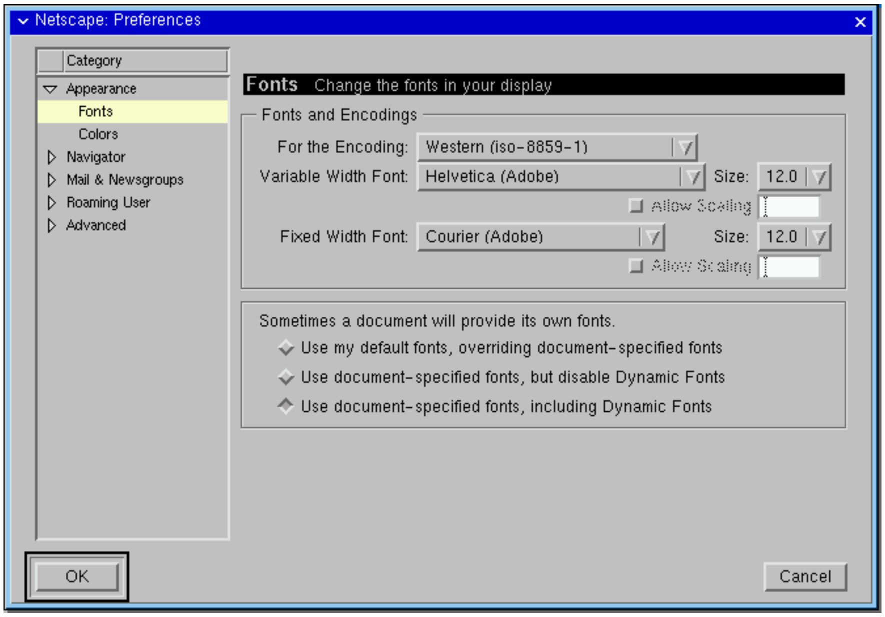
● Pictures and Text
○ Pictures Only
○ Text Only

☒ Show ToolTips

Figure 309. Configuring Netscape startup component

On the Appearance main panel (Figure 309), you configure which component the browser should launch at startup:

- **Navigator**: This launches the browser component, which enables you to start viewing Web pages.
- **Messenger Mailbox**: This launches the e-mail component. This startup option is also selectable from NSM.
- **Newsgroups**: This launches the news groups (NNTP) component.



Fonts Change the fonts in your display

Fonts and Encodings

For the Encoding: Western (iso-8859-1)

Variable Width Font: Helvetica (Adobe) Size: 12.0

□ Allow Scaling

Fixed Width Font: Courier (Adobe) Size: 12.0

□ Allow Scaling

Sometimes a document will provide its own fonts.

○ Use my default fonts, overriding document-specified fonts

○ Use document-specified fonts, but disable Dynamic Fonts

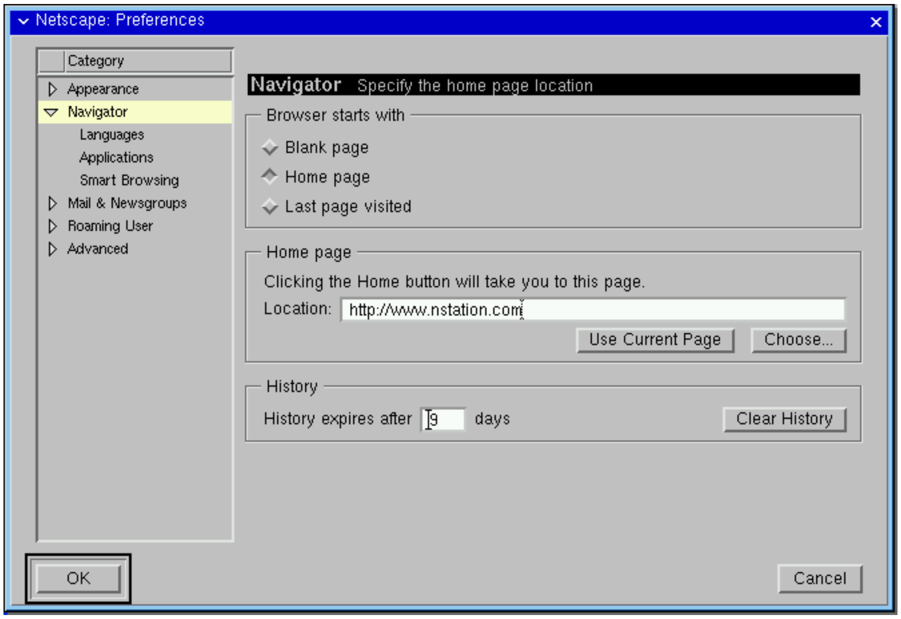
● Use document-specified fonts, including Dynamic Fonts

Figure 310. Configuring Netscape fonts

On the Fonts panel (Figure 310), you can customize how the browser should treat fonts and which fonts to use. We found the Helvetica (Adobe) and Courier (Adobe) fonts to be clear and readable. When you pick a font, try to pick one that is available in many different sizes. That's really why we chose the Adobe version of the fonts. Otherwise, we liked the IBM versions better.

By default, the font you select is not used unless a Web page lacks pre-defined font information (which very few Web pages do today). You can override this behavior and tell the browser to use the fonts you select by choosing one of the following two options:

- **Use my default fonts, overriding document-specific fonts**: This option overrides the font selection made by the Web page creator. *Always* use your selected fonts instead.
- **Use document-specific fonts, but disable Dynamic Fonts**: This option overrides the font selection made by the Web page creator *only* in case the fonts specified in the HTML page are not locally available on your Network Station, thus requiring them do be downloaded. Using this option can speed up downloading of Web pages since the fonts you selected will be used instead and no font downloading will take place.



Navigator Specify the home page location

Browser starts with

○ Blank page
● Home page
○ Last page visited

Home page

Clicking the Home button will take you to this page.

Location: http://www.nstation.com

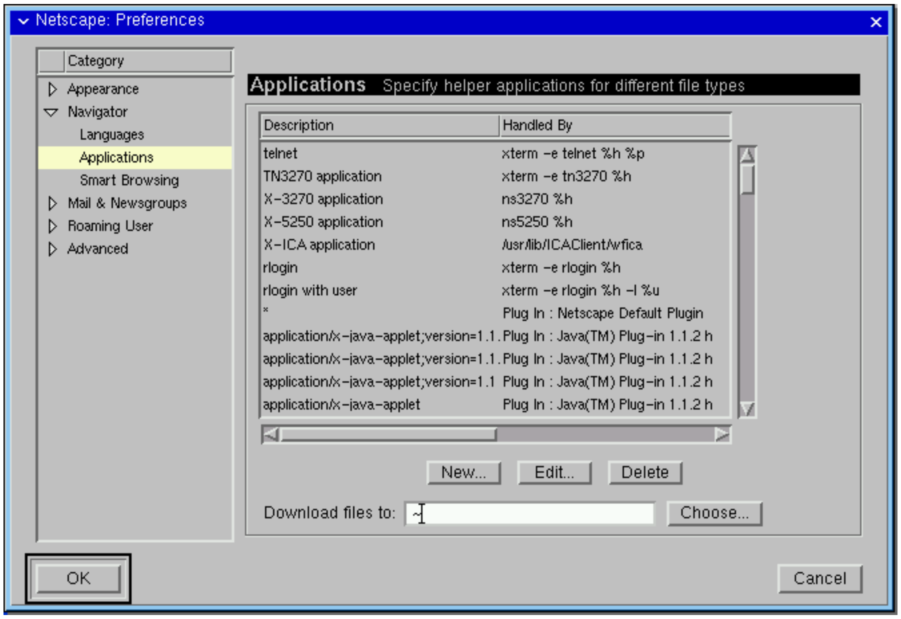
History

History expires after 9 days

Figure 311. Configuring Netscape startup page

On the Navigator main panel (Figure 311), you can configure the browser startup page. This setting can also be configured in NSM. You can select between Blank page, Home page or Last page visited.

On the Home page location field, you can enter the name of your default Home page. This information is taken from NSM (if configured there), but it can be overridden here.



Applications Specify helper applications for different file types

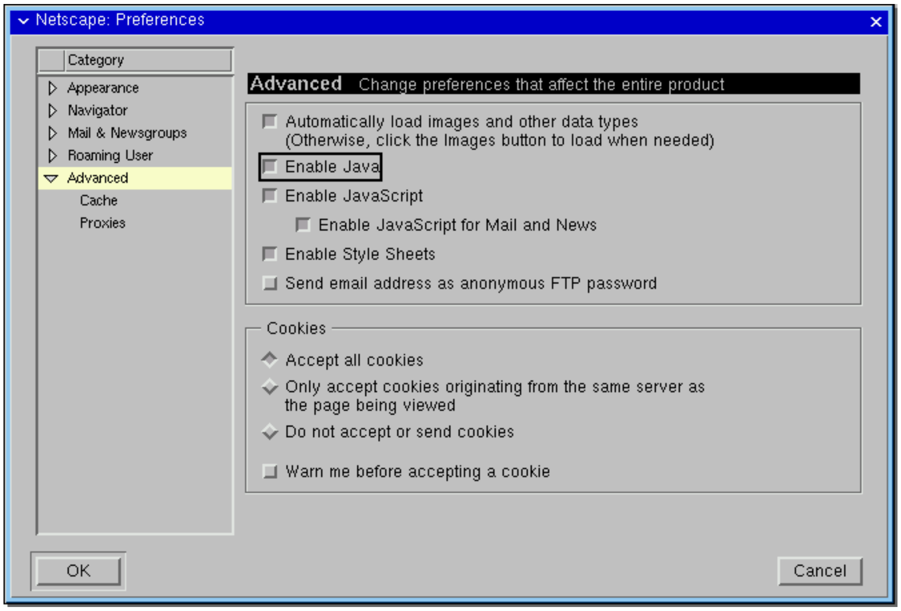
Description	Handled By
telnet	xterm –e telnet %h %p
TN3270 application	xterm –e tn3270 %h
X–3270 application	ns3270 %h
X–5250 application	ns5250 %h
X–ICA application	/usr/lib/ICAClient/wfica
rlogin	xterm –e rlogin %h
rlogin with user	xterm –e rlogin %h –l %u
*	Plug In : Netscape Default Plugin
application/x–java–applet;version=1.1.	Plug In : Java(TM) Plug–in 1.1.2 h
application/x–java–applet;version=1.1.	Plug In : Java(TM) Plug–in 1.1.2 h
application/x–java–applet;version=1.1	Plug In : Java(TM) Plug–in 1.1.2 h
application/x–java–applet	Plug In : Java(TM) Plug–in 1.1.2 h

Download files to: ~

Figure 312. Configuring Netscape helper applications

On the Applications panel (Figure 312), you can define helper applications that are used whenever the browser detects a MIME type that it cannot handle on its own. It then launches the corresponding external helper application. The Netscape Communicator comes with a number of pre-defined helper applications already configured but, if you like, you can add your own. However, for these applications to work, they must be executable by the Network Station's operating system which means they must be written and specifically compiled for it, or, as a better alternative, written in Java. Since there are no useful native Network Station applications that are not already pre-defined, we won't describe how to add any.

In the Download files to field, you can specify a default directory where files downloaded by the browser are saved. The information in this field is just a default value and can easily be overridden by the file save dialog that appears when the user downloads a file. If you enter a directory that does not exist, the browser will create it for you. We specified a tilde, ~, which is a shortcut for the user's home directory.



Advanced Change preferences that affect the entire product

☑ Automatically load images and other data types (Otherwise, click the Images button to load when needed)

☑ Enable Java

☑ Enable JavaScript

☑ Enable JavaScript for Mail and News

☑ Enable Style Sheets

☐ Send email address as anonymous FTP password

Cookies

● Accept all cookies

○ Only accept cookies originating from the same server as the page being viewed

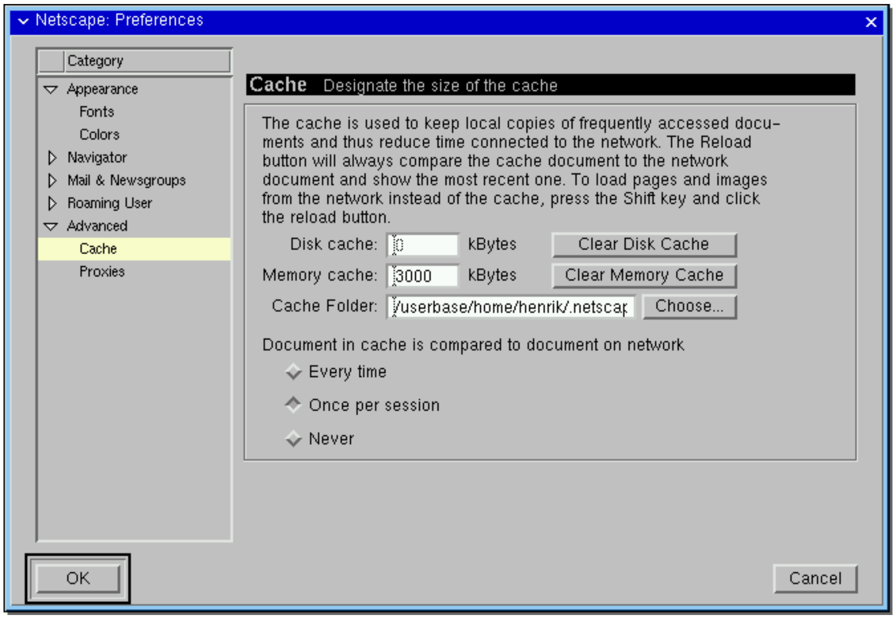
○ Do not accept or send cookies

☐ Warn me before accepting a cookie

Figure 313. Configuring advanced settings, Java

On the Advanced main panel (Figure 313), you configure such settings as Java and cookie support.

By default, the browser comes with Java applet support disabled. The support, which can also be enabled or disabled with NSM settings, can be overridden by this value. We strongly recommend enabling the Java applet support. Today's Web pages often contain Java applets to provide functionality. If the browser ignores those applets, the Web pages may not work as designed. Therefore, select the **Enable Java** check box.



Cache Designate the size of the cache

The cache is used to keep local copies of frequently accessed documents and thus reduce time connected to the network. The Reload button will always compare the cache document to the network document and show the most recent one. To load pages and images from the network instead of the cache, press the Shift key and click the reload button.

Disk cache: 0 kBytes

Memory cache: 3000 kBytes

Cache Folder: /userbase/home/henrik/.netscap

Document in cache is compared to document on network

- ○ Every time
- ● Once per session
- ○ Never

Figure 314. Configuring browser cache settings

On the Cache panel (Figure 314), you configure the browser's cache settings. Since the Network Station has no local storage, the browser is configured not to use any disk cache. You should not try to enable this in any way, since it will only severely reduce the performance of the browser. Memory cache, however, can be increased if the Network Station has enough memory to improve the performance and responsiveness of the browser. The memory cache is also configurable in NSM.

The Cache Folder specifies where the browser stores its cached files. Since the browser does not use any disk cache, this folder is never created or used.

12.4 External helper applications

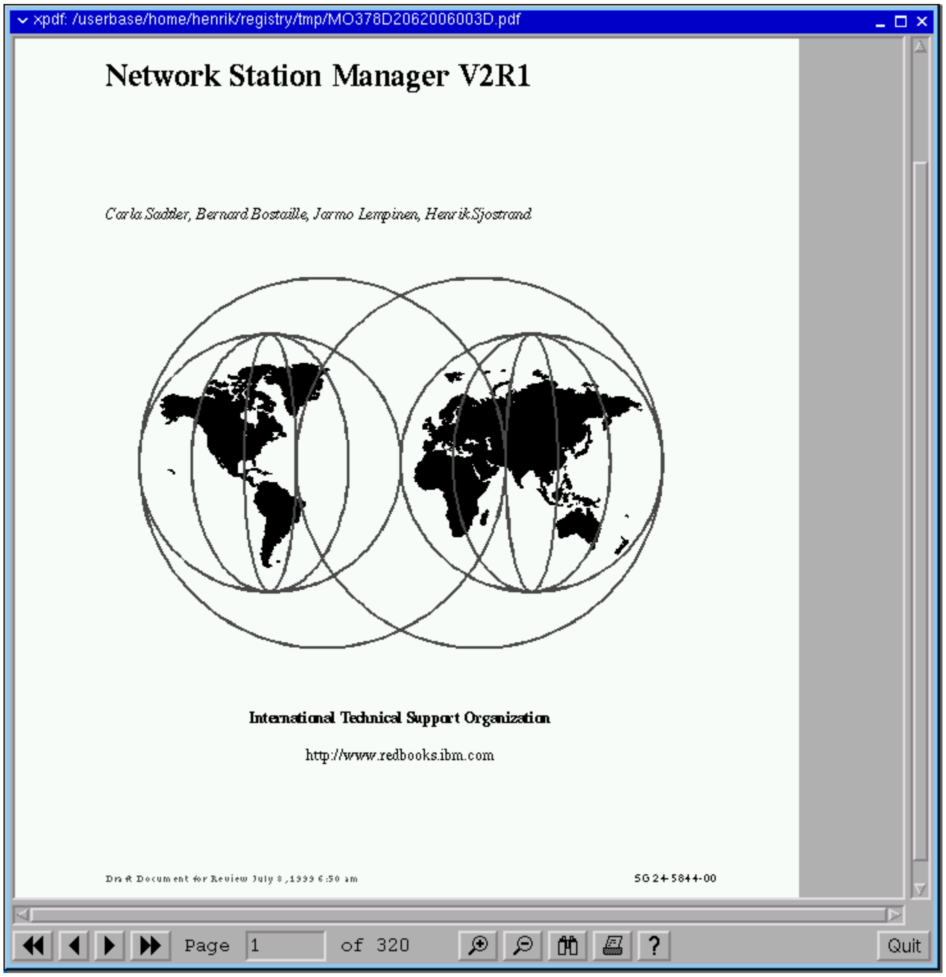
NSM V2R1 ships with a number of external helper applications that are pre-configured to start whenever the browser detects the corresponding file or MIME type.

12.4.1 PDF viewer

The PDF viewer (Figure 315 on page 352) shipped with NSM V2R1 is a version of the XPDF PDF viewer. It supports the Adobe Acrobat PDF 1.2 format. It is a basic PDF viewer without too many bells and whistles. However, it can generate PostScript output from the document viewed and store it in the user's home directory.

The viewer is pre-configured to automatically launch whenever the browser detects a file with the .pdf extension. When launched, it displays in its own window, outside of the browser. If a user clicks on multiple PDF files in the browser, multiple instances of the PDF viewer are started so the user can view many PDF documents on the screen simultaneously.

The file to be viewed is downloaded into the tmp directory in the user's home directory and is given a temporary file name. When the PDF viewer terminates, the temporary file is deleted.



xpdf: /userbase/home/henrik/registry/tmp/MO378D2062006003D.pdf
Page
1
of 320
?
Quit

Network Station Manager V2R1

Carla Sadtler, Bernard Bostaille, Jarmo Lempinen, Henrik Sjostrand

International Technical Support Organization

http://www.redbooks.ibm.com

Draft Document for Review July 8,1999 6:50 am

SG24-5844-00

Figure 315. PDF viewer

To navigate in the PDF document, the keyboard combinations shown in Table 48 are used (some only work when the document is zoomed in enough).

Table 48. PDF viewer keyboard combinations

Key	Action
Up, down arrows	Scroll one line up, down
Left, right arrows	Scroll left, right
Page Up, Page Down	Scroll up (previous page), down (next page)
Home, End	Jump to top of page, end of page
Home	Jump to top of page
End	Jump to end of page

The mouse combinations shown in Table 49 are used.

Table 49. PDF viewer mouse combinations

Mouse combination	Action
Left mouse button	Select text
Right mouse button	Display pop-up menu with options to open new file, save current file, rotate left or right, and quit
Both mouse buttons	Pan in the window (all directions)

The PDF viewer also has a number of icons at the bottom. They perform the functions listed in Table 50.

Table 50. PDF viewer navigation icons

Icon	Action
Left, right double arrows	Previous, next 10 pages
Left, right arrow	Previous, next page
Page field	Enter the page number you want to jump to directly
Zoom in, out	Zooms the document in, out
Binoculars	Search for text
Printer	Create PostScript output file
Question mark	Display About box. The URL in the About box is outdated, the correct one should be: `http://www.foolabs.com/xpdf`

12.4.2 NC Audio player

NSM V2R1 also ships an audio player application. This is pre-configured to automatically launch when the Netscape browser detects an audio file. The supported file formats are RIFF Wave files (.wav extension), Sun AU files (.au extension), and the Audio Interchange Format files (.aif, .aiff, .aifc extensions).

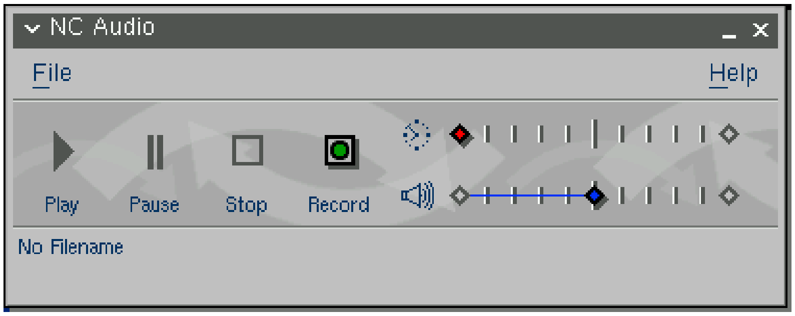


Figure 316. NC Audio player

The audio player is also an application without too many bells and whistles. It has buttons for play, pause, stop, and record. There are two bars to the right. The upper one displays an indicator for the current position in the file, and the lower one is the volume bar.

Note

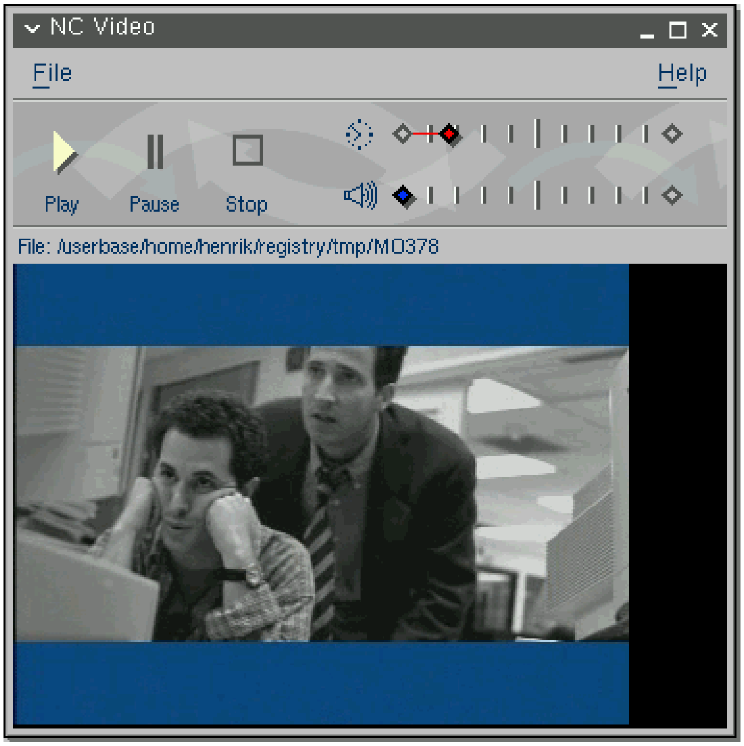
- The WAV, AU and AIFF audio formats are *non-streaming* media types. Therefore, the NC Audio player needs to load the entire file into RAM before it can start playing it. This may require a lot of RAM, depending on the size of the file.
- At the time this redbook was written, there was a known problem with the record function. This problem is planned to be fixed in PTF 2 for Network Station Manager which is already available.

12.4.3 NC Video player

In NSM V2R1, there is also a video player application, which is a repackaged version of the open-source Xanim player. It is pre-configured to automatically launch when the Netscape browser detects a video file. The supported file formats are MPEG video (.mpeg, .mpg, .mpe extensions), Microsoft Video (.avi extension), Apple Quicktime (.qt, .mov extensions) and SGI Video (.movie extension). NC Video player is shown in Figure 317.

Notes

- As of today, the NC Video player does not support Apple’s latest version of the QuickTime video format, Version 4.0. The NC Video player support corresponds to QuickTime 2.0.
- More information on the Xanim player can be found at:
  `http://xanim.va.pubnix.com`



File: /userbase/home/henrik/registry/tmp/MO378

Figure 317. NC Video player

Just as the other players, the video player is a basic application without too many bells and whistles. It has buttons for play, pause, and stop. There are two bars on the right. The upper one displays an indicator for the current position in the file, and the lower one is the volume bar.

Note

The MPEG, AVI, QuickTime, and SGI Video formats are *non-streaming* media types. Therefore, the NC Video player needs to load the entire file into RAM before it can start playing it. This may require a lot of RAM, depending on the size of the file.

12.4.4 RealPlayer

NSM V2R1 also includes a RealPlayer 5.0 helper application. The latest version of the RealPlayer for the Windows platform is called G2, which is more recent than the one shipped with NSM V2R1. The RealPlayer application (Figure 318 on page 356) is pre-configured to automatically launch whenever the browser detects the .ra, .rm or .ram file extensions.

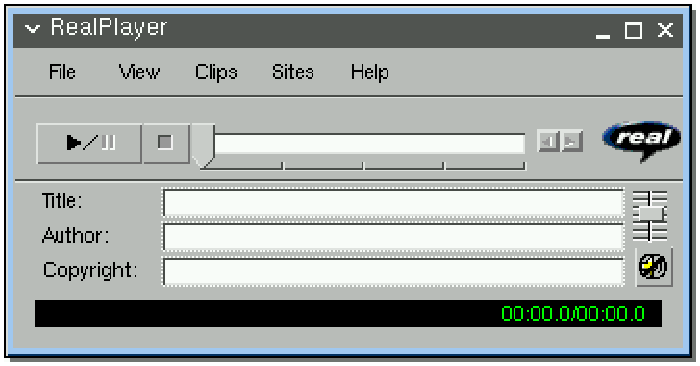


Figure 318. RealPlayer

Note

The RealAudio and RealMedia (.ra, .rm, .ram) media types are *streaming* media types. This means the RealPlayer does not have to load the entire file into RAM before it can start playing.

12.5 Using the Java Plug-In feature

Netscape Communicator 4.5 includes its own JVM, capable of running Java applets embedded in Web pages visited by the browser. By default, this internal JVM is used to run the Java applets, which provide full compatibility with Netscape Communicator 4.5 on other platforms.

When we ran our sample Java applet (described in Chapter 11, “Java environment” on page 305) in the browser’s internal JVM, the Java system properties had the following values:

```
java.version = 1.1.5
java.vendor = Netscape Communications Corporation
java.class.version = 45.3
os.name = NetBSD
os.version = 1.3I-NCOS
os.arch = i386
```

Then, we configured the browser to use the IBM enhanced 1.1.8 JVM using the Java Plug-In feature. To do this, go to **Applications->Netscape Communicator** in NSM. Change the Runtime Plug-In for Network Station parameter to **Enabled**. When we ran the same Java applet again, the browser loaded the IBM enhanced 1.1.8 JVM. The Java system properties had the following values:

```
java.version = nwsbld:08/07/07-08:52
java.vendor = IBM Corporation
java.class.version = 45.3
os.name = NetBSD
os.version = 1.x
os.arch = x86
```

As you can see from the java.version property, the Java applet now runs in the IBM enhanced JVM.

Note

The first time the browser encounters a Java applet that is to be redirected to the IBM enhanced external JVM, it takes some time for the Network Station to load the JVM before it displays the applet. However, once the JVM is loaded, the applets display much quicker.

12.6 Java-based MIME viewers

Using Java, you can develop your own viewer for any MIME type that is not available or shipped with the Network Station Manager. The browser can then be configured to automatically launch your MIME viewer whenever the corresponding MIME type is detected in a Web page.

12.7 Command line options and parameters

Table 51 and Table 52 on page 359 list the command line options and parameters that can be used to launch the Netscape Communicator 4.5. Unfortunately, we did not find any command line options that we found interesting and useful to use in a thin client environment. These listings are merely for reference. Also, we have not verified that all these command line options actually work on Network Station. The listings are, however, valid for the UNIX versions of the Netscape Communicator 4.5 browser, which the Network Station uses. The command line options can be displayed by issuing the `netscape -help` command from the Advanced Diagnostics shell.

Table 51. Netscape Communicator 4.5 command line options

Result	Command	Parameters
Display a list of all the command line options, with a brief explanation of each.	`-help`	
Open NetHelp at startup.	`-nethelp`	`[nethelp_URL]`
Bypass the license page that appears at startup.	`-no-about-splash`	
Show the version number and build date.	`-version`	
Specify the X server to use.	`-display`	`[dpy]`
Start up iconified.	`-iconic`	
Force session management on. Session management is supported by default.	`-session-management`	
Force session management off. Session management is supported by default.	`-no-session-management`	

Result	Command	Parameters
Force session management on. Session management is supported on Irix by default. This may be needed on Irix systems that require explicit settings, as with some SGI systems.	`-irix-session-management`	
Force session management off. Session management is supported on Irix by default. This may be needed on Irix systems that require explicit settings, as with some SGI systems.	`-no-irix-session-management`	
Ignore window geometry saved for session.	`-ignore-geometry-prefs`	
Don't save the session's window geometry.	`-dont-save-geometry-prefs`	
Use a specific server visual.	`-visual`	`[id-or-number]`
Install a private color map.	`-install`	
Use the default color map.	`-no-install`	
Set the maximum number of colors to allocate for images (when not using `-install`).	`-ncols`	`[N]`
Force 1-bit deep image display.	`-mono`	
Set a specific X resource.	`-xrm`	`[resource-spec]`
Run a command in an already running Netscape process.	`-remote`	`[remote-command]`
Following a `-remote` command, cause the window to raise to the top.	`-raise`	
Following a `-remote` command, do not cause the window to raise to the top.	`-noraise`	
Ignore the `alwaysraised`, `alwayslowered`, and `z-lock` attributes of JavaScript `window.open()`.	`-dont-force-window-stacking`	
The ID of an X window to which `-remote` commands should be sent (if unspecified, the first window found is used).	`-id`	`[window-id]`
Show only the Component Bar.	`-component-bar`	

Result	Command	Parameters
Position and size the Messenger and Collabra windows.	`-geometry`	`=WxH+X+Y`
Open Messenger (displays the Inbox by default).	`-messenger`	
Open Messenger (an alternate option that also displays the Inbox by default).	`-mail`	
Open the Message Center, and go to the first subscribed discussion group server.	`-discussions`	
Open the Message Center, and go to the first subscribed discussion group server (an alternate option that works the same as `-discussions`).	`-news`	
Open Composer and optionally open the document at the specified URL.	`-composer`	`[URL]`
Open Composer and optionally open the document at the specified URL (an alternate option that works the same as `-composer`).	`-edit`	`[URL]`

Note

Since the NSM V2R1 Netscape Communicator does not include all of the functions found in Netscape Communicator on other platforms, some of the above command line options have no effect. Specifically the `-composer` and `-edit` have no effect since the Composer component is not used for creating or editing Web pages. Also the `-no-about-splash` parameter has no effect, since the browser is configured not to display the splash screen by default.

Table 52. Netscape Communicator 4.5 command line parameters

Parameter	Definition
`path to initialization file`	The full path to the appropriate initialization file. The default name for this file is `netscape.ini`.
`"user's profile name"`	The individual user's name as it appears in the Profile Manager, bracketed by quotes.
`file_name`	The full path to the HTML document.
`URL`	The URL of the page to display.
`LDIF_file_name`	The full path to the LDIF file.
`message`	The name of a file containing a message, including its full path. The default search location is the `Temp` directory.

Parameter	Definition
attachments	The name or names of the attachments or attachment lists, including the full path for each. Lists are preceded with the @ symbol, individual attachments are preceded with a hyphen. Multiple names are delimited by a vertical bar (|), and single names are preceded by a hyphen (-). The default search location is the Temp directory.
nethelp_URL	The URL of the NetHelp content, usually located in folders under \nethelp\netscape.
dpy	The name of the UNIX X server to use, in the format machinename:0.
id-or-number	The specific server visual to use.
N	The integer for the maximum number of colors to allocate for images.
resource-spec	The name of a specific X resource.
remote-command	The remote command to execute in an already-running Netscape process. For more information, see http://home.netscape.com/newsref/std/x-remote.html
window-id	The ID of an X window to receive -remote commands.

12.8 Advanced customization using JavaScript

Important note

Using these advanced customization techniques, it’s possible to create a combination of settings that render the Netscape Communicator non-working. Some of these customizations can create an unsupported setup.

It is important that you test your setup before putting it into a production environment. Also, if reporting a problem to IBM Service, make sure you can reproduce your problem with all advanced settings removed and with a supported setup, before contacting IBM Service.

As mentioned previously, the Netscape Communicator retrieves its settings from four different locations: the IBM-shipped default settings, the settings made using NSM or NSMCL, the settings made in the browser itself, and settings made in hand-edited configuration files. When the browser starts, it reads the following configuration files and extracts settings from them:

- **$ProdBase/<x86|ppc>/usr/local/netscape/netscape.cfg**

  This file contains miscellaneous settings shipped as Netscape default settings. Typical settings are MIME types, helper applications, etc. On other platforms, this file is not in ASCII format, but on the Network Station platform, it is to allow NSM to modify its contents. This file should not be manually modified.

- **$UserBase/home/{userid}/.netscape/preferences.js**

  This file is the sum of the settings retrieved from NSM, netscape.cfg, and the settings the user made in the browser using the Edit->Preferences dialogs. This file should not be manually modified since it's created by the browser. Settings in this file are overridden by settings in the netscape.cfg file. This means that if a setting exist in both files, the netscape.cfg file setting is what is used.

- **$ProdBase/<x86|ppc>/usr/local/netscape/overrides.js**

  This file contains settings that override the settings in both netscape.cfg and preferences.js. All advanced customizations should be put in this file. This file does not exist after an NSM installation but must manually be created and populated with settings.

Notes

- In addition to these files, the browser also creates a file called liprefs.js in the .netscape subdirectory in the user's home directory. This file is used for storing a local backup copy of the preferences stored on a roaming server when the roaming users feature is used. Since the NSM V2R1 browser does not support roaming users, this file is not used. However, it is still created in order to maintain compatibility with Netscape Communicator on other platforms.
- Netscape Communicator 4.5 supports Netscape AutoConfig URLs. These are URLs that the browser can visit on startup and re-visit with regular intervals to get configuration settings. We do not document this feature here, since it works just like it does on all Netscape platforms. For more information on this configuration technique, visit Netscape at:
  `http://developer.netscape.com/docs/manuals/deploymt/index.htm`
- The preferences are set via shipped.nsm, which is read before all Netscape files. Thus, shipped.nsm would have to be modified by removing the desired Netscape preferences from the shipped.nsm file altogether.

All these files are JavaScript files, which means they conform to the JavaScript programming language syntax. They are read every time the browser starts. If you make a modification, you only need to restart the browser, not logoff or power off.

The only file that should be manually created and updated is the overrides.js file. The syntax of this file is shown here:

```
//Begin CE prefs
with (PrefConfig) {
config(param, value);
defaultPref(name, value);
lockPref(name, value);
unlockPref(name, valie);
} // with (PrefConfig)
```

The preferences you want to set should be wrapped within the PrefConfig{} object as shown here:

```
with (PrefConfig) {
...
...
} // with (PrefConfig)
```

Each line must end with a semicolon (;).

The JavaScript functions listed in Table 53 are available for configuring the preferences.

Table 53. Overrides.js file syntax

Function	Purpose
//	Remarks. If used in the beginning of a line, it remarks the whole line. If used in the middle of a line, it remarks the rest of the line.
config(param, value)	Sets configuration parameters for items that are not possible to modify through user dialogs, for example, custom logo art or menu commands.
defaultPref(name, value)	Sets a preference and leaves it open for a user to modify the value. This is used to provide default values and can also be used to show the user the correct syntax, for example, in the e-mail address field.
lockPref(name, value)	Sets a preference and locks it. This means the user cannot modify its value.
unlockPref(name)	Explicitly releases a preference to allow a user to modify its value.

Note

- There are many more commands available in the JavaScript language. We do not describe them here since JavaScript programming is not within the scope of this redbook. For more documentation, visit Netscape at:
  `http://developer.netscape.com/docs/manuals/deploymt/index.htm`
- While viewing Netscape JavaScript configuration files on various platforms, you may also come across the command `userPref(name, value)`. This is exactly the same as `defaultPref(name, value)`.

The Netscape Communicator 4.5 browser supports several hundred different preferences that can be used in the overrides.js file to customize the browser. A full list of the supported parameters can be found at the Netscape URL:
`http://developer.netscape.com/docs/manuals/deploymt/index.htm`

Note, however, that the full list includes many preferences that do not apply to the NSM V2R1 Netscape Communicator browser, for example, roaming users, Offline work mode, and so on.

We do not reproduce the full list here, but only a few of them to show how the advanced configuration concept works.

Table 54. Netscape advanced configuration preferences

Preference	Description
internal_url.net_search.url	Specifies the URL called by the Search button on the Navigation toolbar.
browser.use_document_fonts	Controls how Navigator responds to the fonts specified, or not specified, in Web pages. The default is 2, which always uses any font specifications that appear in documents, including any for Dynamic Fonts. Other values are: 0, never use fonts named in HTML documents (use only Navigator's defaults); 1, use any font specifications that appear in documents, but exclude any for Dynamic Fonts.
network.hosts.socks_server	Specifies the host name or IP address of a SOCKS server. The default is an empty string. If not using the default SOCKS port number of 1080, specify the port number with network.hosts.socks_serverport.
network.hosts.socks_serverport	Specifies the non-default port number of a SOCKS server. This preference isn't needed when using the default port number of 1080. The default is 1080. The correct port number is determined at the server.
browser.cache.memory_cache_size	Sets the size of the Web page cache Navigator maintains in memory. The default size is 3000 KB. The default sizes are the recommended minimum sizes.

Using these commands, we created the overrides.js file:

```
//Begin CE prefs
with (PrefConfig) {
config("internal_url.net_search.url", "http://www.altavista.com");
defaultPref("browser.use_document_fonts", 0);
lockPref("network.hosts.socks_server", "socks.raleigh.ibm.com");
lockPref("network.hosts.socks_serverport", 1080);
unlockPref("browser.cache.memory_cache_size");
defaultPref("browser.cache.memory_cache_size", 4096);
} // with (PrefConfig)
```

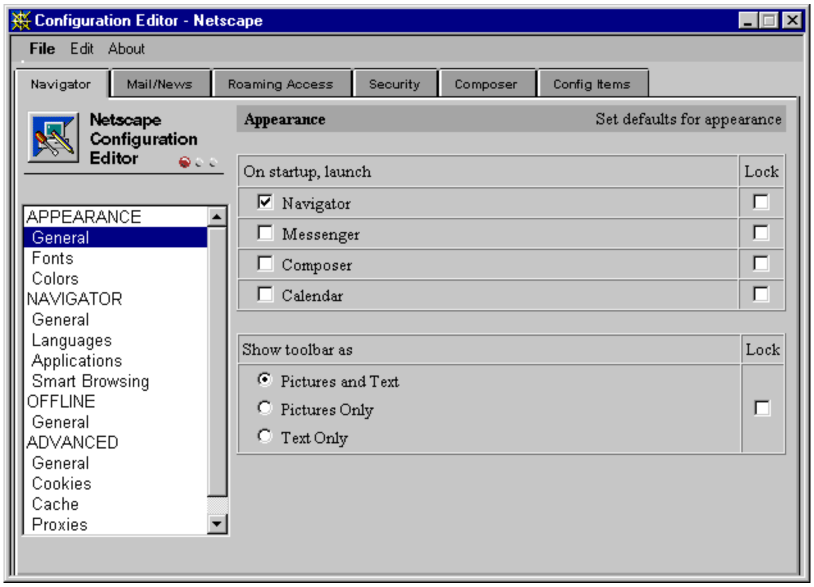
Using this file, we could change the search URL from Netscape’s default to AltaVista. We were also able to change the default font behavior. We set the socks address and also locked the value so a user could not modify it themself. We changed the cache size from the default 3000 KB to 4096 KB, but left it open so a user could change it themself. The parameters that are locked using the `lockPref` keyword are visually shown as locked in the browser’s dialogs.

12.8.1 Netscape Client Customization Kit

To simplify the creation of the JavaScript configuration files, Netscape provides two toolkits: the Netscape Mission Control and the Client Customization Kit. The Netscape Mission Control kit includes functions to create installable packages of the Netscape browser with customized settings and make them easily available to a large number of workstations (PCs). These features are not necessary in the Network Station environment since Network Station Manager manages all that. Therefore, we found the Client Customization Kit to be more suitable for the

Network Station environment. This toolkit can be downloaded free-of-charge from Netscape at the URL: `http://www.netscape.com/download/cck.html`

We downloaded the kit and installed it onto an Windows NT workstation. To start the toolkit, select **Start->Programs->Netscape Client Customization Kit->Netscape Configuration Editor**. This launches the Netscape browser and starts the Client Customization Kit, which is written as a Java applet (a signed applet so it can be granted file read and write accesses). Once granted access, the window shown in Figure 319 appears.



Appearance — Set defaults for appearance

On startup, launch	Lock
☑ Navigator	□
□ Messenger	□
□ Composer	□
□ Calendar	□

Show toolbar as	Lock
● Pictures and Text ○ Pictures Only ○ Text Only	□

Figure 319. Netscape Client Customization Kit

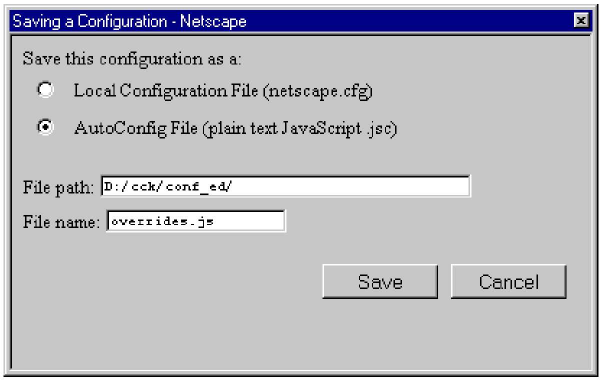
Using this graphical user interface, it is easy to customize the settings for the Netscape browser. Some of the settings this toolkit can customize do not apply on the Network Station Netscape browser, since it does not include all functions found in Netscape on other platforms. Examples of functions the toolkit can handle but the Network Station Netscape browser does not recognize are the Offline work mode, Smart Update, Roaming Access, Composer, and so on.

Important note

We strongly recommend that you *do not* customize any of the settings not supported by the Network Station Netscape browser. The IBM shipped defaults may contain special settings for some of these functions, and modifying them may render the browser as non-working.

While configuring the settings, it is possible to view the resulting output file by selecting **Edit->View**.

When you are done customizing the settings, make sure you save this file in the *ASCII* format by performing the following actions:



Save this configuration as a:

○ Local Configuration File (netscape.cfg)

● AutoConfig File (plain text JavaScript .jsc)

File path: D:/cck/conf_ed/

File name: overrides.js

Figure 320. Saving Client Customization Kit settings

1. Choose **File->Save As**, and select the **AutoConfig File (plain text JavaScript.jsc)** radio button. Enter a path and a file name.
2. When done, copy the file created by the Client Customization Kit to the \prodbase\<x86|ppc>\usr\local\netscape directory, and call it `overrides.js`.

Note

The Netscape Developers site contains a lot of information for anyone interested in tailoring the Netscape Communicator browser. Visit the site at: `http://developer.netscape.com`

12.9 Deploying standard enterprise bookmarks

When a user launches the browser for the first time, the browser creates a .netscape subdirectory in the user's home directory and populates this directory with a set of files. One important file is the bookmarks.html file that stores the user's bookmarks. The default set of bookmarks a user is given when they launch the browser for the first time is taken from the \prodbase\<x86|ppc>\usr\local\netscape\bookmark.htm file, which is created during the installation of NSM. When the browser starts for the first time, this file is simply copied (and renamed, see below) into the user's home directory.

If you want, you can populate this file with the default set of bookmarks you want to give your users. For example, you may want to initialize the browsers with bookmarks for your intranet, your suppliers, or your customers.

The bookmarks.html file in the user's home directory is an HTML file. The easiest way to modify this file is to run Netscape (on the Network Station, a PC or a Unix workstation) and create a set of bookmarks and folders using the tools available within the Netscape browser. Then, simply copy the bookmarks.html file from the user directory you are using (on the Network Station, the PC or UNIX system) and overwrite the \prodbase\<x86|ppc>\usr\local\netscape\bookmark.htm file (note the two different file names). All users launching the browser for the first time will then receive the default set of bookmarks you prepared for them. They will still be able to add, delete, and modify the bookmarks themselves. The bookmarks provided are just an initial set.

If a user (by accident) deletes their bookmarks file, the browser re-creates the file by using the \prodbase\<x86|ppc>\usr\local\netscape\bookmark.htm file, just as if the browser was started for the first time. The modifications the user had made will be lost, and the bookmarks will revert to those defined in the \prodbase\<x86|ppc>\usr\local\netscape\bookmark.htm file.

Notes

- The file in the \prodbase\<x86|ppc>\usr\local\netscape directory must be called bookmark.htm. When the Network Station Netscape browser reads it and copies it into the user's home directory, it renames it to bookmarks.html, which the file *must* be called when in the user's home directory. On the Windows platform, the file is called bookmark.htm, both in the Netscape program directory and in the user's home directory.
- On the Network Station, the bookmark file is a flat UNIX ASCII file. On a Windows system, the bookmark file is a flat DOS/Windows ASCII file. If you copy the bookmark.htm file from a Windows system, the Network Station Netscape browser can read the file but it is converted to the UNIX ASCII file format. If you copy the file back to Windows, the Windows Netscape browser can read the file, but will convert it back to the DOS/Windows ASCII file format.

12.10 Using the browser as the desktop to build a 'Web-top'

The NSM V2R1 Netscape Communicator 4.5 browser has had a few non-standard URL types added to it. Using these URL types, it is possible to launch applications that run *locally* in the Network Station. This feature can be used to build a 'Web-top', a browser-based desktop, which can be used instead of the normal NC Desktop. The application URLs shown in Table 55 are available.

Table 55. Local applications, URL names, and active status

Application	Application URL
3270 emulator	X-3270
5250 emulator	X-5250
ICA client	X-ICA
ICA Remote application Manager	X-ICAMgr

As a quick test, you can try these commands on the browser by entering, for example:

```
x-3270://ip_address_of_host
```

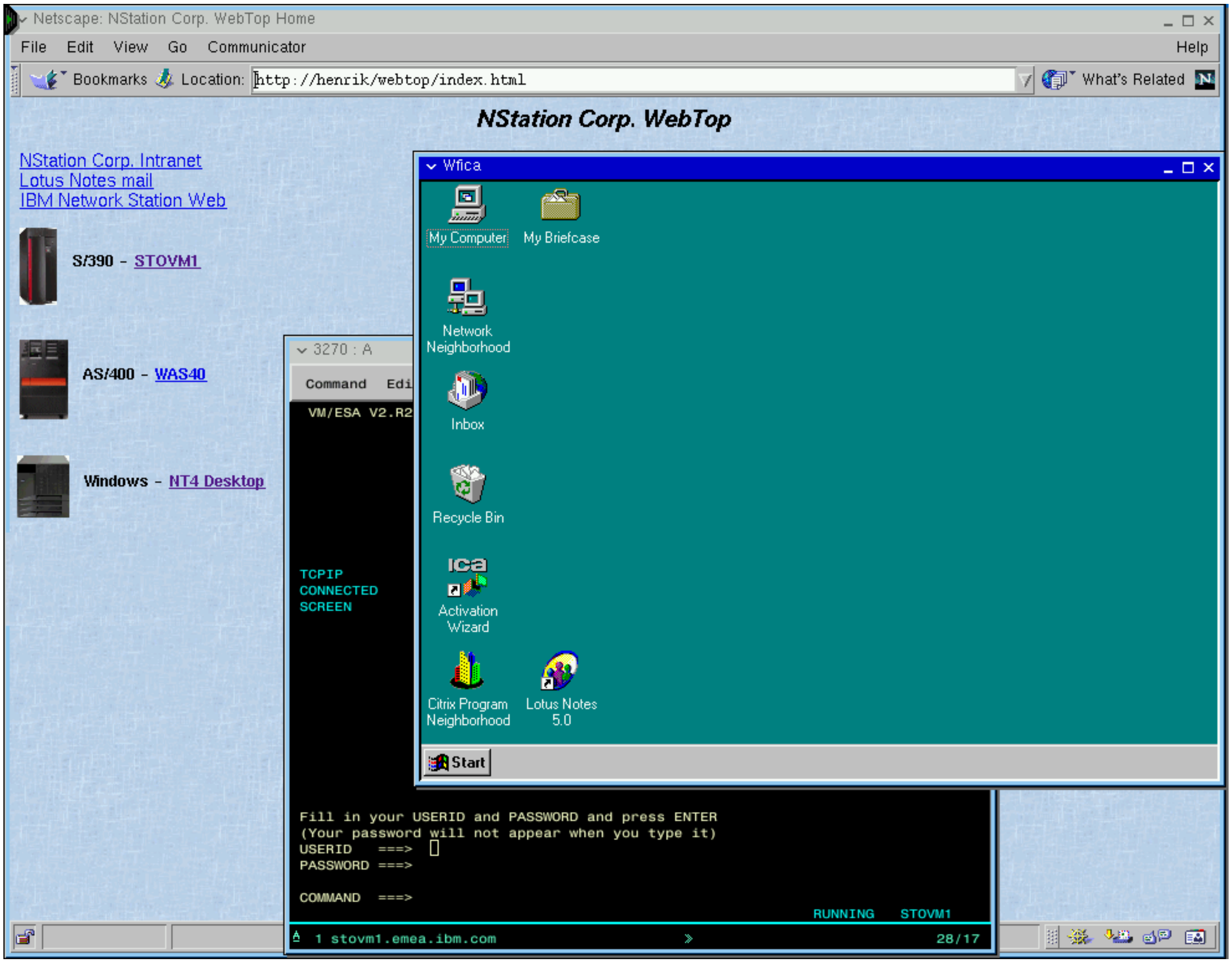
A new window opens with the application.

The netscape.cfg file located in the $ProdBase/<x86|ppc>/usr/local/netscape directory includes statements that determine whether the local launch capability should be enabled, and which applications should be allowed to start. You will see more applications listed than those in Table 55. However, there is currently no support for them. That support may be added in the future.

To allow or deny specific local applications to be launched from the browser, create the /prodbase/<x86|ppc>/usr/local/netscape/overrides.js file and add the following commands to it. True means the application is allowed to start, and false means it is not allowed to start:

```
lockPref( "applications.X-3270","ns3270 %h %o" );
lockPref( "applications.tn3270.active", true );
lockPref( "applications.X-5250", "ns5250 %h %o");
lockPref( "applications.X-5250.active",  true);
lockPref( "applications.X-ICA", "/usr/lib/ICAClient/wfica %o");
lockPref( "applications.X-ICA.active",  true);
lockPref( "applications.X-ICAMgr", "/usr/lib/ICAClient/wfcmgr %o");
lockPref( "applications.X-ICAMgr.active",  true);
```

Change true to false to prevent the applications from being launched. When all applications that should be allowed to be launched have been configured as `active` in the configuration file (this is the default), the HTML file for the desktop should be built. For demonstration purposes, we built a simple desktop with a few icons to illustrate the concept (Figure 321).



```
VM/ESA V2.R2

TCPIP
CONNECTED
SCREEN

Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>
PASSWORD ===>

COMMAND  ===>
                                        RUNNING    STOVM1
1 stovm1.emea.ibm.com                                28/17
```

Figure 321. Sample Web-top

To create our simple Web-top, we used the HTML coding shown in Figure 322.

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
   <meta name="Author" content="Henrik Sjostrand">
   <meta name="GENERATOR" content="Mozilla/4.6 [en] (WinNT; I) [Netscape]">
   <title>NStation Corp. WebTop Home</title>
</head>
<body background="bgbitmap.jpg">

<center><b><i><font face="Arial,Helvetica"><font size=+2>NStation Corp.
WebTop</font></font></i></b></center>

<p><font face="Arial,Helvetica"><font size=+1><a href="http://intranet.nstation.com">NStation Corp.
Intranet</a></font></font>
<br><font face="Arial,Helvetica"><font size=+1><a href="http://notesmail.nstation.com">Lotus Notes
mail</a></font></font>
<br><font face="Arial,Helvetica"><font size=+1><a href="http://www.ibm.com/nc">IBM Network Station
Web</a></font></font>
<p><img SRC="s390.gif" height=62 width=30 align=ABSCENTER><b><font face="Arial,Helvetica">
&nbsp;&nbsp;
S/390 - <a href="X-3270://stovm1.emea.ibm.com">STOVM1</a></font></b>
<p><img SRC="as400.gif" height=64 width=39 align=ABSCENTER><b><font face="Arial,Helvetica">
&nbsp;&nbsp;
AS/400 - <a href="X-5250://was40.got.se.ibm.com">WAS40</a></font></b>
<p><img SRC="netfinity.gif" height=50 width=42 align=ABSCENTER><b><font face="Arial,Helvetica">
&nbsp;&nbsp;
Windows - <a href="X-ICA://9.24.104.159">NT4 Desktop</a></font></b>
<br>&nbsp;
</body>
</html>
```

Figure 322. HTML file for sample Web-top

The key HTML tags in this file are those that launch the Network Station's local applications. In Table 55 on page 366, the Application URL column lists the tags that can be used in the HTML file. For example, the `<a href="X-3270://stovm1.emea.ibm.com">S/390 - STOVM1</a>` tag is used to launch the 3270 emulator against the stovm1.emea.ibm.com mainframe. The `<a href="X-ICA://9.24.104.159">Windows - NT4 Desktop</a>` tag is used to launch an ICA session against the NT/TSE-Metaframe server 9.24.104.159.

Using this technique, more advanced Web-tops can be built, but that HTML coding is well beyond the scope of this redbook.

Tip

Configure the Web-top HTML page to be the browser's startup and home page. Users can then simply click the Home button to return to their corporate application menu.

Note

Since only the NSM V2R1 Netscape Communicator supports the special URL types we use (X-3270, X-5250, X-ICAetc.), a Web-top HTML page built with them will only work on the Network Station.

Chapter 13. Emulators

NSM V2R1 provides the following emulator functions:

- 3270 emulation to provide access to System/390 systems
- 5250 emulation to provide access to AS/400 systems
- VT emulation to provide access to UNIX systems and the Digital VAX/VMS environment

IBM SecureWay Host On-Demand

The IBM SecureWay Host On-Demand version 4.0.1 announces support for the IBM Network Station series 2200 and 2800 with NSM V2R1. Due to the product architecture of the Network Station, IBM does not support the use of the Host On-Demand Cached Client with the Network Station.

SecureWay Host On-Demand offers secure access to host applications and data via the Network Station Navigator browser. A click on the hyperlink launches the Host On-Demand Java applet that supports secure, scalable, and reliable access, with S/390 (TN3270), AS/400 (TN5250), and DEC/UNIX (VT52/100/220) emulation in a single package. CICS Gateway for Java access is also provided. Users may access any number of host sessions and still use their browser for other tasks. A default graphical user interface is provided for users unfamiliar with traditional host screens.

Complete Host On-Demand product information can be accessed at:
`http://www.ibm.com/software/network/hostondemand/`

The VT, 3270, and 5250 emulators provide terminal emulation access to host systems. Users enter the IP address or host name of the UNIX, S/390, or AS/400 system (if not pre-configured in NSM), and the emulator provides a terminal window interface. The emulators have many features including:

- Customized pull-down menu, which can be controlled within the Network Station Manager configuration panels.
- A status Operator Information Area (OIA) line with Shift/Caps indicators, input inhibited indicators, and cursor position.
- Screen print capability to PostScript, PCL, and ASCII printers.
- 3270 and 5250 Record/Playback capability, including auto-logon. Any key (defined in the keyboard remapping) can now start a playback file.
- Copy/Cut/Paste using the Edit menu (linear and rectangular copy/paste are available).
- 3270 and 5250 pop-up and pull-down keypads that can be customized by the user.
- Color-mapping program for 3270 and 5250 emulator sessions, giving you the ability to change the colors in the session. Some color changes are available for VT sessions.
- Miscellaneous preferences can be set to define many emulator attributes such as cursor style, rule line, and audio alarm.

- 5250 display and print (PCL and PostScript) of monochrome image and fax (3489 emulation).
- With the 16-bit color image support, extended baseline JPEG image types, TIF color and PCX color image formats are now supported.
- Keyboard remapping files can be named to allow the administrator to set up multiple default keyboard remapping files for different users.
- Advanced keyboard mapping is available for 3270 light pen emulation.

New in V2R1, you will find the following enhancements:

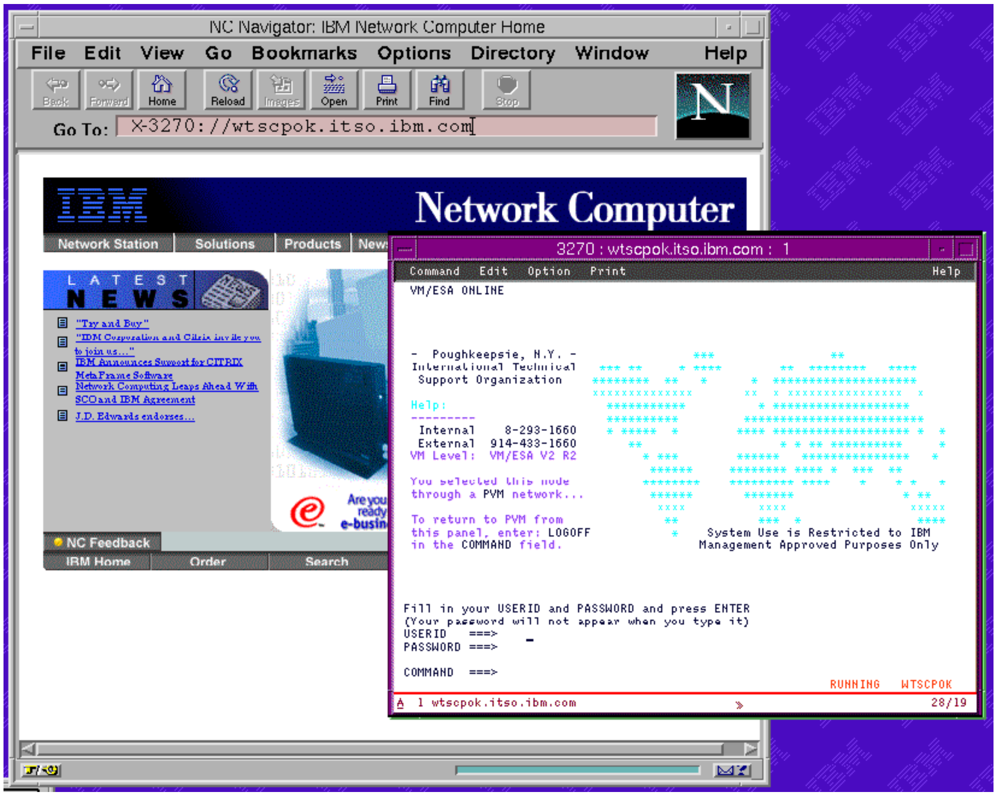
- Scalable fonts for 3270 and 5250 emulation for better full-screen coverage
- Anti-aliasing support with 16-bit color
- Integration of R3 PTFs
- SSL version 3 Telnet support for secure 3270 and 5250 host session access via the Internet, including password and user ID encryption
- Session jump keys can be defined in the keyboard remapper for 3270 and 5250 sessions
- New VT emulator, supporting XTERM, ANSI, VT100, VT102, VT200, VT220, VT300, and VT320
- GUI-based keyboard remapping for VT emulator sessions
- Ability to edit and restore playback files
- Ability to automatically use the TCP/IP host name as the 3270 or 5250 session name
- Printer Definition Table (PDT) support for 5250 and 3270 emulation

Many of these settings and their availability to the user can be controlled through NSM.

In addition to starting 5250 and 3270 sessions through the Host Access Folder on your desktop, these emulators may also be launched from within the browser by entering either of these URLs:

```
X-5250://hostname
X-3270://hostname
```

Here, `hostname` is the IP address or name of your host. For example, as shown in Figure 323, to launch a 3270, session we entered a URL of `X-3270://wtscpok.itso.ibm.com`. We were also able to start a 5250 session by entering a URL of `X-5250://10.1.1.1`. The browser can also launch a Telnet session by specifying a URL of `telnet://host`


NC Navigator: IBM Network Computer Home
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Go To:
IBM Network Computer
Network Station Solutions Products News
LATEST NEWS
"Try and Buy"
"IBM Corporation and Citrix invite you to join us..."
IBM Announces Support for CITRIX MetaFrame Software
Network Computing Leaps Ahead With SCO and IBM Agreement
J.D. Edwards endorses...
Are you ready e-busin
NC Feedback
IBM Home Order Search
3270 : wtscpok.itso.ibm.com : 1
Command Edit Option Print Help

```
X-3270://wtscpok.itso.ibm.com
```

```
VM/ESA ONLINE


 -  Poughkeepsie, N.Y. -
 International Technical
  Support Organization

 Help:
 ----------
  Internal    8-293-1660
  External  914-433-1660
 VM Level:  VM/ESA V2 R2

 You selected this node
 through a PVM network...

 To return to PVM from
 this panel, enter: LOGOFF
 in the COMMAND field.
                                          System Use is Restricted to IBM
                                         Management Approved Purposes Only


Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>
PASSWORD ===>

COMMAND  ===>
                                                             RUNNING   WTSCPOK
A  1 wtscpok.itso.ibm.com                    »                          28/19
```

Figure 323. Launching a 3270 emulation from Netscape

13.1 VT emulator

NSM V2R1 includes a completely new VT emulator. This emulator is based on the dtterm emulator from IBM AIX. It supports XTERM, ANSI, VT100, VT102, VT200, VT220, VT300, and VT320.

When adding a VT emulator icon to the launch bar, you choose one of the terminal types to emulate. If a UNIX program is written using the “curses” API library, then it really should not matter which emulation you choose. The curses library provides a set of functions that enable the program to manipulate a terminal's display regardless of the terminal type. When you use a program written to the curses API, the runtime library will match the keys to the program calls. However, there may be problems if the UNIX program was not written to the curses API and has hardcoded function key and keypad key definitions. In this case, you need to choose the correct emulator so the keys map to what the program expects:

XTERM This maps to what the standard UNIX “xterm” program expects. It is usually similar to VT100, but a bit different. In general, the UNIX definitions of what it expects are stored in terminfo files (some systems use termcap files). In AIX, the definitions for terminals are in /usr/lib/terminfo. The XTERM program usually has 10 function keys defined and doesn't use shifted values. This emulation doesn't support color (from UNIX definitions), but it still has color if you use the escape sequence.

ANSI This is usually based on early PC emulators that did almost nothing. Rather than being a standard, many manufacturers chose their own definitions. Often customers expect “SCO ANSI” when they say ANSI. The function keys are a little different than either XTERM or VT emulators. The one thing that people often expect with this emulation is the use of an IBM850 codepage to give PC-type line drawing characters. To use PC-type line drawing characters, a font server on the UNIX host is needed, and the emulator must be started with the “-fn FONT” flag. FONT is the font metric or alias for an IBM-850 or PC-427 codepage font on the font server.

VT100 This terminal only had four function keys defined, but also had some special keys including a GOLD key, which was really a "dead" key that changed the value of the next key pressed. This function is not widely used, but we have some customers who may want this. Many VT100 emulators support more than four function keys.

VT200-VT320 These terminals all have the same function key sequences and often don't use the F5 key as a function F5, but give it special meaning. There are also keys defined as khelp, kdo, and other special escape sequences. There are both 7-bit (usually used in the US), and 8-bit versions of these terminals and emulation. You need 8 bits to support European characters such as the French Franc and the British Sterling symbol input.

13.2 Settings for emulator sessions

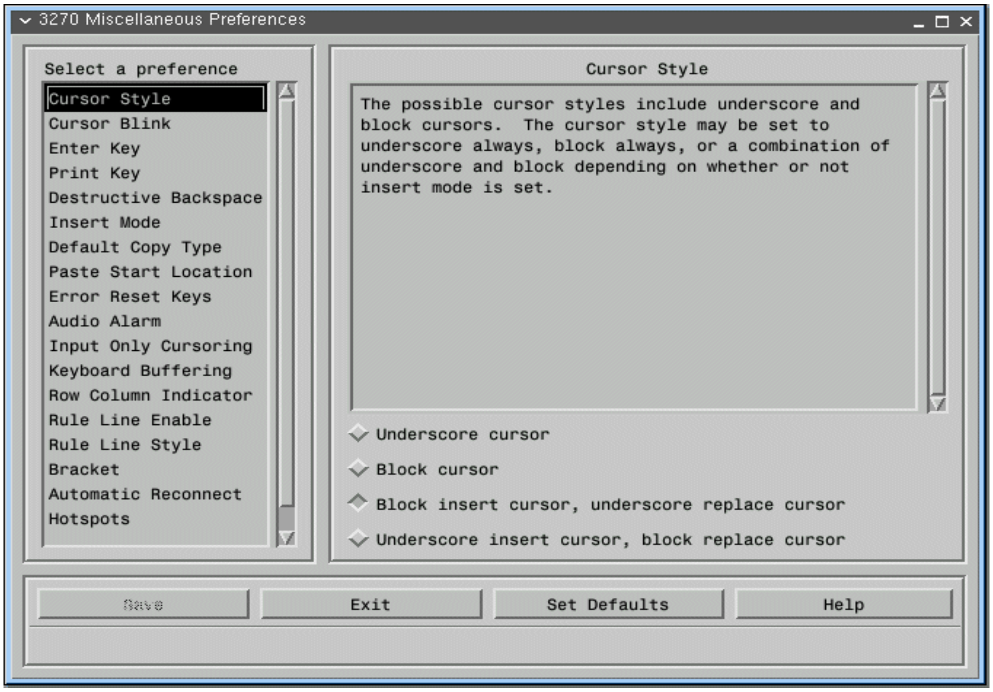
The NSM administrator and Network Station user can define parameters to customize their sessions. There are four ways to define parameters for emulator sessions:

- **Miscellaneous preferences option:** The user can set miscellaneous preferences from the option pull-down of the emulator window.
- **Application menu settings:** Settings for all sessions at the system, user, or group level can be set in the application menu. The parameters have pull-down menus to choose the appropriate setting. The majority of these settings are only available to the NSM administrator. However, a few can be modified by the user through NSM.
- **NSM application settings Additional parameters field:** The NSM administrator can set parameters that apply to all sessions by adding them to the Additional parameters field. These set default miscellaneous preferences for the users and other preferences.
- **Launch Bar Other parameters field:** The NSM administrator can set parameters that apply to a particular Launch Bar item by adding them to the Other parameters field.

Preferences can be set for emulation at the system, group, or user level using NSM. Individual users can override these settings using miscellaneous preferences.

13.2.1 Using the miscellaneous preferences

Users can override preferences set by the NSM administrator by using the miscellaneous preference options in the emulator window (Figure 324). Preferences set this way are true for all sessions of that type started for that user. They override all other options set for this user.



The possible cursor styles include underscore and block cursors. The cursor style may be set to underscore always, block always, or a combination of underscore and block depending on whether or not insert mode is set.

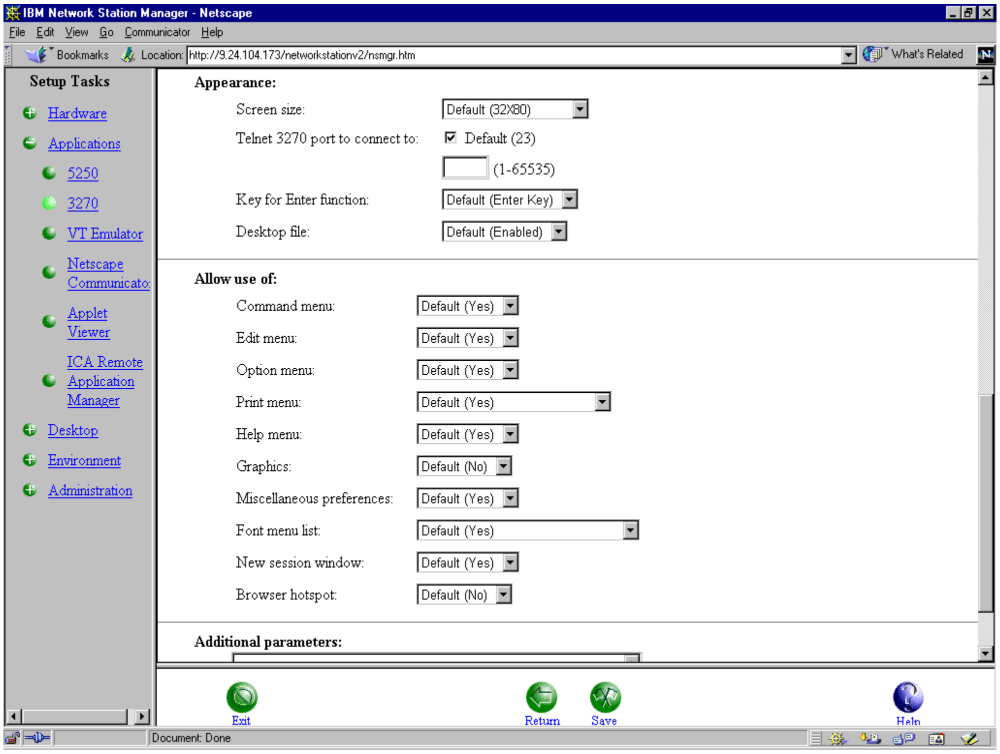
Figure 324. Miscellaneous preferences

Each option can be highlighted and a value chosen from the list that is presented.

Note: The NSM administrator has control over whether the user sees the miscellaneous preference option by setting a field in the NSM application settings for the emulator.

13.2.2 Setting NSM application settings

The NSM administrator can set a variety of options for the emulator sessions at the system, group, or user level. Many of these fields determine what menu bar items are available to the user. For example, the administrator can prevent the user from changing fonts, using the record/playback feature, and so on. Figure 325 on page 374 shows an example of 3270 application settings.


IBM Network Station Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://9.24.104.173/networkstationv2/nsmgr.htm
What's Related
Setup Tasks
Hardware
Applications
5250
3270
VT Emulator
Netscape Communicator
Applet Viewer
ICA Remote Application Manager
Desktop
Environment
Administration
Exit
Return
Save
Help
Document: Done

Appearance:

Screen size: Default (32X80)

Telnet 3270 port to connect to: ☑ Default (23)

(1-65535)

Key for Enter function: Default (Enter Key)

Desktop file: Default (Enabled)

Allow use of:

Command menu: Default (Yes)

Edit menu: Default (Yes)

Option menu: Default (Yes)

Print menu: Default (Yes)

Help menu: Default (Yes)

Graphics: Default (No)

Miscellaneous preferences: Default (Yes)

Font menu list: Default (Yes)

New session window: Default (Yes)

Browser hotspot: Default (No)

Additional parameters:

Figure 325. 3270 application settings

Note: Setting the Miscellaneous preferences field to yes, as shown in Figure 325, allows the user to override these options using the Miscellaneous Preferences option in the emulator window.

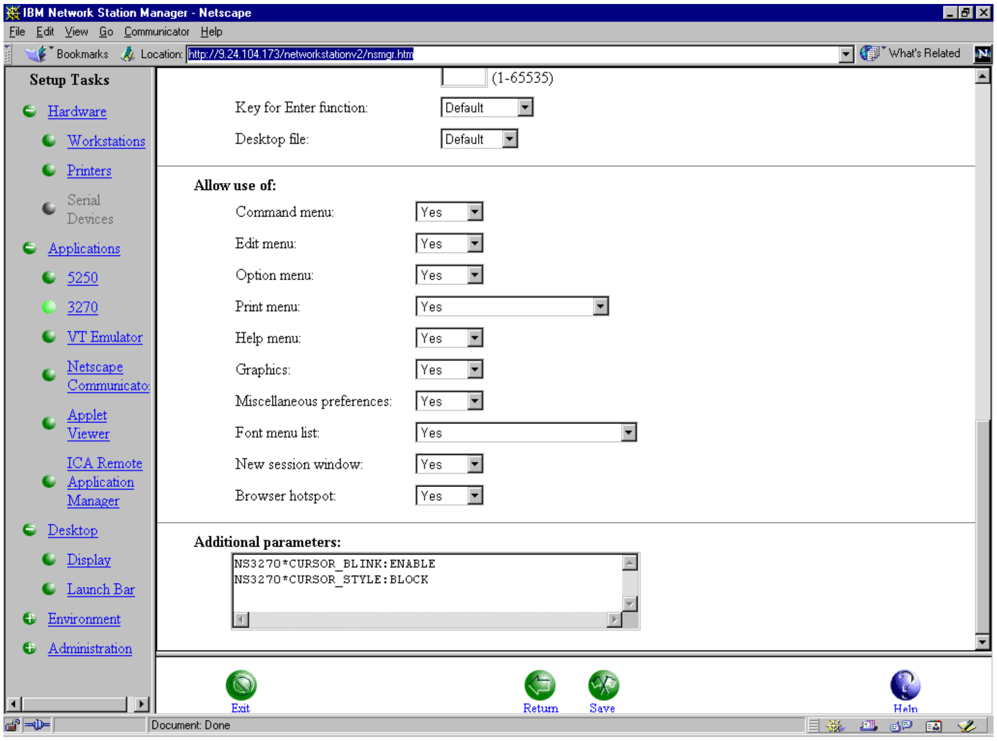
The Network Station user also has access to a small subset of these options through NSM. For the 3270 emulator, the user can modify the screen size, the key for the enter function, the availability of graphics, and whether the edit menu is available.

For 5250 emulator sessions, the user can modify the screen size, enable or disable column separators, and determine the availability of the edit menu and control menu.

For the VTxxx emulator, the user can only change the option to enable or disable the edit menu (for copy, paste, and cut).

13.2.3 Using the Additional parameters field

The last field in the NSM application settings window allows the administrator to add additional parameters affecting the emulator session. Many of these parameters affect the same functions as the user miscellaneous preference settings and are used to set the defaults for these settings. There are additional settings that can be made with these parameters that are not available to the user in the miscellaneous preferences (Figure 326).



(1-65535)

Key for Enter function: Default

Desktop file: Default

Allow use of:

Command menu: Yes

Edit menu: Yes

Option menu: Yes

Print menu: Yes

Help menu: Yes

Graphics: Yes

Miscellaneous preferences: Yes

Font menu list: Yes

New session window: Yes

Browser hotspot: Yes

Additional parameters:

```
NS3270*CURSOR_BLINK:ENABLE
NS3270*CURSOR_STYLE:BLOCK
```

Figure 326. 3270 Application Additional parameters

The format of the Additional parameters field is:

```
NS3270*CURSOR_STYLE:BLOCK
```

NS3270 is the 3270 program name, followed by a “*”, the parameter name, a “:”, and the parameter value. The command model is similar for 5250 and VT sessions, except that the line starts with NS5250 and NSTerm, respectively. Each parameter is entered on a separate line.

If a miscellaneous preferences file exists for a user, the Additional parameters values are not used for any preferences that also exist in the miscellaneous preferences. In other words, if the user sets any setting in the Miscellaneous preference panel, all other settings available the miscellaneous preferences are taken as defaults, regardless of any settings the administrator has made in the additional parameter field. If the user sets miscellaneous preferences to Set Defaults, the miscellaneous file is erased and the additional parameter values are used.

For example, the default for the cursor in a 3270 emulation session (no additional parameters or miscellaneous preferences set) is that the cursor does not blink.

Table 56 shows you the affect of using the miscellaneous options and additional parameters.

Table 56. Effect of using additional parameters on emulation sessions

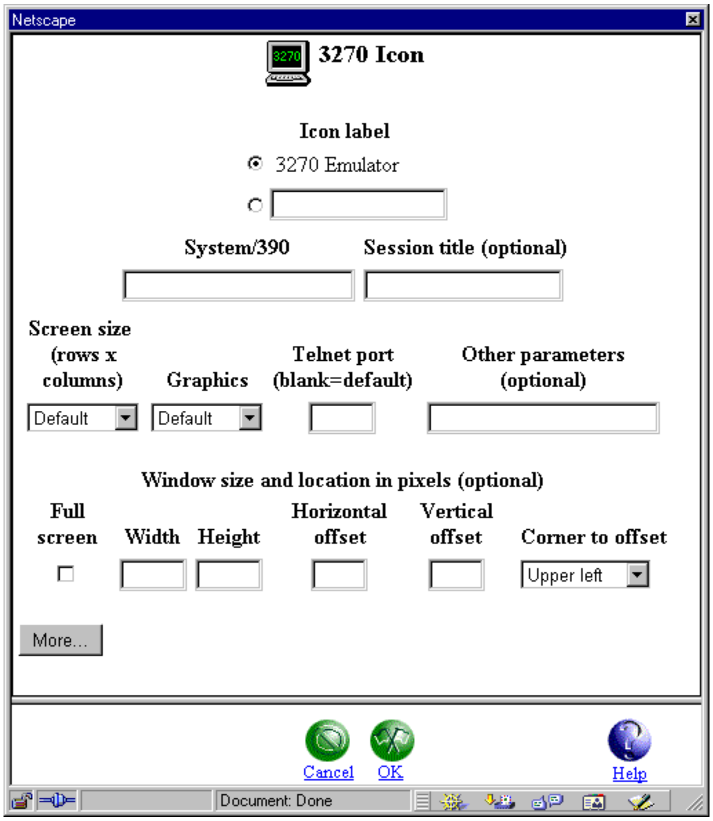
	Miscellaneous preferences set?	**Additional parameter field**	**Will the cursor blink?**	**Session title**
No action has been taken by the user or the administrator to change the 3270 preferences.	No	No	No	default
The administrator changes the default for all users to make the cursor blink.	No	CURSOR_BLINK:ENABLE	Yes	default
The user decides to change the cursor style to block by using the miscellaneous preferences, and thus creating a miscellaneous file.	Sets cursor style to block. (The user does not change any other settings. But looking at the default for cursor blink in the miscellaneous preferences, they can see it is set to enable)	CURSOR_BLINK:ENABLE	Yes (because miscellaneous preferences exist and set the cursor to blink)	default
The administrator decides to disable the cursor blink feature for all users.	Cursor style is still set to block and all other miscellaneous preference defaults apply	CURSOR_BLINK:DISABLE	Yes (because miscellaneous preferences exist and set the cursor to blink)	default
The administrator decides to give the 3270 sessions a meaningful title	Cursor style is still set to block and all other miscellaneous preference defaults apply	CURSOR_BLINK: DISABLE SESSION_TITLE: HOSTA+99	Yes (because miscellaneous preferences exist and set the cursor to blink)	HOSTA1 There is no corresponding miscellaneous preference so this value is picked up from the additional parameters.

Note: This is not currently a concern for VT emulator sessions since they have no settings common to both miscellaneous preferences and additional parameters.

Help text is available for the parameters by clicking on Help in the Network Station emulator window.

13.2.4 Setting the Launch Bar parameters

Settings for sessions started from a particular icon on the launch bar can be set by editing the NSM application from the Launch Bar Content window (Figure 327). A few settings are available for emulator sessions.



Icon label
● 3270 Emulator
○

System/390

Session title (optional)

Screen size (rows x columns): Default

Graphics: Default

Telnet port (blank=default)

Other parameters (optional)

Window size and location in pixels (optional)

Full screen □

Width

Height

Horizontal offset

Vertical offset

Corner to offset: Upper left

Figure 327. 3270 Launch Bar settings

The parameters you can set for emulator sessions on the NSM Launch Bar window are:

- Icon label
- TN3270 server, 5250, or VT remote host
- VT terminal type
- Screen size
- Session title
- TN3270 Telnet port
- 3270 graphics
- 5250 image/fax display
- Window size and location
- Minimum memory needed to start the application (More... button)
- Application priority when memory is low (More... button)
- Whether to restrict the application to a single window (More... button)

The Other parameters field allows the administrator to enter special parameters, including LU printer information, SSL, LU display name, and language.

13.2.5 Preference settings

Preferences (application and launch bar settings) set by the user or administrator for the user using NSM are stored in a profile under the user's name.

Windows NT servers

Preferences set at the *system level* using NSM are stored in $UserBase/profiles/allusers.nsm.

Preferences set at the *group level* using NSM are stored in $UserBase/profiles/groups/*groupname*.nsm*.*

Preferences set at the *user level* using NSM are stored in $UserBase/profiles/users/*userid*.nsm.

Preferences set by the user using the Miscellaneous preferences option in the emulator window are stored in:

- $UserBase/nsmshared/*userid*/Ns3270/Miscellaneous
- $UserBase/\nsmshared/*userid*/Ns5250/Miscellaneous
- $UserBase/nsmshared/*userid*/Nsterm/Miscellaneous

Note: While you can edit these files (with the exception of the miscellaneous file), you should only update them by using NSM. The file names are provided here for your information and diagnostic purposes only.

13.2.5.1 3270 and 5250 settings

Table 57 shows the various types of settings that can be made for a 3270 and 5250 emulator session in addition to those shown on the NSM graphical interface (launch bar and applications settings). For information on the possible values, see the online help in NSM and in the emulator sessions in the Network Station.

Table 57. Additional 3270 and 5250 emulator session preferences

Type of setting	3270/5250 Miscellaneous preferences	NSM 3270/5250 Application menu or additional parameters	NSM 3270/5250 Launch Bar “Other Parameters”
Cursor style	Yes	CURSOR_STYLE	
Cursor blink	Yes	CURSOR_BLINK	
Enter, new line, field exit (5250) key	Yes	ENTER_KEY (5250). menu (3270)	
Print key	Yes	PRINT_KEY	
Destructive Backspace	Yes	DESTRUCTIVE_BACKSPACE	
Insert mode	Yes	INSERT_MODE	
Default copy type	yes	DEFAULT_COPY_TYPE	
Paste start location	yes	PASTE_LOCATION	
Automatic help (5250 only)	yes	AUTOMATIC_HELP	
Error reset keys	yes	ERROR_RESET_KEYS	
Audio alarm	yes	AUDIO_ALARM	
Input only cursoring	yes	INPUT_ONLY_CURSOR_MOVE MENT	

Type of setting	3270/5250 Miscellaneous preferences	NSM 3270/5250 Application menu or additional parameters	NSM 3270/5250 Launch Bar “Other Parameters”
Keyboard buffering	yes	KEYBOARD_ BUFFERING	
Large-screen behavior (5250 only)	yes	LARGE_SCREEN_ BEHAVIOR	
Row column indicator	yes	ROW_COLUMN_ INDICATOR	
Rule line enable	yes	RULE_LINE	
Rule line style	yes	RULE_LINE_STYLE	
Blue underscore (5250 only)	yes	BLUE_UNDERSCORE	
Bracket (3270 only)	yes	BRACKET	
Automatic reconnect (3270 only)	yes	AUTOMATIC_ RECONNECT	
Hotspots	yes	HOTSPOTS	
Hotspot highlighting	yes	HOTSPOT_ HIGHLIGHTING	
Window title		TITLE_OPTION	
Session ID		SESSION_ID	
Maximum sessions		MAX_SESSIONS	
Host display name		DISPLAY_NAME	-DISPLAY_NAME
Retry communication errors		RETRY_COUNT	
Retry interval		RETRY_INTERVAL	
Timeout session		INACTIVITY_TIMEOUT	
Euro symbol		EURO	
Fixed versus standard fonts		FONTS_TO_USE	
Keyboard buffering delay (3270 only)		KEY_BUFFERING_ DELAY	
Playback delay		PLAYBACK_DELAY	
Language			-LANGID
Telnet port			-port
SSL			-SSL
Printer (3270 only)			-PRINTER_ GENERAL
Printer LU name (3270 only)			-PRINTER_NAME
Play a recorded file		menu	-playback

Type of setting	3270/5250 Miscellaneous preferences	NSM 3270/5250 Application menu or additional parameters	NSM 3270/5250 Launch Bar “Other Parameters”
Use the PDT table (PDT.819)			-PDT
Keyboard map file		menu	-KEYFILE
Keypad file		menu	-KEYPAD

13.2.5.2 VT settings

Table 58 shows the various types of settings that can be made for VT emulator sessions in addition to those shown on the NSM graphical interface (launch bar and applications settings). For information on the possible values, see the online help in NSM and in the emulator sessions in the Network Station.

Table 58. Additional VT emulator session preferences

Type of setting	VT Miscellaneou s preferences	VT Application menu or Additional parameters setting	Launch Bar “other Parameters”
Cursor style (block/underscore)	yes		
Cursor blink	yes		
Application cursor mode: application or cursor - When in application mode, ANSI escape sequences are generated rather than standard cursor movements when the arrow keys are used.	yes		
Application keypad mode: application or numeric - When in application mode, control functions are generated rather than numeric characters when the keypad is used.	yes		
Auto line feed	yes		
Auto wrap around	yes		-aw (yes) * +aw (no)
Visible status line	yes		
Iconified state		iconic	
Name to display beneath the VT emulator icon		iconName	
De-iconify (map) upon output from application		mapOnOutput	
Reverse foreground/background colors		reversevideo	
* Overrides miscellaneous preference settings ** Overrides application settings			

Type of setting	VT Miscellaneous preferences	VT Application menu or Additional parameters setting	Launch Bar "other Parameters"
File name for debug log		logFile	
Recognize/Ignores the DECCOLM sequence (to switch between 80- and 132-column mode)		c132	-132 (yes) +132 (no)
Border color			-bd (color)
Application window background color		background	-bg (color)
Width (in pixels) of the border surrounding the windows.			-bw(borderwidth)
Text cursor color		cursorColor	-cr (color)
Specifies whether 8-bit characters should be emitted from function and keypad sequences. Default is false. Note: -ebe is the opposite of +ebe; -ebe is 8-bit characters whereas +ebe is 7-bit characters		menu (eightBitEmit)	-ebe** +ebe
Specifies whether 8-bit characters should be accepted.		menu (eightBitInput)	-ebi **
Use/do not use euro currency symbol			-euro (use) +euro (don't use)
Text color		foreground	-fg
Use/do not use jump scrolling, which moves multiple lines at a time instead of one line at a time.	yes		-j (use) * +j (don't use)
Specifies that you use your own customized key mapping. This overrides any Network Station specified value.		menu	-KEYFILE **
Run/do not run the debug log			-l (run) +l (don't run)
Specifies that if your window has been minimized, and data is being written to that window, the window will return to an active state.			-map
Specifies that if your window has been minimized, and data is being written to that window, the window remains in an minimized state. This is the default.			+map

* Overrides miscellaneous preference settings
** Overrides application settings

Type of setting	VT Miscellaneous preferences	VT Application menu or Additional parameters setting	Launch Bar “other Parameters”
Enable/disable margin bell when the user types near the right end of a line. This overrides any values specified in Miscellaneous preferences.	yes		-mb (enable) * +mb (disable)
Specifies the color of the pointer.		pointerColor	-ms (color)
Specifies the text which will appear under the icon when Terminal is minimized.			-n (icon title)
Specifies the number of characters from the right end of a line at which the margin bell, if enabled, rings. The default is 10. This overrides any values specified in Miscellaneous preferences.	yes		-nb (number) *
Specifies the port number to use for this connection. The default is 23.			-port
Specifies that Terminal starts in reverse video.			-rv
Enable/disable reverse wraparound, which permits backspacing of the cursor from the left-most column of one line to the right-most column of the previous line. This overrides any values specified in Miscellaneous preferences.	yes		-rw (enable) +rw (disable) *
Display/don’t display a scrollbar. This is the default and overrides the NSM program.		menu	-sb (display) ** +sb (no)
Specifies that a visual bell not be used instead of an audible bell. This overrides any values specified in Miscellaneous preferences.	yes		+vb *
Specifies that a resource string be used for a specific instance of terminal.			-xrm (resourcestring)
* Overrides miscellaneous preference settings ** Overrides application settings			

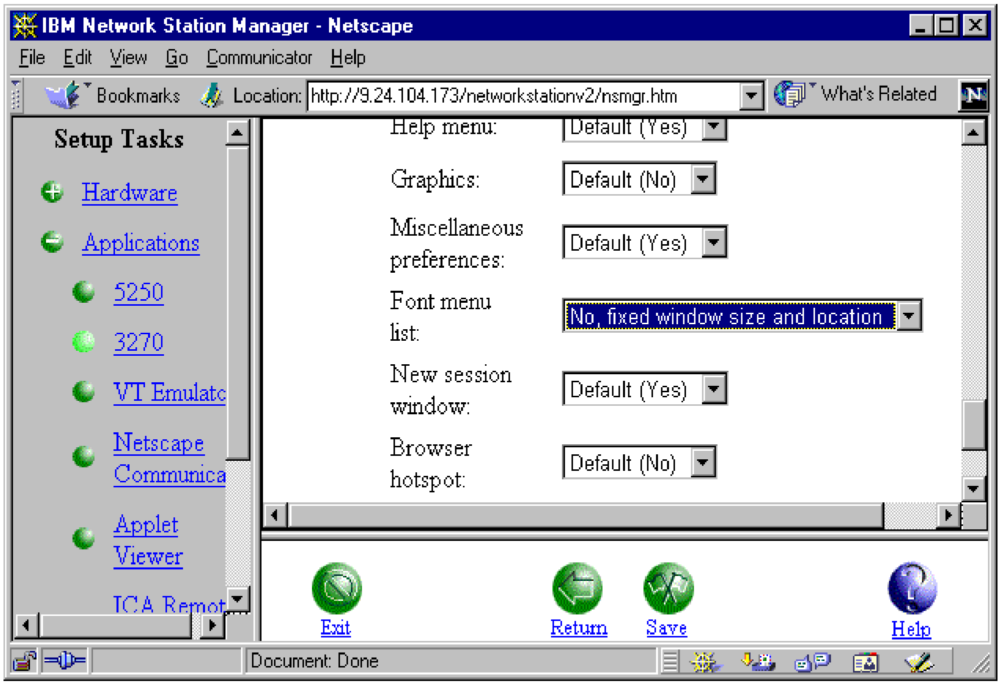
Note

Settings for the VT emulator made in the Other parameters field override comparable miscellaneous preference settings made by the user. The user can change the settings by altering the miscellaneous preferences, but the change is temporary. Once the session is restarted, the settings from the Other parameters field take affect once again.

13.3 Scalable fonts for 3270 and 5250 sessions

Network Station Manager V1R3 used fixed font sizes, but V2R1 provides a set of bitstream scalable fonts for 3270 and 5250 emulator windows. These fonts give an improved full-screen coverage, filling nearly all of the available window area.

The administrator can change the ability of the 3270 and 5250 emulators to use the scalable fonts by through the application settings in NSM (Figure 328).



IBM Network Station Manager - Netscape

Location: http://9.24.104.173/networkstationv2/nsmgr.htm

Help menu: Default (Yes)

Graphics: Default (No)

Miscellaneous preferences: Default (Yes)

Font menu list: No, fixed window size and location

New session window: Default (Yes)

Browser hotspot: Default (No)

Document: Done

Figure 328. Choosing 3270 emulator font options

The options are shown in Table 59.

Table 59. Font menu list options

Font Option	Meaning
Default (Yes) or Yes	Scalable fonts are used. The font size changes with the window size automatically. The user will have the font menu available.
No	The user will not have the font option. Scalable fonts are still used and change automatically with the window size, but the user does not have the option of changing the fonts from the window.

Font Option	Meaning
No, fixed window size and location	The window size and location are fixed. The user cannot drag it to a new location or resize it. The font cannot be changed.
Fixed fonts only	The window size can change and the window can be moved, but the same font is always used.

The user can change the font size by selecting **Option->Fonts** from the menu bar in the emulator window or resizing the 3270 session window by dragging the 3270 window borders or window corners (using the mouse). Changing the window size affects the font shown and the fonts available from the font Option menu.

13.4 Anti-aliasing

When anti-aliasing is turned on (enabled), it allows the network station to draw characters with certain types of scalable fonts that are much smoother in appearance than can be obtained with those fonts when anti-aliasing is turned off. Anti-aliasing is not really a 3270/5250-specific feature. Only those clients or operating system components using specific types of fonts for which the operating system can do anti-aliasing are affected by this. The 5250, 3270, and VTxxx emulators specifically use these types of fonts as their default fonts, and so will likely be affected by whether this gets set. This has no effect for most other client applications.

Anti-aliasing can be enabled or disabled for workstations. Using NSM at the system level, the option is under the Workstation item under the Hardware setup task.

The ability to perform anti-aliasing may be restricted by factors other than the NSM setting. Anti-aliasing cannot be done if the network station is not 16-bit color capable. Therefore, as an example, Model 300s will not be anti-alias capable.

A possible reason for disabling anti-aliasing may be for situations in which there are performance concerns with the display of data. As a general rule, handling the anti-aliasing function is more compute intensive within the Network Station's operating system. Having anti-aliasing on may affect performance.

13.5 Requesting a specific TN3270 or TN5250 session LU name

There is often the situation where an administrator wants to control the host connection down to the LU level. This may happen when a user needs a particular logmode or automatic connection to a particular host program. One of the capabilities of TN3270E and TN5250 is to allow the user to specify an LU (or LU pool name in the 3270 environment), to control SNA connectivity at the LU level. The administrator can control this by adding the -DISPLAY_NAME parameter to the 3270 or 5250 session parameters.

13.5.1 3270 display naming

Figure 329 shows an example of controlling the 3270 emulation connection at the LU level.

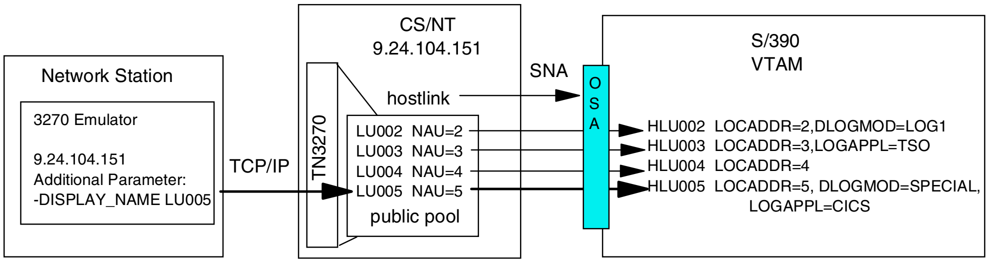


Figure 329. TN3270E connection

In Figure 329, the Network Station uses a Windows NT machine running IBM eNetwork Communications server for Windows NT (CS/NT) as a TN3270 server. The CS/NT server has a host connection to the System/390. The network station starts an emulation session, specifying the IP address of the CS/NT server and the display name of the LU defined in CS/NT to which to be connected. The session between the Network Station and CS/NT uses TCP/IP.

The CS/NT server takes that request, allocates the requested LU name defined to CS/NT for the session (LU005), and requests a connection to the host using the network addressable unit (NAU) defined for that LU. The host allocates an LU with the same NAU (5) to the session.

The SNA characteristics associated with the host LU (HLU005) are now used for the session, including the logmode (SPECIAL), the application to automatically connect to (CICS), or any other specification. The session between CS/NT and the host is an SNA connection.

Another example is shown in Figure 330.

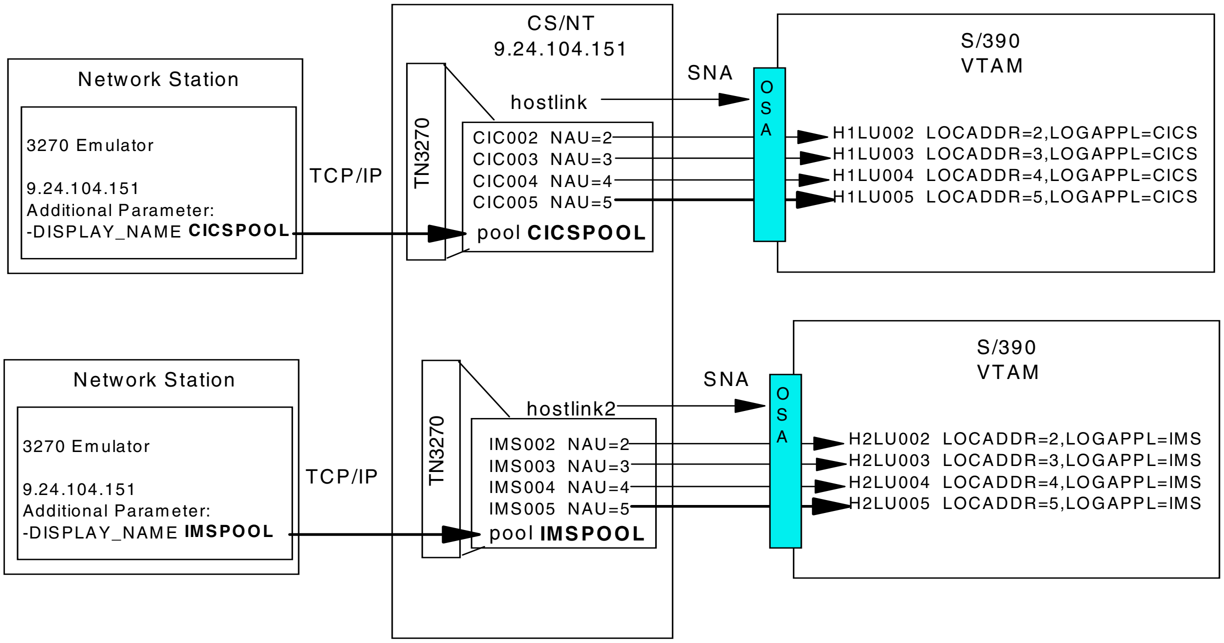


Figure 330. TN3270 connection example

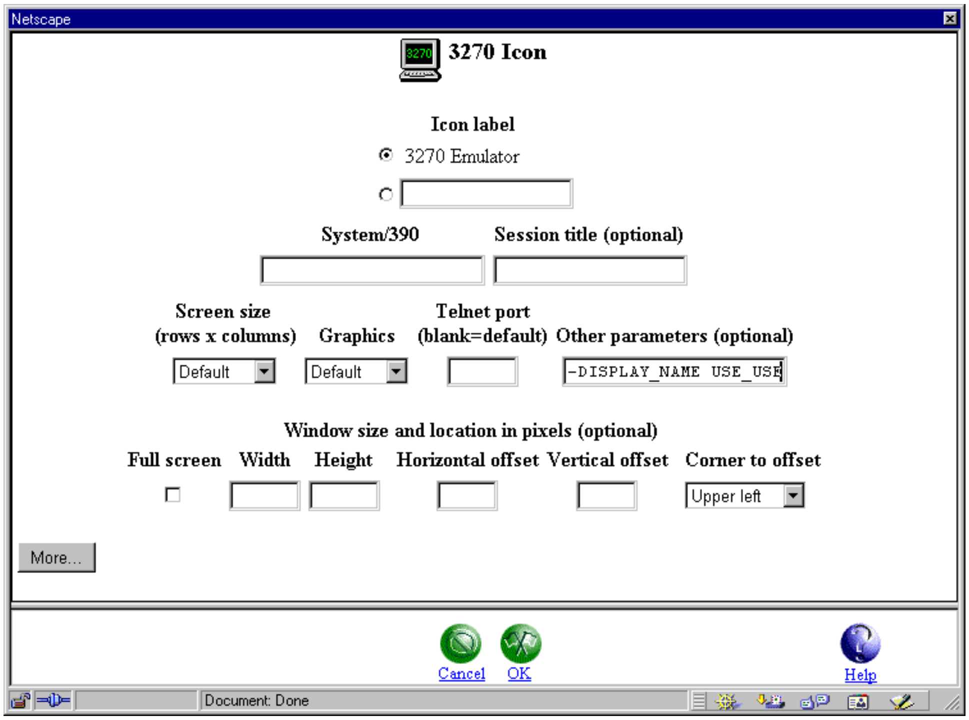
In the example in Figure 330 on page 385, some Network Station users require a connection to CICS and others to IMS. The CS/NT server is set up with a link to two hosts: one with CICS and the other with IMS. The LUs belonging to each link are grouped into pools. The NSM administrator can assign the CICS users a 3270 emulation session with the pool name for the CICS pools (CICSPOOL) in the -DISPLAY_NAME parameter. Similarly, the IMS users will have a 3270 emulation session with the IMS pool name (IMSPOOL) in the -DISPLAY_NAME parameter. The connection to CS/NT for each user will be routed to the appropriate pool, and thus, the appropriate host, host LU, and finally the correct application.

13.5.2 5250 display naming

In the AS/400 environment, there may be a need to have static or defined display names. For example, there may be applications on the AS/400 system that rely on specific display names to supply the correct menu screens to the user, so the default QPADEVxxxx names are not usable. Alternatively, the use of display names may be desired by operations or help desk personnel since interactive user jobs would be listed in easily identified terms such as user ID. The way in which specific 5250 (and 3270) display names can be assigned and the associated rules are described in the following sections.

13.5.3 Defining the display name using NSM

To define the 3270 display name in NSM, click **Desktop->Launch Bar**. Select **3270 Emulator** the in Launch Bar Content list box. Click **Edit** on the right of the Launch Bar Content to open the 3270 Icon window (see Figure 331). Enter `-DISPLAY_NAME`, one space, and one parameter (the parameter is described on following sections) in the Other parameters field.



Netscape

3270 Icon

Icon label

● 3270 Emulator

○

System/390

Session title (optional)

Screen size (rows x columns): Default

Graphics: Default

Telnet port (blank=default):

Other parameters (optional): -DISPLAY_NAME USE_USE

Window size and location in pixels (optional)

Full screen □

Width

Height

Horizontal offset

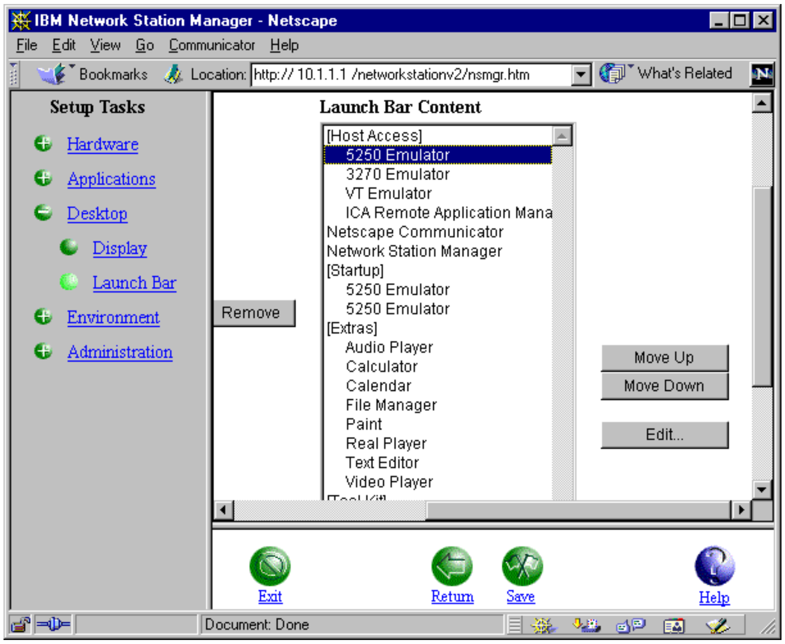
Vertical offset

Corner to offset: Upper left

Document: Done

Figure 331. Editing the 3270 Emulator

For another example, let’s assume that *all* user 5250 sessions should have display names assigned to them that are based on the user ID logged in at the Network Station. To define the 5250 display name on a system-wide basis, click **Desktop->Launch Bar** after ensuring that the System preference level is selected. Click **5250 Emulator** in the Launch Bar Content list box as shown in Figure 332.

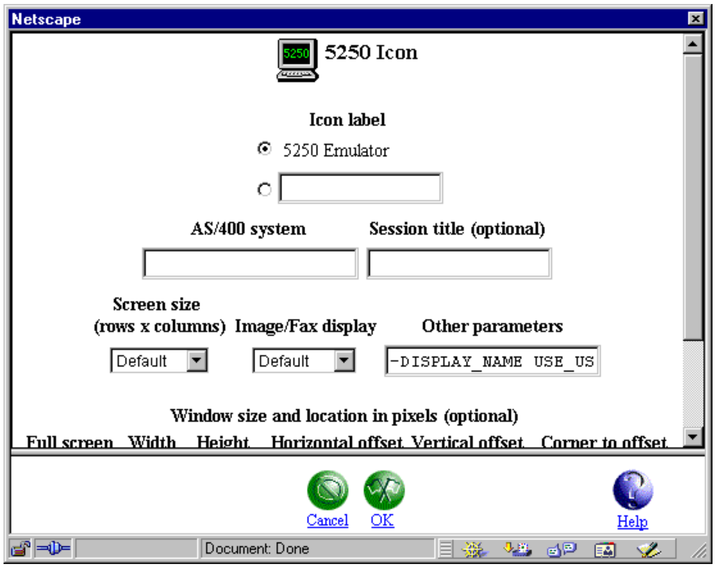


[Host Access]
5250 Emulator
3270 Emulator
VT Emulator
ICA Remote Application Mana
Netscape Communicator
Network Station Manager
[Startup]
5250 Emulator
5250 Emulator
[Extras]
Audio Player
Calculator
Calendar
File Manager
Paint
Real Player
Text Editor
Video Player
[Tool Kit]

Figure 332. 5250 Emulator: Launch Bar Content

Click **Edit** on the right side of the Launch Bar Content to open the 5250 Icon window (Figure 333 on page 388). Enter `-DISPLAY_NAME USE_USER_ID` in the Other parameters field. Also ensure that you use upper case and that there is a space between -DISPLAY_NAME and USE_USER_ID. Other display name alternatives are discussed in the following section.

Note: If you had only one AS/400 system, you could enter its IP address or name in the AS/400 system field. The user would *not* be prompted for the AS/400 name or address in the normal 5250 pop-up window.



5250 Icon

Icon label

● 5250 Emulator

○

AS/400 system

Session title (optional)

Screen size (rows x columns): Default

Image/Fax display: Default

Other parameters: -DISPLAY_NAME USE_US

Window size and location in pixels (optional)

Full screen Width Height Horizontal offset Vertical offset Corner to offset

Figure 333. 5250 display name based on user ID

13.5.4 LU Display name parameters

-DISPLAY_NAME can be specified using a specific LU name or LU pool name. You can also define multiple valid names by specifying more than one name or using a number and prefix to determine the number of valid names and their value. In effect, the -DISPLAY_NAME value also controls the number of sessions that can be started since there is a finite number of LU names defined.

The rules for S/390 display names are:

- Each active 3270 session must have a unique session name (virtual display name).
- Display names must be two to eight characters in length.
- The first character must be an alpha character, @, #, or $.
- All characters must be alpha, numeric, @, #, or $.

The rules for AS/400 display names include:

- Each active 3270 session must have a unique session name (virtual display name).
- Display names must be 2 to 10 characters in length.
- The first character must be an alpha character.
- All characters must be alpha, numeric, a period, or an underscore.
- All alpha characters must be in upper case.

The target AS/400 system must be at Version 3 Release 2, Version 3 Release 7, Version 4 Release 1, or later.

The display names can be specified in the following ways. Remember that the length of the name is determined by whether it is a 3270 (2-8 characters) or 5250 (2-10 characters):

- XXXXXX, where XXXXXX is the character name of the session. The user is limited to a single session.
- XXXXXX+n, where XXXXXX represents the first characters of the display name. The user is limited to n sessions. n is a number from 2 and 9. For example: JUAN+3 would allow the user to start three sessions where the first session would be JUAN1, the second JUAN2, then JUAN3.
- "XXXXX YYYYYYYY ZZZZ" is a list of possible display names separated by a space. The starting and ending quotes are required. The maximum number of names is determined by the size of Other parameters field in IBM Network Station Manager (256 characters). For example, if a user were to be limited to three 5250 sessions, each with the respective names of SALES, PERSONNEL and FINANCE, the parameter -DISPLAY_NAME "SALES PERSONNEL FINANCE" would be set through Network Station Manager. Please note that the parameter must be in upper case and that a space is needed between each display name.
- USE_USER_ID allows the user to start a single session where the session name is the same as the user's user ID.
- USE_USER_ID+n allows the user to start n sessions where the session name is the same as the user's user ID with the number n appended to the end. n is a number from 2 to 9. For example, USE_USER_ID+3 and a User ID of JUAN would have session names of JUAN1, JUAN2, and JUAN3.
- USE_HOST_NAME allows the user to start a single session where the session name is the TCP/IP Host Name of the Network Station. The Host Name is read from the DNS (Domain Name Server) at Network Station login time. Lower-case characters are converted to upper case by the 3270 emulator. If the Host Name exceeds the required length, the session name is truncated starting from the end, up to a period delimiter. For example, a Network Station with a Host Name of hondo3.mycompany.com would have a session name of HONDO3.
- USE_HOST_NAME+n is also supported. n is a number from 2 to 9. For example, USE_HOST_NAME+3 would allow the user to start three sessions where the first session would be HONDO31, the second HONDO32, and then HONDO33.
- USE_MAC_ADDRESS allows the user to start a single session where the session name is created starting with an alpha character which indicates the type of communication card (T for Token-Ring and E for Ethernet) followed by the lower bytes of the MAC address (lower four bytes for 5250, three bytes for 3270). The MAC address is displayed on the IBM Network Station “View Hardware Configuration” screen (boot monitor screen). For example, USE_MAC_ADDRESS with a Token-Ring Network Station and MAC address of 00.00.E5.68.D5.99 for a 5250 session would result in a session name of TE568D599.
- USE_MAC_ADDRESS+n allows the user to start n sessions where the session name is created as above but with n appended to the end. n is a number from 2 to 9. For example, USE_MAC_ADDRESS+3 with a Token-Ring Network Station and MAC address of 00.00.E5.68.D5.99 would result in 5250 session names of TE568D5991, TE568D5992, and TE568D5993.

- 5250 only:
  - – USE_USER_ID+99 is supported (the 99 is required). This option allows multiple users to share the same user ID. Up to 99 3270 sessions can be started. However, for performance reasons, 40 or fewer 3270 sessions is recommended. Session numbers from 1 to 99 are chosen randomly and appended to the user ID. If the user ID is 9 characters, the last character is removed before the 1- or 2-digit number is added. Two characters are removed for a 10-character user ID.
  - – USE_USER_ID+999 is supported (the 999 is required). Up to 999 3270 sessions can be started. Session numbers from 1 to 999 are chosen randomly and appended to the user ID. If the user ID is eight characters, the last character is removed before the 1- to 3-digit number is added. Two characters are removed for a nine character user ID and three characters are removed for a 10 character user ID.
- text+USE_USER_ID is another variation of USE_USER_ID. text indicates characters that precede the user's user ID. For example, DSP+USE_USER_ID and a user ID of JUAN would have a session name of DSPJUAN. The text can be from one to eight characters.
- text+USE_USER_ID+n is also supported. n is a number from 2 to 9.

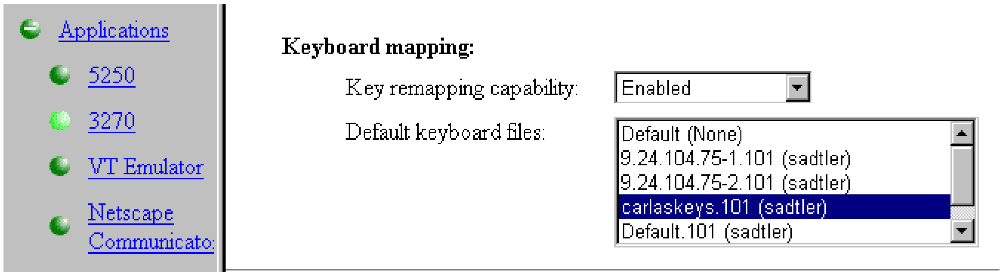
  text+USE_USER_ID+99 and text+USE_USER_ID+999 are supported.

13.6 Keyboard remapping

Keyboard remapping allows the user or administrator to reformat the keyboard for ease of use. Remapping can be done by the administrator for users at the system, group, or user level and stored. Users can do their own individual remapping at the emulator level for a single session or all sessions of that type. Keyboard remapping is available for 3270, 5250 and VTxxx emulators.

13.6.1 Who can create keyboard mapping files

Users can use the keyboard remapping program from their emulation session if the administrator has enabled it for their use (Figure 334). The key remapping capability is set at the application level in NSM for each emulator type.



Keyboard mapping:

Key remapping capability: Enabled

Default keyboard files:
Default (None)
9.24.104.75-1.101 (sadtler)
9.24.104.75-2.101 (sadtler)
carlaskeys.101 (sadtler)
Default.101 (sadtler)

Figure 334. Enabling the key remapping capability for an emulator application

An administrator can use the Keyboard Remapping program to create keyboard mapping files and then use NSM to assign them as defaults for users at the system, group, or user level.

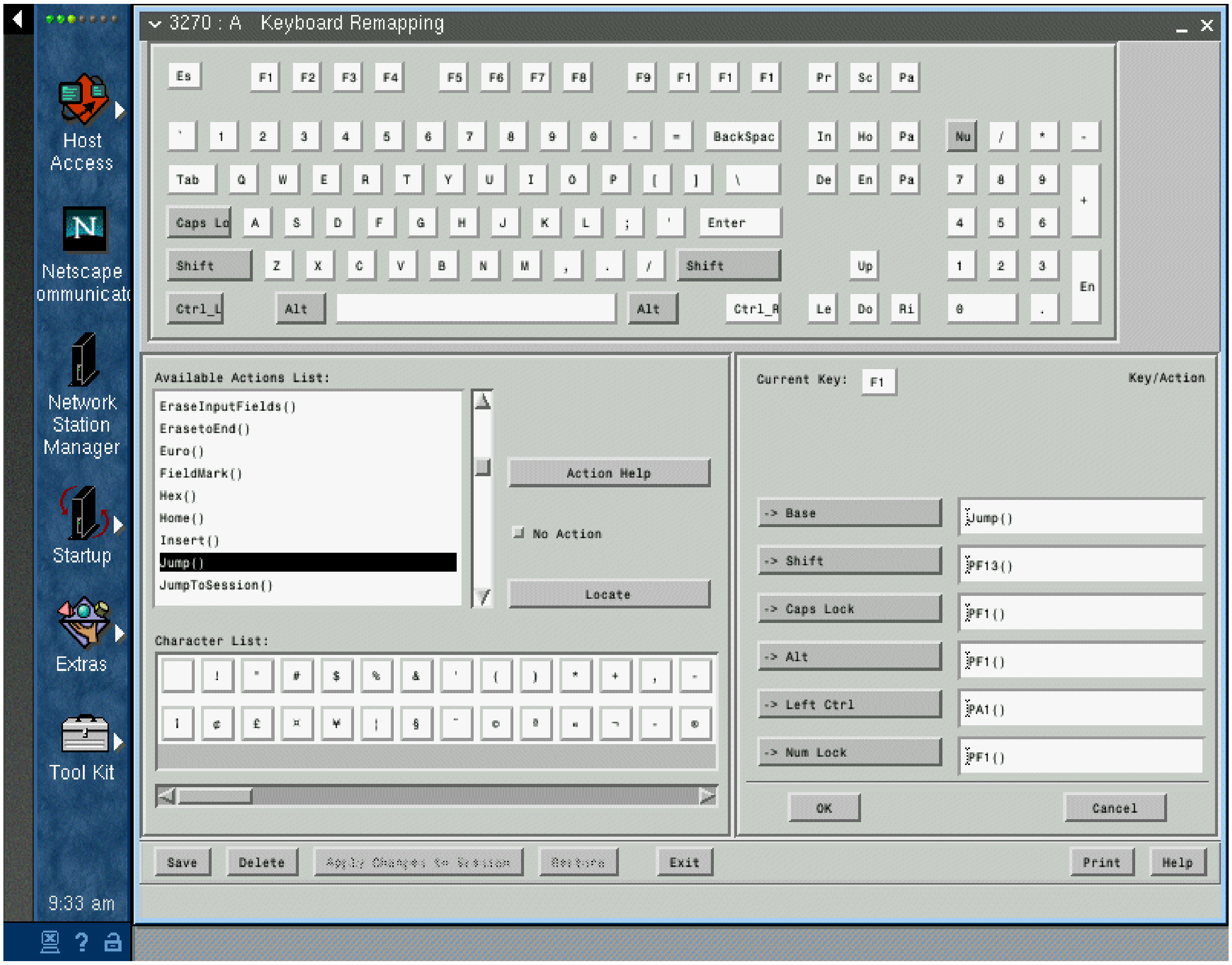
Note: The Keyboard Remapping program is not supported on monitors with a resolution of less than 800x600.

13.6.2 How the keyboard mapping files are created

A keyboard mapping file is created as described in the following sequence of events:

1. Use the **Keyboard Remapping** program from the **Option** pull-down menu in the emulator session to create and test keyboard mapping changes (Figure 335).

   If you have network stations with multiple keyboard types (for example, 101 and 102 PC keyboards), use a network station with the matching type of keyboard to create the keyboard mapping file. A keyboard mapping file applies to one type of keyboard.



Current Key: F1

-> Base: Jump()

-> Shift: PF13()

-> Caps Lock: PF1()

-> Alt: PF1()

-> Left Ctrl: PA1()

-> Num Lock: PF1()

Figure 335. The Keyboard Remapping main window

   On the top half of the Keyboard Remapping program window is the image of a keyboard. On the left is a list of available actions. The current definitions for a key button are displayed on the right (with the combination keys Shift, Caps Lock, Alt, Left Control, and Num Lock).

For example, Figure 335 shows changing the action for F1 so when a user presses F1 they jump to the next active 3270 emulator session.

To do this example, start by clicking (selecting) the F1 button from the keyboard image. This shows F1 in the Current Key box and lists the current Actions for it.

a. Search for the **Jump()** action from the Available Actions List, and click on it in the list.

b. Click the **--> Base** button on the Key/Action to assign the F1 key to the Jump() action.

c. Click **OK** to confirm the change.

d. If you want to apply these changes to the current session, click **Apply Changes to Session**.

2. Save your keyboard mapping changes. The keyboard mapping file is written to the user's IBM network station user directory. See the following section.

   When saving the new keyboard map, you have three options for the 3270 and 5250 and two options for VT:

   - The first option saves the keyboard mapping file as a default for all sessions of this emulator type, using this keyboard type, and for this user.
   - The second option (3270 and 5250 only) saves the keyboard mapping file for use with this user, emulator type, host, and session *instance* only. *Instance* means that if you are mapping this from the first emulator session to IP address 9.24.104.99, this keyboard map will only be used by this user, starting the first window of this type of emulator to host 9.24.104.99. If the user opens a second emulator session to the same IP address, this mapping will not be used.
   - The third option allows an administrator to create a keyboard mapping file for this type of session and keyboard and to give it a particular name. It can be set as a default for other users.

13.6.3 Where the keyboard files are stored

Keyboard mapping files are created when the user or administrator uses the keyboard remapping program. The files are stored in /userbase/nsmshared/userid/emulatortype/K/mapname.

In this pathname, note the following points:

- *userid* is the ID under which the map was created. When the administrator selects a keyboard map to be a system, group, or user default, the file is not moved from the system administrator's directory. Rather, a pointer is used to point back to the file in the administrator's directory.
- *emulatortype* is NSTERM, NS3270, or NS5250.
- *mapname* is:
  - If you choose **Save as default for all your sessions**, the format is:

    ```
    default.keyboardtype
    ```

    For example, default.101.

    Note: The mapname for NSTERM includes the emulation name such as default.101_xterm, default.101_vt100, sco.101_ansi

- If you choose **Save for this session only**, the format is:

  ```
  host_designator-session.keyboardtype
  ```

  host_designator is the IP address or host name used to connect to the host.

  session is the instance of the emulator session. For example, the first session to a particular host designation is 1, the next is 2, and so on.

  For example, if you save a keyboard mapping file (assume a 101 type keyboard) for the first session to 9.24.104.99, the keyboard name will be 9.24.104.99-1.101. If you save a map for the next instance of that session (whether that happens to be the B session), the map file name will be 9.24.104.99-2.101.

- If you choose **Save as a named key mapping file (administrator only)**, the format is:

  ```
  name_specified.keyboardtype
  ```

  Note that non-administrative users also see the choice to save the keyboard mapping file under a name. This option allows the user to save a file under a name. However, there is no way the user can use this file. The administrator does not see it as an option to assign to the user, and the user cannot specify it in any way.

13.6.4 Which keyboard file the user will use in a session

Keyboard maps can be associated with an emulator session either by NSM definition or by user definition.

The administrator can use NSM to define a default keyboard map at the user, group, or system level for an emulator at the application level (Figure 334 on page 390). A keyboard map can also be specified for a launch bar icon by using the other parameters field.

The user can also specify a keyboard map by defining the map and saving it at the session or default level. The user does not have the option to change the keyboard mapping using NSM.

The keyboard mapping for a particular emulator session and user are determined as explained in this series of questions:

1. Has a file been assigned using -KEYFILE? The administrator can specify a named keyboard mapping file by specifying -KEYFILE "*filename*" (use quotes if there are spaces in the file name) in the Other parameters field of the Launch Bar menu for the desired emulation icon.

   Note: At the this redbook was written, there was a known problem with the use of -KEYFILE with VT emulation.

2. (For 3270 and 5250 only) Is there a keyboard mapping file saved for this session by the user (option 2 (host_designator-session.keyboardtype) in the previous section? If so, use this keyboard map.

   Note: A map saved for a session only applies to the session in which you are working. For example, the first time you go to a particular host designator is the first session, and the map is specific to this. The second session started to the same host designator will not use the same map as the first.

3. Is there a default map for this session, emulator type, and keyboard type created by the user? (option 1 (default.keyboardtype)). If so, use this keyboard map.
4. Has the administrator assigned a specific default keyboard for the user/group/system level, emulator type, and keyboard type? (option 3 (name_specified.keyboardtype)). If so, use this keyboard map.
5. If not, use the default emulator keyboard.

13.6.5 Modifying an existing keyboard file

The Keyboard Remapping program does not give you the option of opening a particular file. This means that to modify a keyboard map, you need to have a session open that is using that map. Then, when you use the keyboard remapping option from the session, you will see the values for that map and can modify them.

If you need to modify a keyboard map that you do not normally use, you can use the advanced diagnostics to open an emulator session using the keyboard map you want to change. For example, to change a 3270 emulator keyboard map:

For 3270 sessions, use:

```
nsm_wrapper ns3270 host -KEYFILE filename
```

For 5250 sessions, use:

```
nsm_wrapper ns5250 host -KEYFILE filename
```

For VT emulator sessions, use:

```
nsm_wrapper nsterm -host host -KEYFILE filename
```

Note: The variable *host* is the destination IP address or hostname. The variable *filename* is the keyboard map (for example, myfile.101, yourfile.101_xterm, and so on).

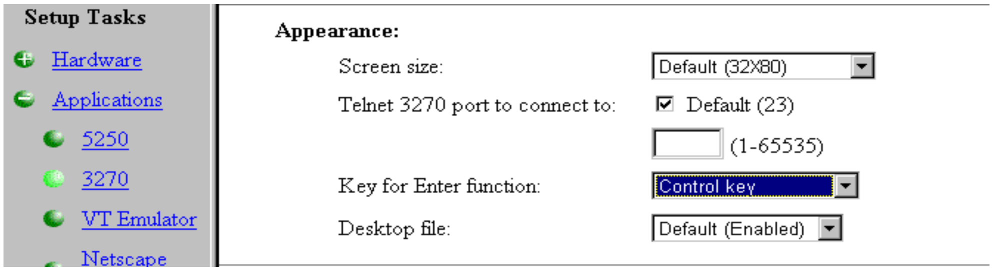
To reset your session to the default emulator mapping, you need to delete any keyboard mapping files that apply to the session. If these are user-specific files (stored in the user’s home directory), anyone with access to the NSM server and access to those directories can delete them.

Note

There may be rare cases where you find you need to update a keyboard mapping file that you cannot use in a session yourself. The keyboard map files are text and can be updated with an editor (for example, PFE). Be very careful!

13.6.6 Changing the Enter key

Many users prefer to use the Control key for Enter, and the Enter key for Newline. Although the Enter key location can be changed using keyboard remapping, it can also be changed through the Network Station Manager. For example, select System, Group, or User for the Preference level and then **Applications->3270 Settings**. You may have to scroll down the page to get to Appearance part. From here, you may specify the Key for Enter function: Enter or Control key as shown in Figure 336.



Appearance:

Screen size: Default (32X80)

Telnet 3270 port to connect to: ☑ Default (23)

(1-65535)

Key for Enter function: Control key

Desktop file: Default (Enabled)

Figure 336. Changing the Enter key for a 3270 session

The Enter key location for the 5250 application can be changed through keyboard remapping, through Network Station Manager, or by the user through Miscellaneous Preferences.

If you have other keyboard changes to make, it would make sense to use keyboard remapping to set the Enter key location. However, the Enter key location may also be changed through the use of a 5250 application setting in Network Station Manager. For example, after starting Network Station Manager, the following could be entered in the 5250 Application Additional parameter field to switch the Enter key location:

```
NS5250*ENTER_KEY:ENTER_NEWLINE_AND_RIGHT_CTRL_ENTER.
```

Other possible 5250 additional parameters are described in the 5250 session online help. Please note that settings in the Miscellaneous Preferences take precedence. However, an administrator can prevent the user from accessing Miscellaneous Preferences through the use of Network Station Manager (under the 5250 Application setup task).

13.6.7 VT considerations

The new VT emulator in Version 2 Release 1 provides additional enhancements as discussed earlier in this chapter. However, there are several considerations which you should be aware of with VT emulation. For example, although the supported emulation types include XTERM, ANSI, VT100, VT102, VT200, VT220, VT300, and VT320, it does not provide IBM 3151, VT340, or VT420 emulation support. In addition, there is currently no SCO ANSII data stream support. Unlike the 5250 and 3270 emulators' graphical color mapping interface, color mapping within VT is done through a command-line interface. For example, the background and foreground colors of a VT session can be specified through Network Station Manager by using the following flags:

-bd (color) Specifies the border color; black is the default

-bg (color) Specifies the color of the application window background; white is the default

-cr (color) Specifies the color of the text cursor; the default is black.

-fg (color) Specifies the color of the text characters; the default is black

-ms (color) Specifies the color of the pointer; the default is black

13.7 Keypad support

The 3270 emulator and 5250 emulator sessions allow users to create pop-up and pull-down keypads and to use keypads created by the administrator. A keypad has keypad buttons. Each keypad button has a key sequence or playback file associated with the button. Using the NSM applications settings for the 3270 and 5250 emulators, the administrator can control whether the user is allowed to use the keypad customizer and can make a list of keypads available using the IBM Network Station Manager program.

Users can use default pop-up or pull-down keypad files made available by the administrator, even if they are not authorized to use the Keypad Customizer program.

Figure 337 shows an example pop-up keypad.

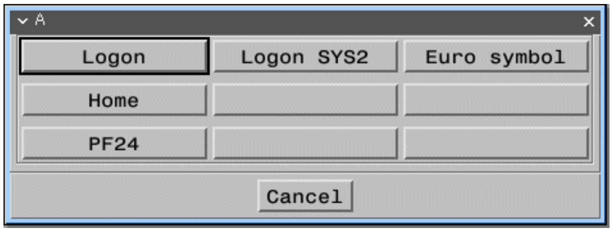


Figure 337. The pop-up keypad

An administrator can use the Keypad Customizer program and IBM Network Station Manager program to create system, group, and user default keypad files.

Notes

- Default keypad files are not copied. If the administrator accidentally changes a default keypad file, users use the changed file. When the administrator selects a keypad to be a system, group, or user default, the default file is not moved from the system administrator's directory. Rather, a pointer is used for that user's scope that points back to the default keypad file, in the admin directory.
- The Keypad Customizer program is not supported on monitors with a resolution of less than 800x600.

13.7.1 Creating a keypad

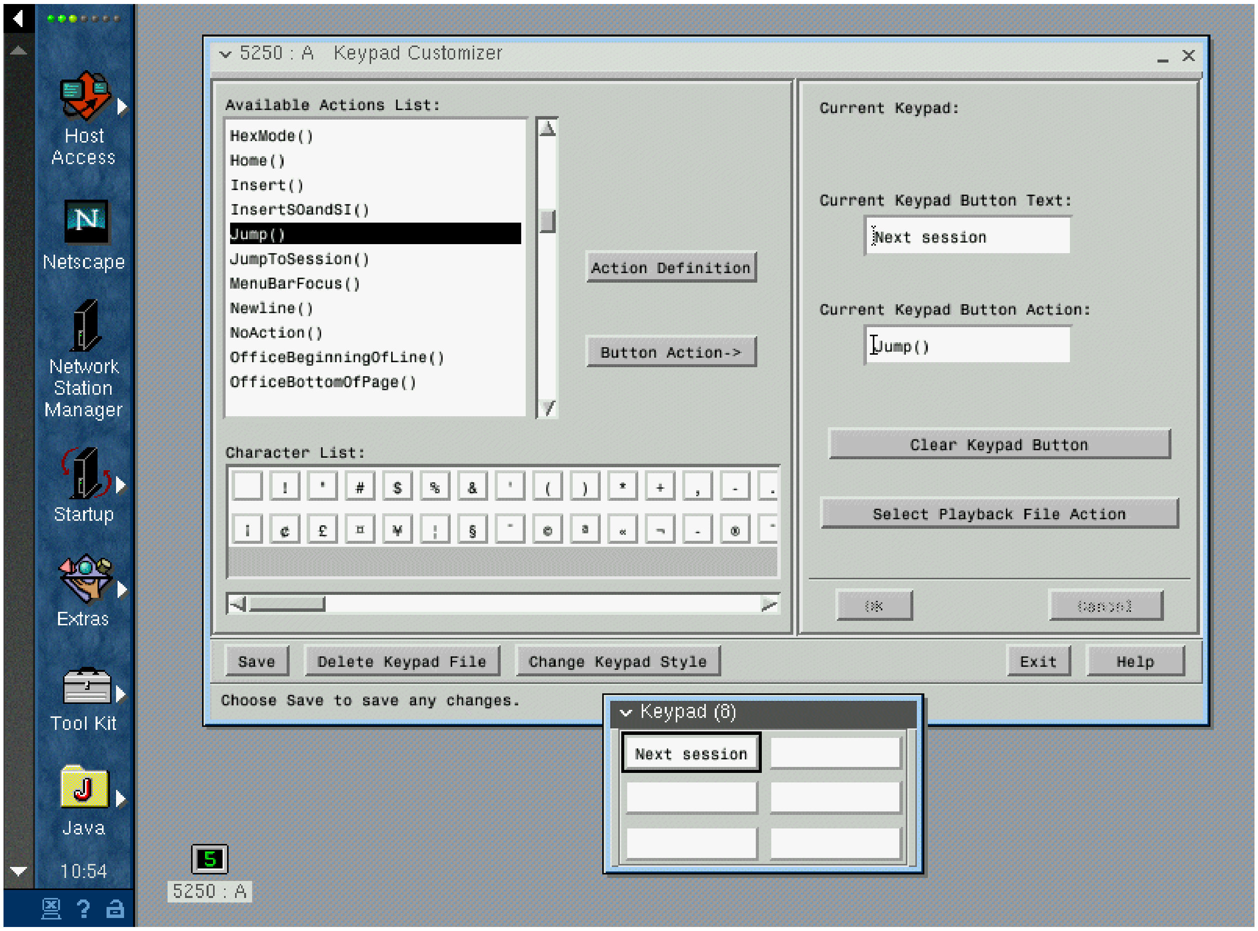
A keypad file is created as described here:

1. Logon to the Network Station. Use an administrator user ID if you want to save this file for use by others.
2. Start an emulator session.
3. Start the Keypad Customizer program. Select **Options->Customize Keypad...** Select the keypad you want to modify from the list. If there are no customized keypad defined, like in our example, click **New Keypad** to start.

4. Selecting New Keypad opens the Keypad Customizer program Figure 338). The program starts with the main window and a floating keypad window. The keypad has only empty boxes because this is a new keypad file.

   The box labeled Change Keypad Style at the bottom of the main window allows you to modify the style of the keypad with the following options:

   - Change number of rows (min 1, max 8)
   - Change number of columns (min 1, max 8)
   - Change text length (min 1,max 20)
   - Change Keypad style between pop-up and pull down



Current Keypad Button Text: Next session

Current Keypad Button Action: Jump()

Choose Save to save any changes.

Figure 338. The desktop of a network station with the menu bar on the left and the Keypad Customizer program running

5. To customize the keypad, complete these steps:

   a. Select an empty box from Keypad window by clicking it. The main window shows that the Current Keypad Button Action is Noaction().

   b. Click in the Current Keypad Button Text input field and enter the text that will be displayed in the Keypad box, for example: `Logon`. If you leave this field empty, it gets the same text as in the action field after the OK button is clicked.

   c. Scroll the **Available Actions List** and select the wanted action. In our example, we chose String().

d. Click **Button Action**. The selection is copied into Current Keypad Button Action. Some of the actions require parameters inside the open and close brackets. Click **Action Definition** for information on the format of the action you have chosen. You can add more than one function to the button. They will be added to the end of the definitions already there and will be executed in order.

e. Click **OK** to apply the changes.

f. Repeat the entire process for another Keypad button action.

You can change the order the of the buttons on the keypad. Move the keypad buttons by right-clicking the button to move. The icon changes to a walking stick man. Next, move it to new location and left-click. If you move a button over another that is already defined, these two buttons are switched.

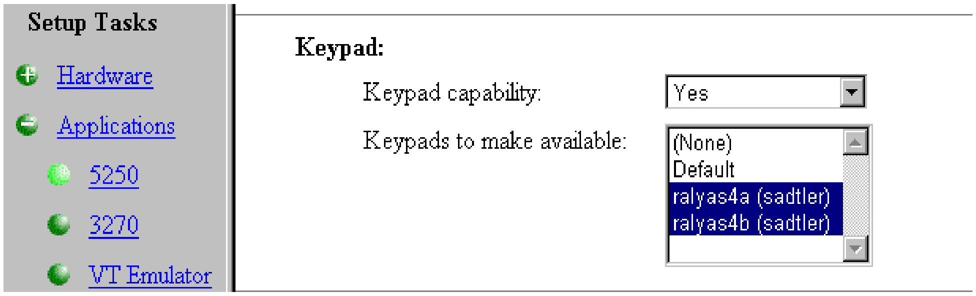
Click **Save** to save the keypad definition to a file. The customized window now shows the file name in the Current Keypad field. The file is saved in $UserBase/nsmshared/*userid*/*NS3270_or_NS5250*/W.

```
1
0 0
3 2
13
Next session: jump()
empty_button: nothing()
home: menu-bar-focus()
empty_button: nothing()
empty_button: nothing()
empty_button: nothing()
```

The keypad file has the number of rows and columns (3x2), the text length (13), and the definitions for the boxes as shown here.

6. Click **Exit**.

7. If the keypad is saved by an administrator, it can be made available to users by modifying the emulation application settings. To choose multiple keypads, hold down the left mouse button and drag it over the file names as shown in Figure 339.



Keypad:

Keypad capability: Yes

Keypads to make available:
(None)
Default
ralyas4a (sadtler)
ralyas4b (sadtler)

Figure 339. Choosing multiple keypads

Note: The -KEYPAD parameter can be used to automatically start a pop-up keypad when the 3270 session starts. -KEYPAD is entered in Other parameters for the Launch Bar content that starts the 3270 session. One space and the (case sensitive) pop-up keypad file name follows -KEYPAD. If your keypad file name contains any spaces, use double quotes around the file name (for example, -KEYPAD "keypad file name").

13.8 Secure host-based transactions

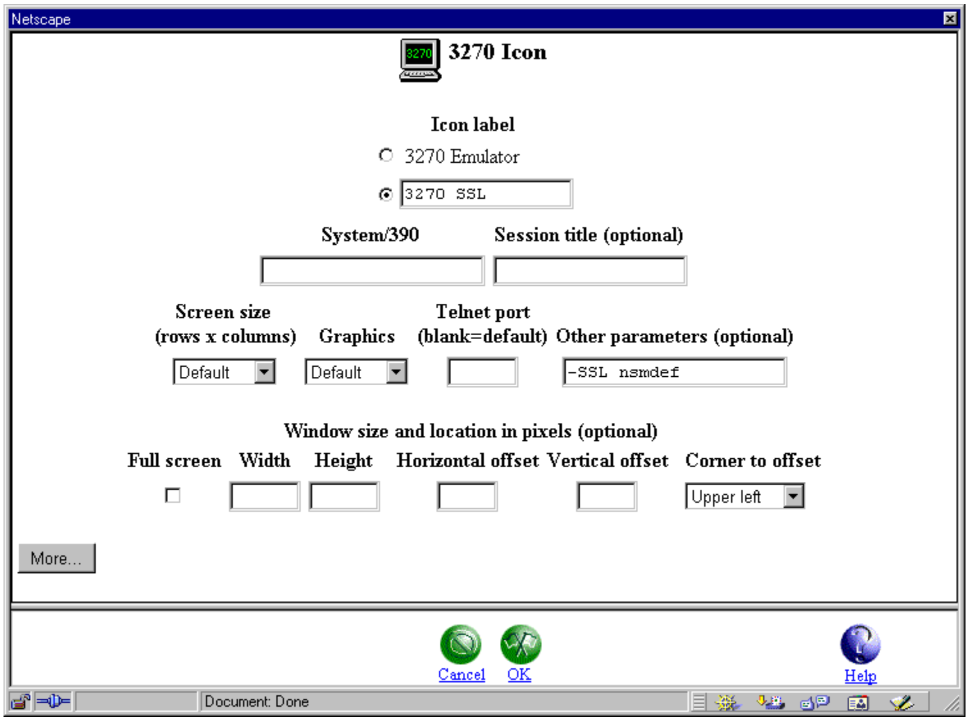
The Network Station Manager V2R1 provides Telnet Secure Sockets Layer (SSL) version 3 for secure host based transactions over Internet connections, including user ID and password encryption.

SSL provides encryption for the transmission of private information over the Internet.

-SSL is followed by a (case sensitive) file name. The file name does not have an extension when specified in Other parameters (the appropriate extension is automatically added by the 3270 emulator). If -SSL is specified, the default port changes from 23 to 992.

The Network Station Manager V2R1 provides a default keyring file called nsmdef.kyr in the $ServBase/defaults directory. Figure 340 on page 400 shows . our example for defining the SSL parameter to a 3270 session in the Launch Bar. Follow these steps:

1. Select **System**, **Group**, or **User level** from Network Station Manager program.
2. Select **Desktop->Launch Bar** from Setup Tasks.
3. Select the applicable host session from Launch Bar Content box, and click **Edit**. A similar window to the example in Figure 340 on page 400 appears. If you are adding a new host session, then select it from Applications box. Click Add, then select it from Launch Bar Content box, and click **Edit**.
4. Add the -SSL `keyring_filename` into the Other parameters field.
5. Click **OK**.
6. Click **Save**.



3270 Icon

Icon label

○ 3270 Emulator

● 3270 SSL

System/390:

Session title (optional):

Screen size (rows x columns): Default

Graphics: Default

Telnet port (blank=default):

Other parameters (optional): -SSL nsmdef

Window size and location in pixels (optional)

Full screen: □

Width:

Height:

Horizontal offset:

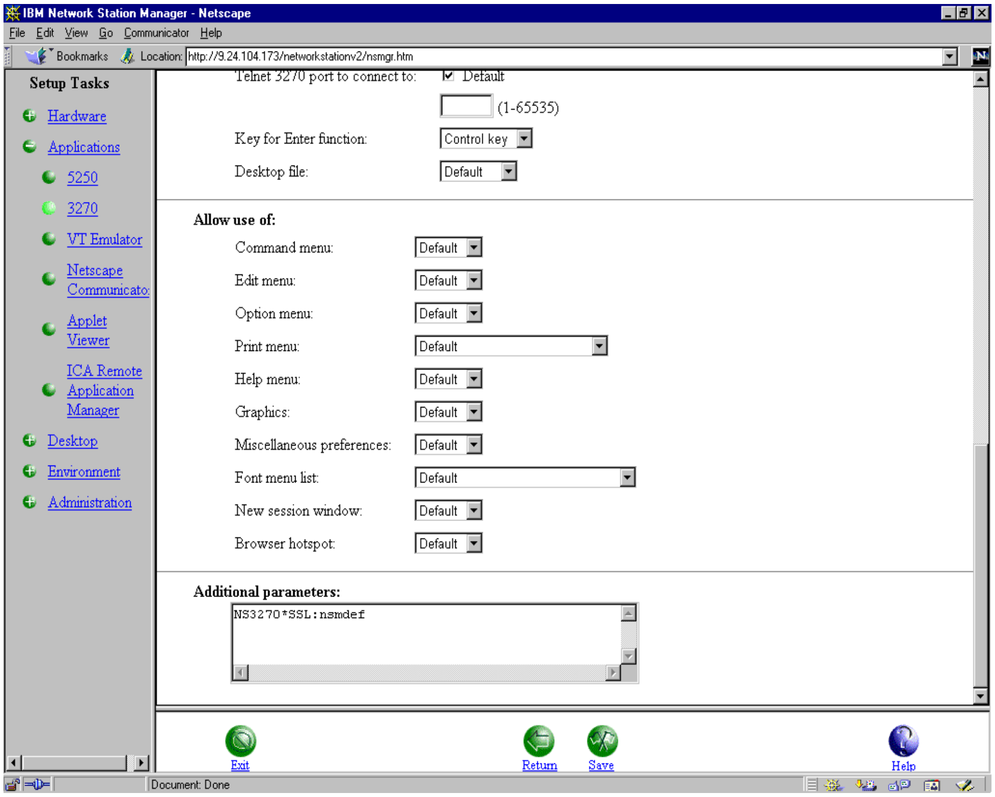
Vertical offset:

Corner to offset: Upper left

Figure 340. Adding a nSLL parameter to a 3270 session

In case the SSL is needed for all host sessions, the administrator needs to define the SSL parameter in the Additional parameters field with **Network Station Manager->Applications->3270 Settings**. Add the following line into Additional parameter, as shown in Figure 341.

```
NS3270*SSL:nsmdef
```


IBM Network Station Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://9.24.104.173/networkstationv2/nsmgr.htm
Setup Tasks
Hardware
Applications
5250
3270
VT Emulator
Netscape Communicator
Applet Viewer
ICA Remote Application Manager
Desktop
Environment
Administration
Exit
Return
Save
Help
Document: Done

Telnet 3270 port to connect to: ☑ Default

(1-65535)

Key for Enter function: Control key

Desktop file: Default

Allow use of:

Command menu: Default

Edit menu: Default

Option menu: Default

Print menu: Default

Help menu: Default

Graphics: Default

Miscellaneous preferences: Default

Font menu list: Default

New session window: Default

Browser hotspot: Default

Additional parameters:

```
NS3270*SSL:nsmdef
```

Figure 341. Adding SSL parameter to 3270 Settings in Network Station Manager

SSL uses a security exchange to secure the TCP/IP connection between the client and the server. The exchange occurs after the TCP/IP connection is established. During the exchange, the client and server agree on the security keys that they will use for the session, and the client authenticates the server. After that, your server uses SSL to encrypt and decrypt all of the information in both the request and the server response. This information includes:

- The URL that the client requests
- The contents of any form that you submit
- Access authorization information (such as user names and passwords)
- All data sent between the client and the server

13.8.1 VT debug log

The user can turn on the debug log in a VT emulation session. Turning on the log causes all activity on the VT emulator (commands and responses) to be sent to a file. The default file name is `$UserBase/nsmshared/userid/Nsterm`.

This file name and location can be overridden by using the Additional Parameters field in the VT emulator applications setup (NSTerm*logFile: path/filename).

You can set the log to automatically run (-l) or not to run (+l) in the Launch Bar Other parameters field for a VT emulation icon. The default is not to run, and the user can turn on or off the log from the Control options in the emulator session.

For the user to have access to the debug log options, the control options must be enabled for the user in the NSM VT emulator application menu.

Chapter 14. Windows application access (ICA)

The ICA client is a V2R1 IBM Network Station application that provides access to a Windows session running on high-performance Citrix servers. Once the connection to a Citrix server is established, you can access Windows applications and work with files in a similar way to working on a local PC.

The ICA client displays the Windows session in a separate window on the IBM Network Station screen and is fully integrated with your other IBM Network Station applications. You can cut and paste text and graphics between Windows applications in the ICA client window and your other applications.

Your IBM Network Station's mouse and keyboard can be used with Windows applications in the usual way. You can set up key mappings to enable you to enter PC keys not available on your IBM Network Station's keyboard.

Note: See Appendix K, “ICA error messages” on page 665, for a list of possible error messages and a short description of possible solutions.

14.1 The Citrix servers and ICA client features overview

This section describes the Citrix servers that work with the IBM Network Station and the features found in the ICA client support.

Citrix servers

Citrix WinFrame and Citrix MetaFrame are fast and easy Windows NT application server solutions for delivering Windows applications to the IBM Network Station and other desktops, including PCs, Apple Macintosh computers, X terminals, and UNIX workstations. Citrix server software usually runs on a high-performance PC. A single-processor Citrix server typically supports up to 15 simultaneous client connections.

Windows 2000 support

Citrix has announced the latest version of its MetaFrame application server software family—MetaFrame 1.8 for Windows 2000 Servers. This choice was not available at the time this redbook was written. However, you should consider it if you are planning on running Windows 2000 in your business.

The Citrix server communicates with the ICA client over a standard TCP/IP network connection. For detailed information about Citrix and their family of products, visit the Web site at: `http://www.citrix.com/`

Readme file for the ICA client

A readme file for the ICA client can be found in the product directory <PRODBASE>\x86\usr\lib\ICAClient\readme.

Independent Computing Architecture (ICA) protocol

ICA is a general-purpose presentation services protocol owned by Citrix Systems. Conceptually similar to the UNIX X-Windows protocol, ICA allows an application's user interface to execute with minimal resource consumption on a client machine. Meanwhile, application logic executes on the WinFrame or MetaFrame multi-user application server.

The ICA protocol has been specially designed for transmitting Windows graphical display data, and keyboard and mouse input, over a network connection. The key features of the ICA protocol that help to achieve the high performance are:

- Intelligent command and object-specific compression
- Intelligent caching of Windows objects including bitmaps, brushes, glyphs, and pointers
- Run-length encoding

The ICA protocol is designed to be client independent.

More information about the ICA protocol is available from the Citrix World Wide Web page at: `http://www.citrix.com/`

The ICA clients

An ICA client application presents a list of the ICA connection definitions you have set up and allows you to initiate an ICA connection to a Citrix server.

Once you are connected to a Citrix server, the ICA client application presents the ICA client window to handle communication with the Citrix server and provide the display, keyboard, and mouse interface between the server and your IBM Network Station.

The ICA Remote Application Manager also allows you to create new connection definitions, or edit the definitions of existing connections. For each connection, you can define the following features:

- **Window size and borders**: The ICA client window size can be set to one of four predefined window sizes, full screen size, or a custom size (up to the greater of 1280x1024 or your IBM Network Station display size). Window borders and the title bar can be turned off.

  Window size allows you to select one of four standard window sizes, full screen, or a custom size. If custom is specified, the width must be between 300 and 1280. If height is specified, it must be between 300 and 1024.

- **Number of colors**: The ICA client window can be set to 256 or 16 colors. This is an ICA Protocol limitation. At some future time, the ICA Protocol may be extended to support more than 256 colors, for example, 16-bit TrueColor. In addition, you can define default values for the window size and window colors, which are then used as the default for all new connection definitions.

- **Color approximation**: Color approximation can be used if the IBM Network Station is running in PseudoColor mode. In this mode, differences in the palettes used between the ICA client (and the Windows applications it displays) and the IBM Network Station may cause an annoying flashing that occurs when switching context. The ICA client color approximation scheme eliminates this flashing by using colors from the local desktop palette to display the ICA Windows sessions.

- **True color**: The ICA client maps ICA protocol colors (16 or 256) to true color. Running the IBM Network Station in TrueColor mode provides the most compatible color management if the ICA client is sharing screen space with any other program (including the window manager and desktop).

Two 256 color mapping modes are available: the approximate color and the exact color mapping modes. In the exact color mapping mode, when the Network Station is configured with a 8-bit color depth support (256 colors) and the ICA client with 256 colors, differences in the palettes used by the Network Station's operating system and the ICA client may cause an annoying flashing that occurs when switching context. The ICA client's color approximation scheme eliminates this flashing by using colors from the local desktop palette to display the ICA Windows sessions.

These considerations do not apply when the Network Station is configured with a 16-bit color depth support.

Remote applications and load balancing

The ICA client supports two types of connections: ICA connections and remote applications. An *ICA connection* allows a user to access a Citrix desktop. The user can run any applications available on the desktop, in any order. A remote application is a predefined application and its associated environment (for example, directories and initialization files) that execute on a remote Citrix server. There are several ways to define a remote application:

- By defining an ICA connection that directly executes an application.
- By defining an ICA connection that points to a published application created using the Published Application Manager on the Citrix server. This method also supports load balancing.

The Load Balancing Services can be used with multiple Citrix servers to provide load balancing capabilities. Citrix load balancing support lets you define a remote application that runs on a predefined set of Citrix servers. When a user launches the remote application, the Citrix load balancing software uses a tunable algorithm to select a server to execute the application. The load balancing parameters are configurable and can be tuned to provide maximum throughput and system availability.

Another advantage of load balancing is increased reliability. You can configure a pool of servers that are capable of running your users' applications without your users needing to know which server is actually running the application. This way, you can easily bring servers off-line for maintenance without affecting application availability, or add more servers for increased performance.

Printer mapping

You can redirect printing jobs from applications you are running on a Citrix server and print them to a printer connected to your IBM Network Station.

If a Network Station printer is defined with an associated Windows NT printer device driver name, the ICA client automatically creates the printer on the ICA Server during session logon and deletes it when the session ends. Printers can also be explicitly created by using the Windows NT Printer Wizard to add one or more printers for use in the ICA session.

The ICA client supports any spooled printer available from your IBM Network Station, as long as the associated printer driver is installed on the Citrix server.

See 14.7.3, "Connecting to local printers" on page 476, for more information.

Audio mapping

Audio mapping allows your client computer to play sounds generated by applications running on the Citrix server. ICA client audio support includes configurable sound quality levels that allow you to customize sound quality based upon the amount of bandwidth available.

Windows NT Server Audio is limited in its features:

- Wave sound only (server may convert other formats to Wave)
- Midi music not supported
- CD audio not supported
- no sound card is required on the server

The supported audio characteristics include:

- Linear PCM
- 8 and 16 bit
- 8, 11, 22, and 44 Khz
- Mono and stereo

Device control, for example volume, is not supported.

COM port mapping

Client COM port mapping allows devices attached to the client computer's COM ports to be used from ICA sessions on a Citrix server. This allows local serial devices to be used by applications running on the Citrix server.

See 14.7.4, “Connecting to local serial devices” on page 477, for more information.

Data compression

Data compression reduces the amount of data transferred across the ICA session to increase performance over bandwidth-limited connections.

Caching

Caching stores commonly used graphical objects such as icons in a local cache on the client computer to reduce the amount of data sent over the connection. Caching commonly used bitmaps tends to increase performance, especially for bandwidth-limited connections.

The ICA client employs both an internal transient cache and an external persistent cache.

Since the IBM Network Station does not have a hard disk, the external persistent cache is implemented as an in-memory file system, which is created each time the Network Station is rebooted. By default, this in-memory file system is not enabled due to the finite amount of memory in the Network Station. In V2R1 of NSM, persistent caching must be enabled by following the ICA persistent caching directions in the /.profile file.

Drive mapping

Client drive mapping makes selected directories on the IBM Network Station available to the users when they connect to a Citrix server. Access login and read/write permissions can be set for each selected directory.

Socks support
ICA connections can use the socks networking proxy protocol to enables hosts on one side of a socks server to gain full access to hosts on the other side of the socks server without requiring direct IP reachability. The ICA Remote Application Manager allows the user to specify the socks server address and port number.

Encryption
ICA sessions can be encrypted using basic, 40-, 56-, or 128-bit encryption keys. The ICA client must connect to an Citrix Server that supports an equal or higher number of bits for the encryption key.

User logon parameters
This feature allows you to set up the user's name, password, and authenticating Windows NT domain for an ICA session. If these parameters are not provided, the user is prompted for them each time they connects to a Windows NT multi-user server.

Published applications
See “Citrix MetaFrame” on page 412, for a discussion about published applications.

Shadowing
See “Citrix MetaFrame” on page 412, and the discussion about shadowing in 14.4.1.3, “Shadowing” on page 425.

Clipboard data exchange
The ICA client displays the Windows session in a separate window on the Network Station screen. It is fully integrated with your other locally running Network Station applications, such as the emulators, Netscape browser, etc. You can cut and paste text (but not graphics) between Windows applications in the ICA client window and your other applications.

See 14.7.2, “Copying and pasting text and graphics” on page 475, for more information.

License pooling
Multiple applications launched from the same client device only consume one ICA license slot on the server, if all applications run on the same server.

National Language Support (NLS)
The ICA client supports all keyboards that the NC OS network station supports, except for DBCS and bi-directional keyboards.

Internationalization
Any error messages sent to the end user are translated into the different supported languages.

14.2 Windows NT multi-user environment

A Windows NT *multi-user* server environment is a standard Windows NT server environment that incorporates two new components: a multi-user server core and a display protocol. Users access the Windows NT multi-user environment through a thin client software. The thin client software can present or display the Windows user interface on a wide range of desktop hardware, the Network Station being one of them.

Windows 2000 support

Citrix has announced the latest version of its MetaFrame application server software family—MetaFrame 1.8 for Windows 2000 Servers. This choice was not available at the time this redbook was written. However, you should consider it if you are planning on running Windows 2000 in your business. For detailed information about Citrix and their family of products, see their Web site at: `http://www.citrix.com/`

The multi-user server core provides the ability to host multiple, simultaneous client sessions on a Windows NT server (Figure 342). The display protocol allows the thin clients to communicate with the server over the network. The protocol separates the application logic from the user interface. On the client, users see and work with the application’s interface, but 100% of the application executes on the server. The display protocol sends only keystrokes, mouse clicks, screen updates, and audio across the network.

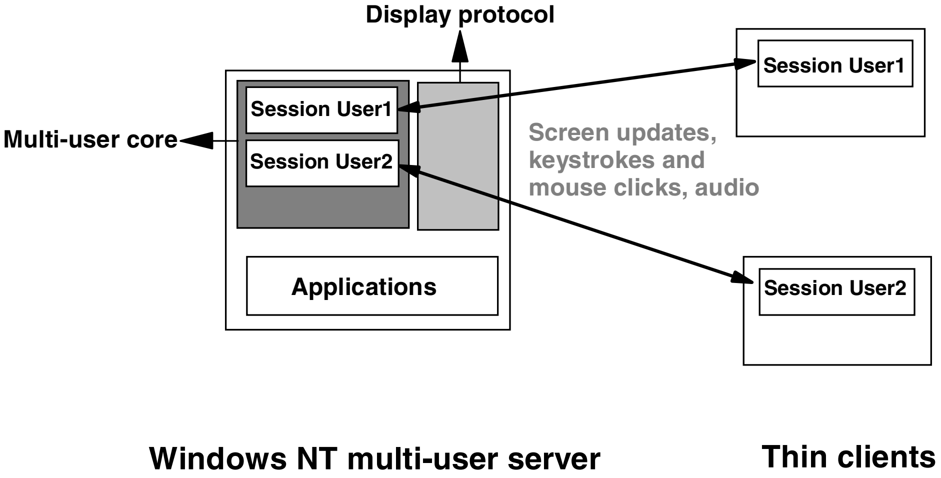


Figure 342. Windows NT multi-user concept overview

Most standard Windows-based applications do not need any modification to run on the Windows NT multi-user environment. However, the system administrator must address the multi-user environment during the installation process. The common settings of an application and the user-specific settings must be separated by the system during the installation.

Note

Even though most Windows NT applications work under the Windows NT multi-user environment, there are applications that are incompatible with the environment. Examples are communication applications where the host system identifies the user with the IP address or the computer name he is using. Since all users on one Windows NT multi-user server use the same IP address and computer name (for example, the server's), this application will not work correctly. Sometimes it is possible to change the protocol the client application uses to communicate with the host (for example, use IPX instead of TCP/IP). This, in some cases, remedies the problem. In other cases, there is simply no solution other than re-designing the application.

Generally, this separation is handled by the system when the administrator types a specific command before proceeding with the installation of a new application. However, there are some exceptions. For additional information, refer to the *IBM Network Station Guide for Windows NT,* SG24-2127, and *IBM Network Station Release 3 Guide for Windows NT,* SG24-5221.

The user data should be stored in secure user home directories to ensure that each user works in a separate session and cannot access the data of another user.

14.2.1 The operating systems and add-on products

There are two main operating systems to be considered in a multi-user environment: Windows NT Server 3.51 and Windows NT Server 4.0. The multi-user products are different depending on which server you are running.

Before going into this topic, it would be best to introduce some terminology:

ICA The Independent Computing Architecture (ICA) protocol is a general-purpose presentation services protocol developed by Citrix Systems. The ICA protocol allows an application's user interface to execute with minimal resource consumption on a client machine, while application logic executes on a WinFrame or MetaFrame multi-user NT application server. The ICA protocol has been specially designed for transmitting Windows graphical display data, and keyboard and mouse input over a network connection. The ICA protocol is well-tuned and offers a high degree of data compression to allow the client to communicate with the server even over bandwidth-limited WAN links.

RDP The Remote Desktop Protocol (RDP) is a protocol developed by Microsoft that, just as the ICA protocol, allows a thin client to communicate with NT Terminal Server Edition over the network. The protocol is based on the International Telecommunications Union's (ITU) T.120 protocol, an international, standard multi-channel conferencing protocol, but has proprietary extensions added to it. The Network Station does not support the RDP protocol.

X11 X11 is a remote graphics protocol, similar in concept to ICA, but designed for graphics-intense operations on more powerful end-user devices. X is not designed for low bandwidth.

Thin client A thin client is an end-user device that uses applications and system resources located on servers in the network. Thin-client software allows the thin client to communicate with an application server.

Windows-based terminals (WBTs)

Windows-based terminals are a new class of hardware devices designed mainly to access Windows NT multi-user application servers. Most of the time, they are powered with Microsoft Windows CE and support RDP and ICA protocol. Most WBTs also support local emulators such as 3270/5250 and VT, but no WBT supports a local browser or have Java capabilities, due to their limited local processing capabilities.

X-based terminals

X-based terminals are devices whose only function is to provide a display, mouse, and keyboard for the X protocol.

Network Computer

A Network Computer is a low-cost end-user hardware device with some local processing capability, specifically designed for a network computing environment, supporting (at least) a standard profile of features. The Network Computer is more than a terminal due to its local processing capability. It can access Windows NT multi-user application servers (and often UNIX application servers via the X protocol) and also have the capabilities to run a local Web browser and have Java capabilities.

Windows-based PCs

Windows-based desktops are any existing 32-bit Windows desktop operating system (Windows 95, Windows 98, Windows NT workstation) or 16-bit Windows based desktops running the Windows 3.11 operating system.

UNIX-based desktops

Windows-based desktops are any of the following UNIX desktop operating systems: Solaris/Sparc, Solaris/x86, SunOS, Compaq Tru64, HP/UX, IBM, SGI, Linux, or SCO.

14.2.1.1 Windows NT Server 3.51

Now that the terms are familiar, we can introduce the multi-user environment. Figure 343 shows an overview of a Windows NT 3.51, the products that implement the multi-user environment, and the clients that can communicate with the server.

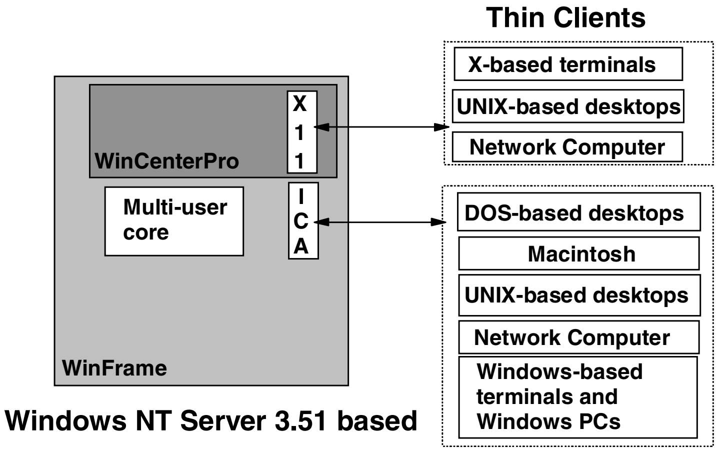


Figure 343. Windows NT Server 3.5.1 multi-user operating systems and add-on products overview

Citrix WinFrame

WinFrame is a derivative of Windows NT Server 3.51 that includes Citrix-developed extensions to the operating system that gives it multi-user capabilities. WinFrame includes the Citrix-developed ICA protocol for communicating with the clients.

In terms of functionality, WinFrame is comparable to MetaFrame. The difference is that WinFrame is an entire Windows NT multi-user operating system and that the interface is Windows NT 3.51 based. MetaFrame is an extension to the Windows NT, Terminal Server Edition product.

Citrix WinFrame uses a concurrent-user licensing scheme. Only one license per simultaneously connected user is required.

NCDi WinCenterPro

WinCenterPro from NCDi is an add-on product installed on top of WinFrame, adding X protocol support in addition to WinFrame's ICA protocol. Most of the WinFrame features are supported except those that are ICA-dependent, such as the load balancing services from Citrix. However, WinCenterPro has its own load balancing technology to allow load balancing from clients connecting via the X protocol.

14.2.1.2 Microsoft Windows NT Server 4.0, Terminal Server Edition

Figure 344 on page 412 shows an overview of a Windows NT 4.0 server, the products that implement the multi-user environment, and the clients that can communicate with the server.

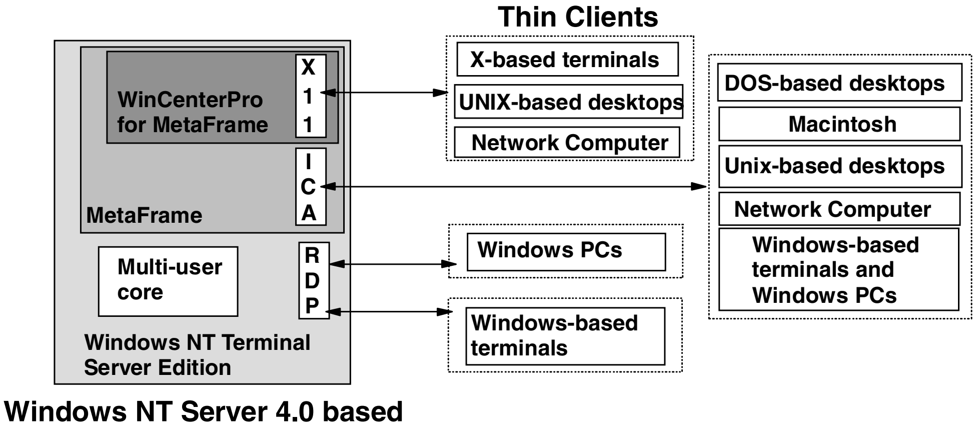


Figure 344. Windows NT Server 4.0 multi-user operating systems and add-on products overview

The Microsoft Windows NT Server 4.0 Terminal Server Edition is a derivative of NT Server 4.0 that includes the Citrix-developed multi-user extensions to the operating system for providing a multi-user Windows NT environment.

Windows NT Terminal Server Edition includes the Microsoft-developed RDP protocol. Windows NT Terminal Server Edition and the RDP protocol do not support such features as load balancing, shadowing (allowing a help desk to take control over a user's screen), audio, or printing to client-attached printers.

The supported client devices are only Windows-based desktops and Windows-based terminals.

Windows NT Terminal Server Edition requires one license for each device that is capable of accessing the Windows NT Terminal Server Edition server. If a company has 100 Network Stations, WBTs, PC, etc. that have the ability to access the server, but only 50 of them are currently in use, the company requires 100 licenses. The license used is a special Windows NT, Terminal Client Access License.

Citrix MetaFrame

MetaFrame is an add-on product for Windows NT Terminal Server Edition adding the ICA protocol and other well-known WinFrame features, such as audio, shadowing, and printing. Using MetaFrame, customers can connect to the Windows NT Terminal Server Edition server from a wide range of hardware devices, such as UNIX workstations and Network Computers, not only Windows-based desktops and Windows-based terminals. The ICA protocol also supports IPX and Netbios LAN protocols.

Just as WinFrame, MetaFrame uses a concurrent-user licensing scheme. In our previous example, with 100 clients, of which only 50 were simultaneously used, the customer only needs to purchase 50 MetaFrame licenses.

MetaFrame can also extend Windows NT Terminal Server Edition with additional functions and tools that provide greater manageability and scalability for a Windows NT multi-user environment. It delivers the following system, application, and user management tools:

- **Load Balancing and Published Application Manager utility**

  Load Balancing Services can be used with multiple Citrix servers (WinFrame, MetaFrame) to provide load balancing capabilities. Load balancing support lets you define, with the Published Application Manager utility, a remote application or desktop that runs on a predefined set of Citrix servers (“server farm”). The application or desktop is then called a published application or desktop. The application code must be installed on each Citrix server in the “server farm” for which the application is to be published.

  Instead of requesting a session to a specific Citrix server using the IP address of the server, the load balancing feature allows the client to request an application by its name. Then, the servers then decide which server is best suited to run this application at this particular moment.

  An overview of the Load Balancing services is shown in Figure 345.

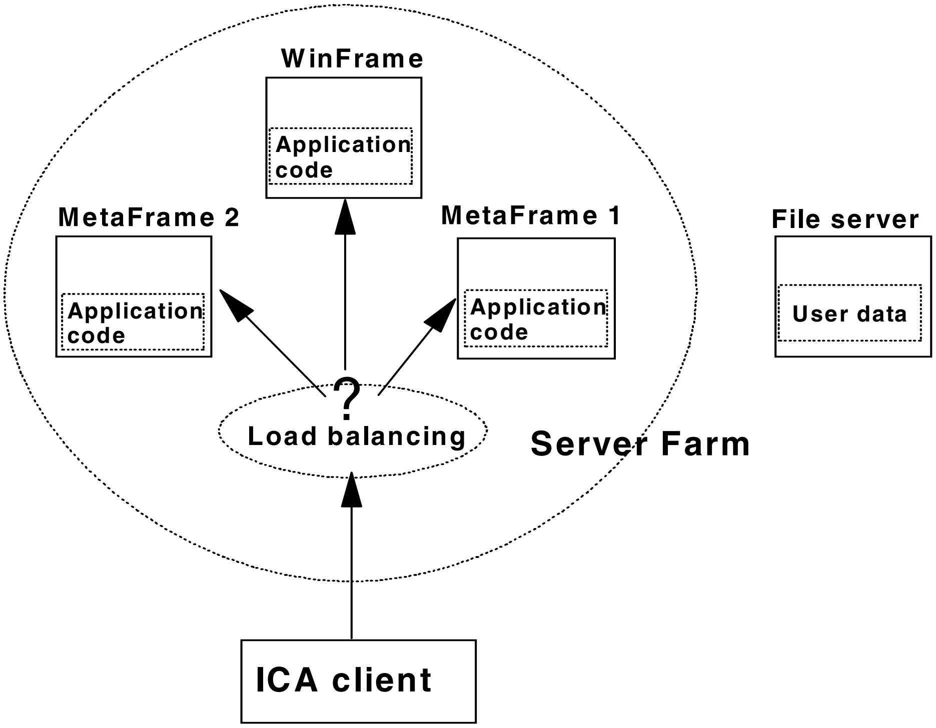


Figure 345. Citrix Load Balancing Services overview

When a user launches the remote published application or desktop from an ICA client, the load balancing software uses a tunable algorithm to select a server to execute the application or desktop. The load balancing parameters are configurable and can be tuned to provide maximum throughput and system availability.

In a load balanced server farm, one server is elected to the ICA Master Browser server. This server keeps track of all other servers, the applications that have been published on them, and the current load they have.

With Load Balancing Services, an administrator can simply add additional MetaFrame servers to the “server farm” for more scaleability. They can also take advantage of a sort of failover implementation, but only if the user data is stored on a separate file server and not on one of the MetaFrame servers. If one of the MetaFrame servers becomes unavailable, users connected to this server simply have to restart their ICA session. The Load Balancing service then redirects the new connections to another available server in the server farm running the same application the users were using. If the users' work is periodically and automatically saved on the file server, the users will only lose a small part of their work.

- **SecureICA Services**

  SecureICA Services offer end-to-end RSA RC5 encryption for the ICA data stream. This can be used when there are requirements for high security or when using the ICA protocol over the Internet.

- **Resource Management Services (RMS**)

  Citrix Resources Management Services provides the following features:

  - *Extensive audit trail*: A administrator can capture user connections and disconnections, track connection durations, and record what applications are used during user sessions. They can view the percentage of time applications are in use as opposed to just being loaded. Application resource requirements can be recorded to assist administrators with capacity planning.
  - *Comprehensive system monitoring*: This feature allows an administrator or a help desk to know about potential system problems before users start calling in. Over 30 real-time performance counters can be analyzed and displayed with status indicators.
  - *Ability to create detailed billing reports*: Based on the duration of user connections, the applications, the access, etc., RMS can create reports that can be used to bill the users' departments.

- **Installation Management Services (IMS)**

  Citrix Installation Management Services automates the application installation process so applications may be quickly and easily replicated to Citrix servers across the enterprise. It is the perfect complement to Citrix Load Balancing Services. When an application is installed onto one MetaFrame server, IMS can monitor the changes made to the server and then replicate all of these to the other servers in the farm. This greatly reduces the administrative burden of having a large server farm.

- **Session shadowing**

  Session shadowing allows administrators to take control of a single user or multiple users' sessions for support, diagnosis and training.

Citrix Device Services (CDS)

Citrix Device Services (CDS) is a Citrix OEM product that can be quickly and easily installed on top of Windows NT Terminal Server Edition servers. The product is free of charge if used with IBM Network Station. The CDS code delivered by IBM only supports IBM Network Stations.

CDS provides ICA connectivity, printing, and COM support. Using the ICA protocol, it also delivers increased application performance and network efficiency compared to Windows NT Terminal Server Edition native RDP protocol. It does not provide the advanced features of MetaFrame like load balancing, application publishing, audio support and session shadowing. CDS can be considered a "MetaFrame light" product.

Citrix CDS is directed toward customers who consider the functions found in Windows NT Terminal Server Edition are sufficient to meet their needs (for example, small business). The customer can always upgrade to a full MetaFrame for Terminals or MetaFrame Enterprise.

Tip

If you want to save money by using the CDS product, but don't want to give up the ability to have load balancing, you can setup a function similar to load balancing at no additional cost.

To do this, create a hostname entry, for example, `cdsserver`, in your DNS. Assign it multiple IP addresses, one for each of your CDS server (so each CDS server's IP address is listed once for this host name), so it becomes a round-robin entry in the DNS. Then configure the Network Station's ICA client to connect to the host cdsserver instead of a specific IP address. The DNS then redirects different users to different servers, spreading the load among the servers.

In NSM V1R3, make sure that the Network Station's TCP/IP cache is flushed frequently so it doesn't remember the IP address for the host name cdsserver, but looks it up for each new request. To do this, add the following line to the \nstation\prodbase\configs\defaults.dft file in an NSM V1R3 system:

```
set tcpip-name-cache-max-lifetime = 1
```

NCDi WinCenterPro for MetaFrame

NCDi WinCenterPro for MetaFrame is an add-on product installed on top of Windows NT Terminal Server Edition *and* MetaFrame. That is, it requires *both* Windows NT Terminal Server Edition and MetaFrame, it can not be installed onto Windows NT Terminal Server Edition as is.

The product adds X protocol support on the Windows NT multi-user server. Most of the MetaFrame features are supported except those that are ICA dependant like the load balancing services from Citrix. WinCenterPro for MetaFrame does not offer load balancing even for X-windows connections.

14.2.1.3 Additional information

Refer to the respective Microsoft, Citrix, and NCD Web sites for more information about these products:

- `http://www.microsoft.com`
- `http://www.citrix.com`
- `http://www.ncd.com`

14.3 Creating an ICA environment for Network Stations

In this section, we describe the different configuration options available for a Windows NT multi-user server that will be accessed by IBM Network Stations acting as Windows-based terminals.

The Network Station supports ICA and X display protocols, but not the RDP proprietary protocol. Therefore, the connection of a Network Station to a

Windows NT multi-user server requires at least the support of the ICA or X protocol on the server side. The most common protocol is the Citrix ICA protocol.

The configuration options are shown in Figure 346. A customer chooses among the different server configurations by determining the balance between their budget and their needs.

Although we have only introduced the Citrix WinFrame and MetaFrame products in the previous section, Citrix proposes different MetaFrame versions. Some of them are specific to network computers (Citrix Devices Services, MetaFrame for Terminals).

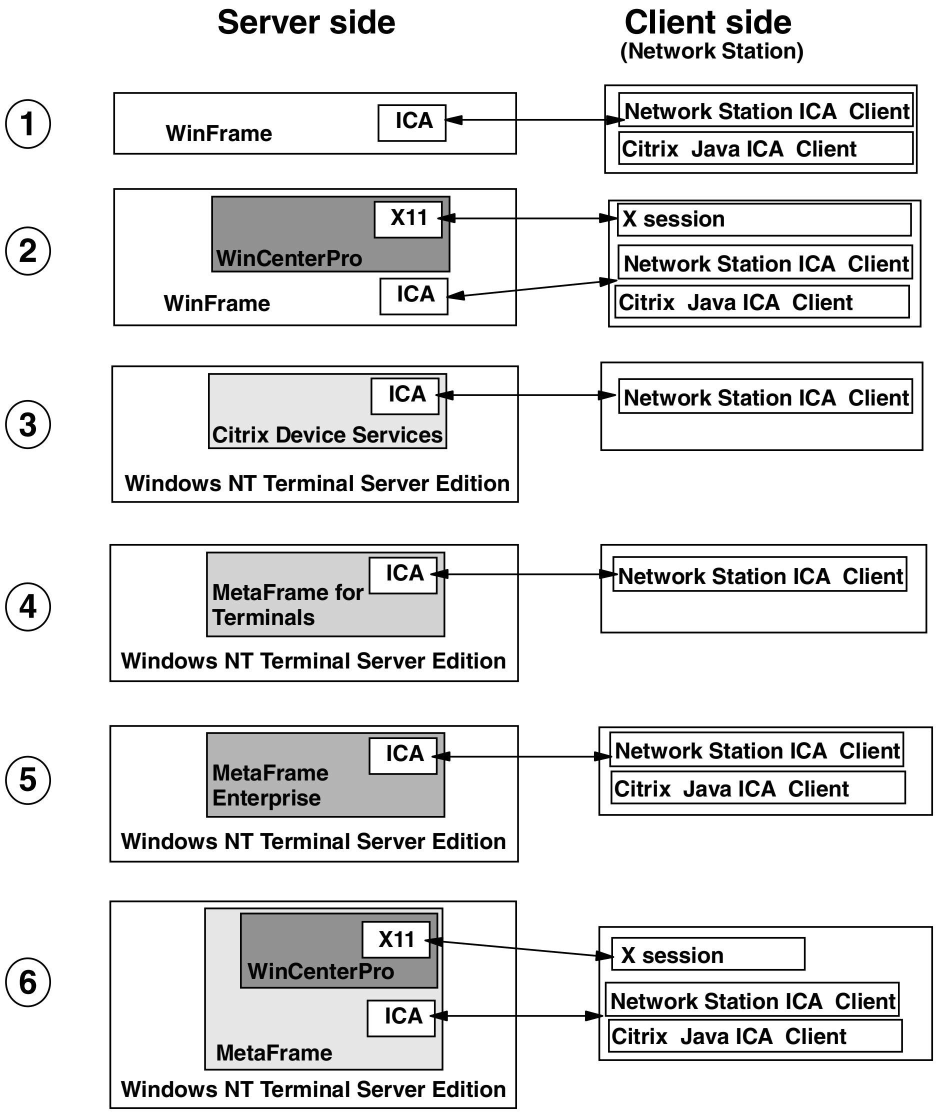

Server side
Client side
(Network Station)
1
WinFrame
ICA
Network Station ICA Client
Citrix Java ICA Client
2
X11
WinCenterPro
WinFrame
ICA
X session
Network Station ICA Client
Citrix Java ICA Client
3
ICA
Citrix Device Services
Windows NT Terminal Server Edition
Network Station ICA Client
4
ICA
MetaFrame for Terminals
Windows NT Terminal Server Edition
Network Station ICA Client
5
ICA
MetaFrame Enterprise
Windows NT Terminal Server Edition
Network Station ICA Client
Citrix Java ICA Client
6
X11
WinCenterPro
ICA
MetaFrame
Windows NT Terminal Server Edition
X session
Network Station ICA Client
Citrix Java ICA Client

Figure 346. Windows NT multi-user configuration options when accessed from a Network Station

14.3.1 The server side

This section offers a series of cases that illustrate different ways you can setup your environment.

Case 1: WinFrame

The user interface is Windows NT 3.51 based. The Network Stations use the ICA protocol to connect to the server. All the features and services from Citrix are available.

By choosing this product, customers will achieve consequent savings on the licenses compared to the Windows NT 4.0 interface solution, due to its concurrent-user licensing scheme.

Case 2: WinFrame and WinCenterPro

The user interface is Windows NT 3.51 based. The Network Stations use the ICA protocol or the X11 protocol to connect to the server.

All the features and services from Citrix are available for Network Stations connecting through the ICA protocol. The ICA dependant features are not available for Network Stations connecting through the X11 protocol, but load balancing is available.

The addition of WinCenterPro on top of WinFrame and the use of the X11 protocol will not improve the way a Network Station connects to a Windows NT multi-user server. On the contrary, it is an additional cost and functions are available.

However, if apart from Network Stations, you want to connect other X-based devices (for example, UNIX workstations) to the server and do not want to install an ICA client at these machines, WinCenterPro and the X11 display protocol is the right solution.

Case 3: Windows NT Terminal Server Edition and Citrix Device Services

The user interface is Windows NT 4.0 based. The Network Stations use the ICA protocol to connect to the server.

This is the most inexpensive solution for a customer to access the Windows NT Terminal Server Edition environment from a Network Station. It does not offer the advanced functions of the full MetaFrame product, but for some customers it may be adequate.

Also, if the customer outgrows the CDS product, they can easily purchase the full MetaFrame product, without losing any money on the CDS product. It’s free-of-charge if used with the Network Station.

Case 4: Windows NT Terminal Server Edition and MetaFrame for Terminals

The user interface is Windows NT 4.0 based. The Network Stations use the ICA protocol to connect to the server.

MetaFrame for Terminals is installed on top of Windows NT Terminal Server Edition Server. It is designed to host only Windows-based terminals from Citrix ICA OEM partners, including the IBM Network Station. All the MetaFrame features are supported.

A customer uses this solution if they do not plan to connect devices other than Windows-based terminals to the Windows NT multi-user environment, now or in the future. MetaFrame for Terminals is a lower cost alternative to the MetaFrame Enterprise version.

Case 5: Windows NT Terminal Server Edition and MetaFrame Enterprise

The user interface is Windows NT 4.0 based. The Network Stations use the ICA protocol to connect to the server.

MetaFrame Enterprise is installed on top of Windows NT Terminal Server Edition Server. This is the full version of the product. All Citrix supported thin clients can connect to MetaFrame Enterprise. The connection is not limited to Windows-based terminals from Citrix ICA OEM partners.

This solution is directed toward customers who want to connect to a Windows NT multi-user environment, as well Windows-based terminals (for example, IBM Network Station) as non-terminal client devices (Windows-based desktops, UNIX-based desktops, Macintosh, DOS-based desktops).

Case 6: Windows NT Terminal Server Edition, MetaFrame and WinCenterPro for MetaFrame

The user interface is Windows NT 4.0 based. The Network Stations use the ICA protocol or the X11 protocol to connect to the server.

All the features and services from Citrix are available for Network Stations connecting through the ICA protocol. The features that are ICA dependent are not available for Network Stations connecting through the X11 protocol.

The addition of WinCenterPro on top of MetaFrame and the use of the X11 protocol do not improve the way a Network Station connects to a Windows NT multi-user server. On the contrary, it is an additional cost and fewer functions are available.

However, if apart from Network Stations, you want to connect other X-based devices (for example, UNIX workstations) to the server and do not want to install an ICA client on these machines, WinCenterPro and the X11 display protocol is the right solution. X11 session does indeed not require a thin client software.

14.3.2 The client side

A network Station can connect to a Windows NT multi-user server via the ICA protocol and the X11 protocol. As we have seen, using ICA protocol offers more advantages and features than the X11 protocol and doesn’t require an additional product on the server. The ICA client can be considered the preferred thin client for the Network Station. Therefore, we only present here the Network Station ICA clients.

To connect to a Windows NT Terminal Server Edition-MetaFrame server, you can choose between two ICA clients on the Network Station; the Network Station’s own ICA client shipped with NSM and the Citrix Java ICA client.

The ICA client shipped with NSM is clearly the preferred choice in most current environments since it offers features not available in the Java ICA client. It is also tuned to run very well on the Network Station’s operating system. Its performance is better than the Java ICA client. However, the Java ICA client could be a suitable choice if you want to use the Netscape Communicator 4.5 browser as the main desktop (see 12.10, “Using the browser as the desktop to build a ‘Web-top’” on page 366) and display the Windows applications in a window within it, instead of a separate windows.

14.3.2.1 The Network Station ICA client

The ICA client shipped with NSM V2R1 is based on Citrix's UNIX ICA client code. IBM has enhanced the code with features that are missing from the Citrix UNIX ICA client.

You should consider the Network Station ICA client as the preferred ICA client because its settings can be centrally configured from Network Station Manager. Furthermore, it offers better performance and features than the ICA Java client and consumes much less memory on the Network Station.

14.3.2.2 The Citrix Java ICA client

Citrix's ICA client for Java (V4.11) allows users to access a Windows NT multi-user server from a Java Virtual Machine (JVM). The JVM can be any device running a JVM or a Web browser that supports Java applets.

The Java ICA client is another way to access a Windows NT multi-user server from a Network Station. It can be used as an applet running in the browser shipped with NSM V2R1, Netscape Communicator 4.5, or from the Network Station's JVM as a Java application.

Features

Version 4.11 of the ICA Java client supports the following features:

- Video resolutions up to 1280 x 1024
- Client printer mapping
- Event logging
- Hotkeys
- Client audio
- COM port mapping
- Business recovery
- Data compression
- Auto-reconnect
- Clipboard data exchange between local and remote desktops (raw textual data only, such as Unicode and ASCII text)
- Shadowing
- International keyboard support
- Multiple locale support
- Euro currency symbol support
- Program Neighborhood native GUI

Version 4.11 of the ICA Java Client does not support the following features commonly supported by other Citrix ICA clients:

- Persistent caching
- Encryption levels higher than Basic
- Color depths other than 256 colors
- Transport protocols other than TCP/IP
- Client drive mapping
- Seamless windows

14.4 ICA Network Station client configuration

An overview of the Network Station ICA client configuration is shown in Figure 347 on page 420.

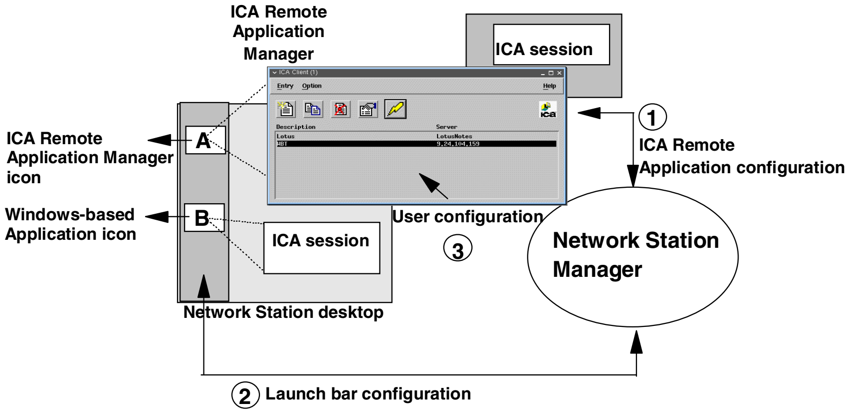


Figure 347. ICA client configuration overview

Using NSM, a system administrator can add either a single Windows-based application icon (B in Figure 347) or the ICA Remote Application Manager icon (A) in the Launch Bar.

When a Windows-based application icon is clicked, the ICA client is started on the Network Station. The ICA client then connects to a MetaFrame server and initiates a session according to the configuration done in NSM (2 in Figure 347).

When the ICA Remote Application Manager icon is clicked, the ICA Remote Application Manager is launched. It presents the end user with a list of MetaFrame servers and published applications to which they can connect. The list is created by the administrator from Network Station Manager (1 in Figure 347). When the end-user selects a MetaFrame server or published application, the ICA client is started on the Network Station. The ICA client then connects to the requested MetaFrame server and initiates a session according to the configuration done in NSM.

An administrator can also allow end users to create their own private connection entries when they use the ICA Remote Application Manager. The users then define new entries with the help of the ICA client Properties dialog box (3) in Figure 347.

Table 60 indicates where to configure each feature of the Network Station's ICA client. The advanced configuration means that you can only change a specific feature by modifying one of the files shipped with NSM.

Table 60. ICA Network Station client: Features configuration location

Features	NSM configuration	ICA command line	ICA Remote Application Manager	Windows NT multi-user server setup
User logon parameters	x	x	x	
Published applications and load balancing	x	x	x	x
Shadowing				x
Client printer mapping				x

Features	NSM configuration	ICA command line	ICA Remote Application Manager	Windows NT multi-user server setup
Client COM port mapping			x	x
Client audio mapping			x	x
Color, numbers of	x	x	x	
256 color Mapping			x	
Video resolution	x	x	x	
Data compression			x	
Bitmap caching			x	
Encryption	x	x	x	x

To illustrate the configuration process, we connect from the Network Station's ICA client to the Lotus Notes 5.0 client application that we will install and configure as a published application on a MetaFrame server.

Tip

Don't use Windows NT Terminal Server Edition or WinFrame screen savers on the Network Station. This will cause a lot of unnecessary graphics to be pushed over the LAN and consume valuable bandwidth. Always use the Network Station's local screen savers.

14.4.1 Windows NT multi-user server set up

This section leads you through a series of steps to help you understand how to set up a Windows NT multi-user server.

14.4.1.1 Application installation

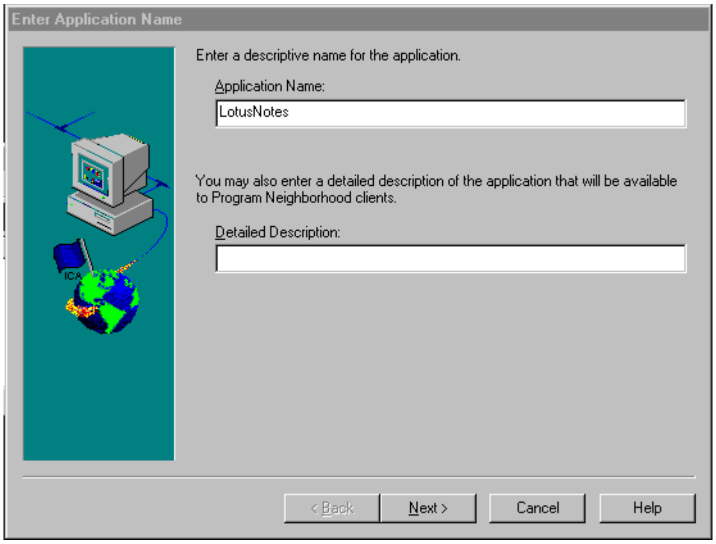
The installation of Lotus Notes 5.0 client on a server running Windows NT 4.0 Terminal Server Edition and MetaFrame 1.8 is covered in 15.1.2, "Lotus Notes Client Release 5.0" on page 487.

14.4.1.2 Application publishing

A published application is an application that has been defined to run on a predefined set of Citrix servers (server farm). ICA clients can be configured to directly access a specific published application (defined by its name). If the server farm contains more than one server, load balancing will select the server to execute the application.

The procedure to publish the Lotus Notes 5.0 client application is described here:

1. Log on to the MetaFrame server using a user name that is part of the Administrators group.
2. Select **Start->Programs->MetaFrame Tools->Published Application Manager**.
3. Select **Application->New**. The display shown in Figure 348 on page 422 appears.


Enter Application Name

Enter a descriptive name for the application.

Application Name: LotusNotes

You may also enter a detailed description of the application that will be available to Program Neighborhood clients.

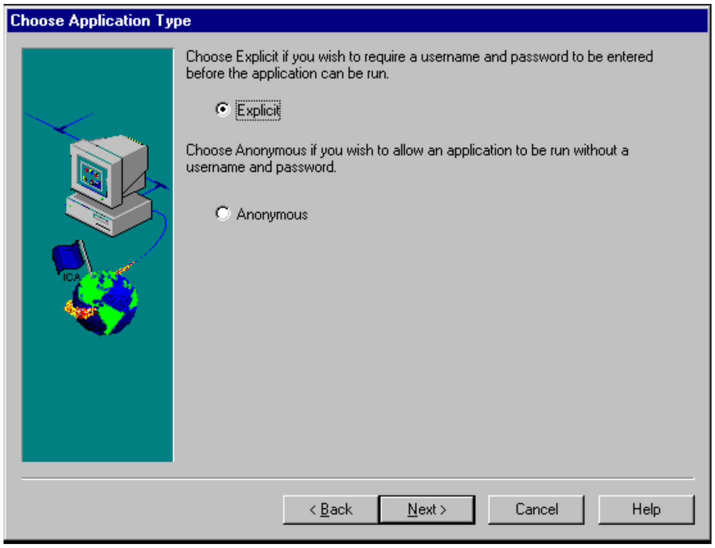
Detailed Description:

Figure 348. Published Application Manager: Enter Application Name panel

Enter a meaningful application name (for example, LotusNotes), and click **Next**. The display shown in Figure 349 appears.

Tip

Avoid using spaces and other “strange” characters, such as a question mark, comma, colon, or dots, for the name of a published application. Use only letters and digits. This will help ensure compatibility with other platforms.


Choose Application Type

Choose Explicit if you wish to require a username and password to be entered before the application can be run.

● Explicit

Choose Anonymous if you wish to allow an application to be run without a username and password.

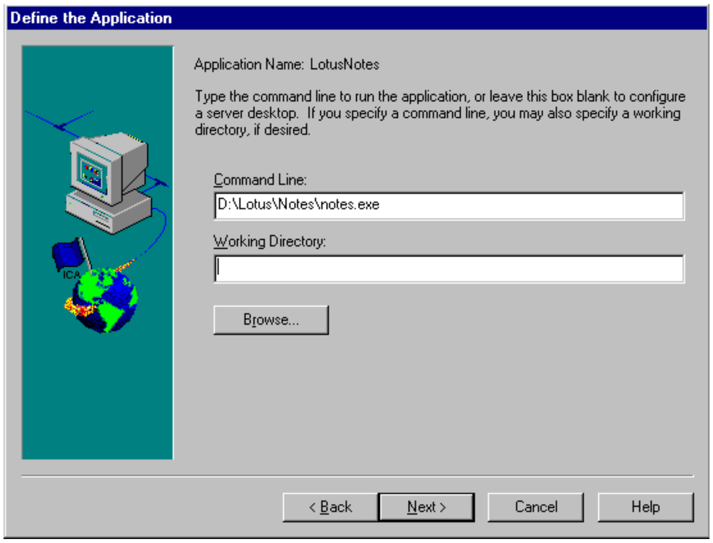
○ Anonymous

Figure 349. Published Application Manager: Choose Application Type panel

We choose the explicit type here because the system needs the user identity in order for the Lotus Notes user to access their home directory. The user home directory contains the user’s Notes data and notes.ini file. If we chose

Anonymous, one of MetaFrame's pre-defined anonymous user IDs would have been used. These are created during the MetaFrame installation. Refer to the MetaFrame publications for more information on anonymous user IDs.

4. Enter the application type, and click **Next**. The display shown in Figure 350 appears.



Define the Application

Application Name: LotusNotes

Type the command line to run the application, or leave this box blank to configure a server desktop. If you specify a command line, you may also specify a working directory, if desired.

Command Line: D:\Lotus\Notes\notes.exe

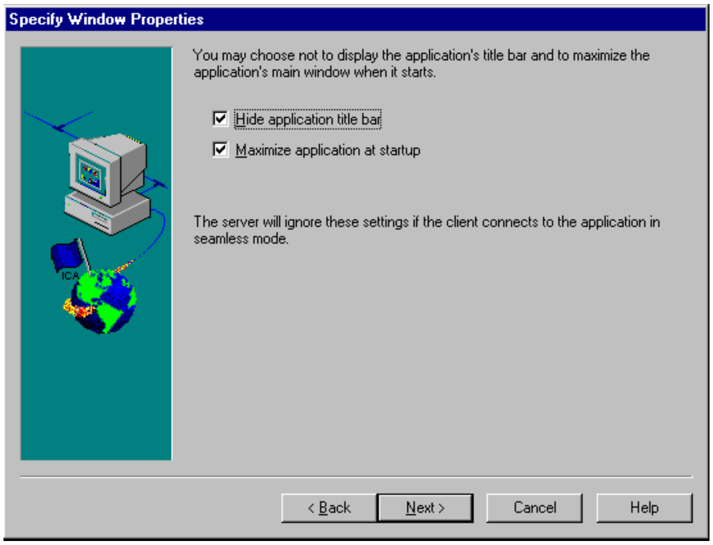
Working Directory:

Figure 350. Published Application Manager: Define the Application panel

5. The Lotus Notes executables are in the d:\Lotus\Notes directory in our example. The working directory does not need to be specified because it is defined in the notes.ini file of each user. Define the application, and click **Next**. Now, you see the panel in Figure 351 on page 424.

Tip

Leave the working directory and command line blank to give the user access to the Windows NT desktop.



Specify Window Properties

You may choose not to display the application's title bar and to maximize the application's main window when it starts.

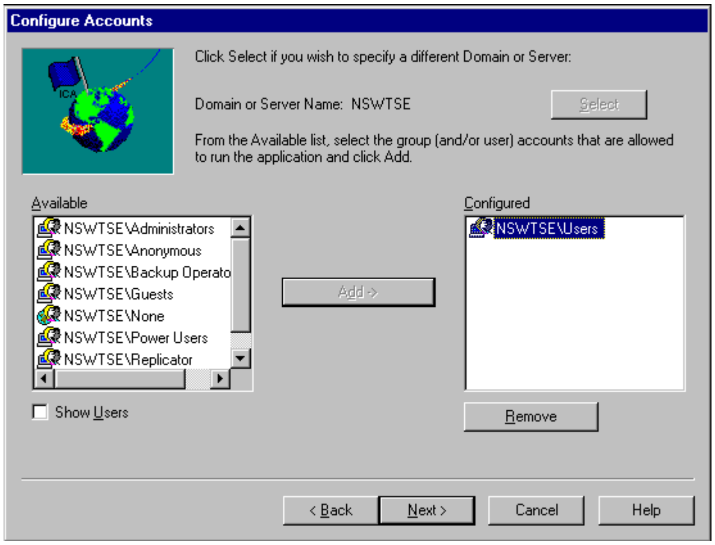
☑ Hide application title bar

☑ Maximize application at startup

The server will ignore these settings if the client connects to the application in seamless mode.

Figure 351. Published Application Manager: Specify Window Properties panel

6. Specify the Window Properties, and click **Next**.
7. Skip the Program Neighborhood Settings and Neighborhood Administration Features, and click **Next**. The Configure Accounts display appears (Figure 352).



Configure Accounts

Click Select if you wish to specify a different Domain or Server:

Domain or Server Name: NSWTSE

From the Available list, select the group (and/or user) accounts that are allowed to run the application and click Add.

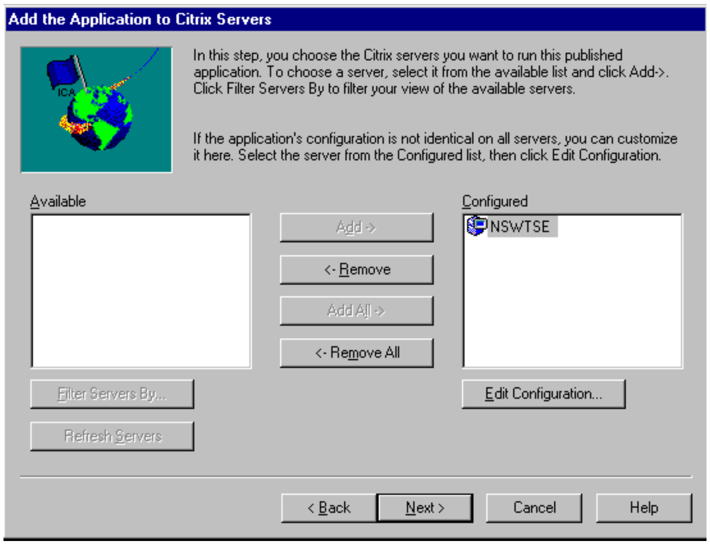
Available
- NSWTSE\Administrators
- NSWTSE\Anonymous
- NSWTSE\Backup Operato
- NSWTSE\Guests
- NSWTSE\None
- NSWTSE\Power Users
- NSWTSE\Replicator

Configured
- NSWTSE\Users

□ Show Users

Figure 352. Published Application Manager: Configure Accounts

8. Specify which users or group accounts are allowed to run the application. In our environment, all users can run the application. Click **Next**. See Figure 353.


Add the Application to Citrix Servers

In this step, you choose the Citrix servers you want to run this published application. To choose a server, select it from the available list and click Add->. Click Filter Servers By to filter your view of the available servers.

If the application's configuration is not identical on all servers, you can customize it here. Select the server from the Configured list, then click Edit Configuration.

Figure 353. Published Application Manager: Add the Application to Citrix Servers panel

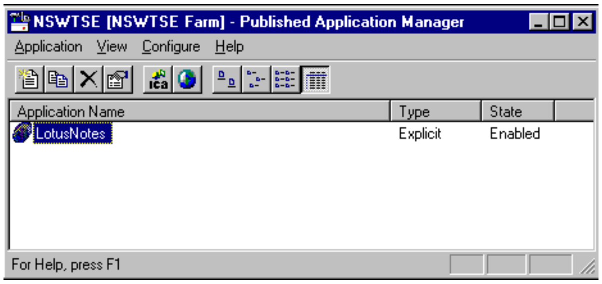
9. Choose the MetaFrame servers on which you want to run the published application. Click **Next**, and then click **Finish**.

   If you want the application to be published for execution on multiple servers, the Load Balancing Services license and the application code must be installed on each of these servers.

   In our example, we have only published Lotus Notes on the single server nswtse because we only have one MetaFrame server in our environment. The Load Balancing Services license is, therefore, not necessary.

Our configuration does not allow us to take advantage of the Load Balancing Services. However, it is sufficient to illustrate how to configure the Network Station's ICA client to access a published application that would have been defined on multiple servers.

Our application is now published and its name, LotusNotes, has been added to the Published Application Manager's list (Figure 354).


NSWTSE [NSWTSE Farm] - Published Application Manager

Application Name	Type	State
LotusNotes	Explicit	Enabled

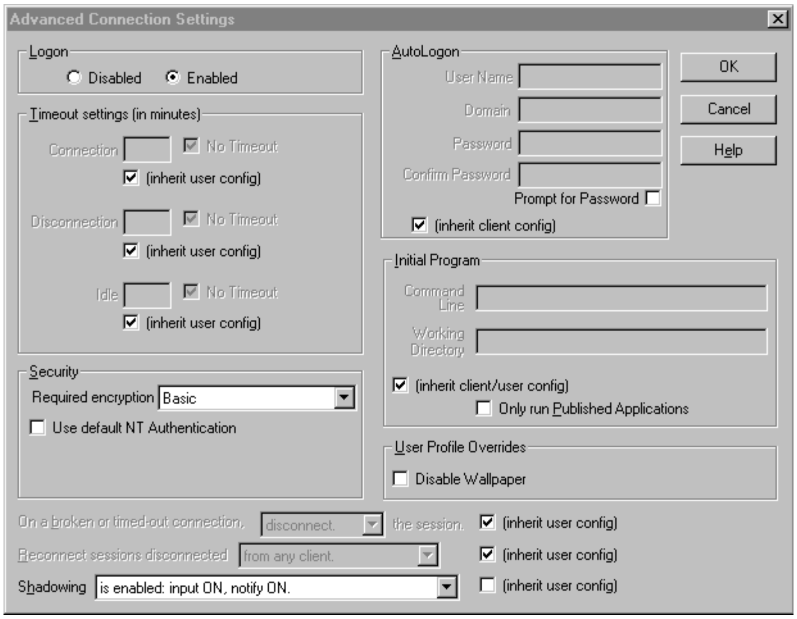
For Help, press F1

Figure 354. Published Application Manager list

14.4.1.3 Shadowing

To specify whether sessions can be shadowed, modify the Advanced Connections settings as described in the following steps:

1. Select **Start->Programs->MetaFrame Tools->Citrix Connections Configuration**.
2. Select the **ica-tcp Connection Name**, and double click.
3. Click the **Advanced** button. The Advanced Connection Settings panel appears (Figure 355).



Logon
○ Disabled ● Enabled

Timeout settings (in minutes)
Connection ☑ No Timeout
☑ (inherit user config)
Disconnection ☑ No Timeout
☑ (inherit user config)
Idle ☑ No Timeout
☑ (inherit user config)

Security
Required encryption Basic
□ Use default NT Authentication

AutoLogon
User Name
Domain
Password
Confirm Password
Prompt for Password □
☑ (inherit client config)

Initial Program
Command Line
Working Directory
☑ (inherit client/user config)
□ Only run Published Applications

User Profile Overrides
□ Disable Wallpaper

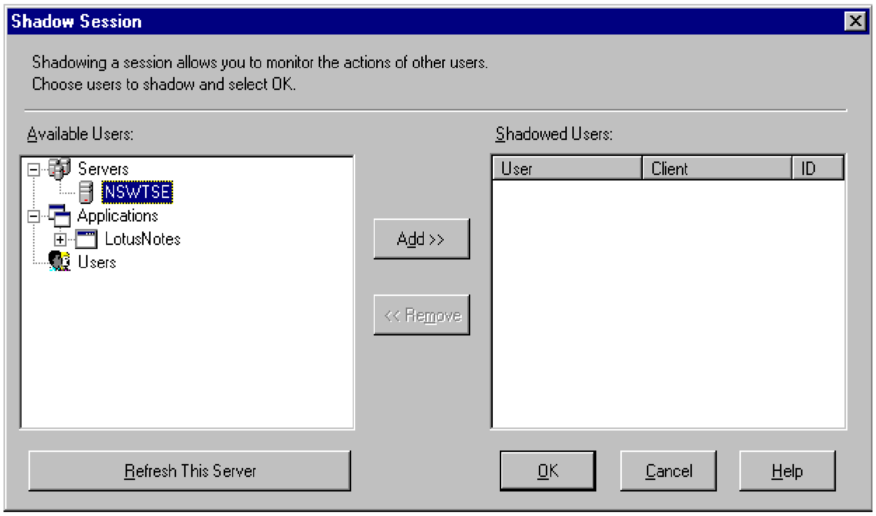
On a broken or timed-out connection, disconnect. the session. ☑ (inherit user config)
Reconnect sessions disconnected from any client. ☑ (inherit user config)
Shadowing is enabled: input ON, notify ON. □ (inherit user config)

Figure 355. Advanced Connection Settings panel

4. Specify one of the shadowing modes on the Advanced Connection Settings panel:
   - Click **is disabled** to disable shadowing of sessions.
   - Click one of the **input ON** values to allow the shadower to input keyboard and mouse actions to the shadowed session.
   - Select one of the **notify ON** values to cause the shadowed user to get a popup asking if it is oK for the shadowing to occur.

To access one or multiple sessions by shadowing, complete the following steps to start the Shadow Session panel:

1. Log on to the MetaFrame server using a user name that is part of the Administrator group.
2. Select **Start->Programs->MetaFrame Tools->Shadow Task Bar**.
3. Enter your administrator password (the first time only).
4. Click the **Shadow** button of the Shadow Task Bar. The Shadow Session panel appears (Figure 356).


Shadow Session

Shadowing a session allows you to monitor the actions of other users.
Choose users to shadow and select OK.

Figure 356. Shadow Session panel

From the Shadow Session panel, select a user session you want to shadow.

14.4.1.4 Client printer mapping

To give a user access from an ICA session to the printer attached to their Network Station, follow the steps described in 14.7.3, “Connecting to local printers” on page 476.

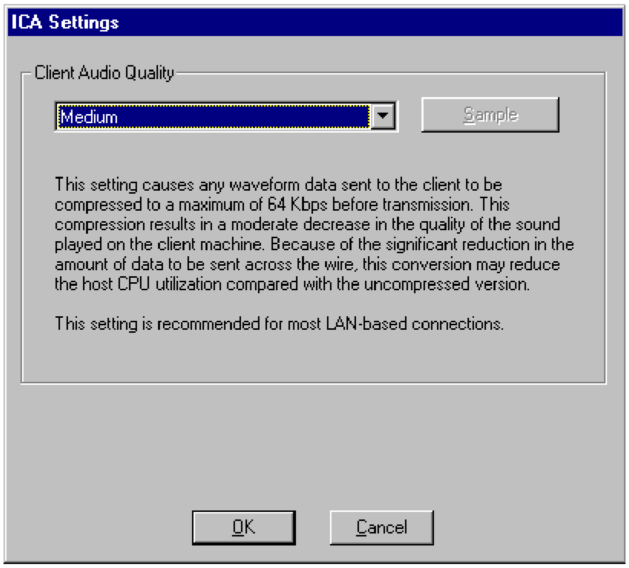
14.4.1.5 Client COM port mapping

See 14.7.4, “Connecting to local serial devices” on page 477, for more information.

14.4.1.6 Client audio mapping

To specify the audio quality received by the ICA clients, modify the ICA Settings as instructed in the following steps:

1. Select **Start->Programs->MetaFrame Tools->Citrix Connections Configuration**.
2. Select **ica-tcp Connection Name**, and double-click.
3. Click the **ICA Settings** button, and the ICA Settings display appears (Figure 357 on page 428).



This setting causes any waveform data sent to the client to be compressed to a maximum of 64 Kbps before transmission. This compression results in a moderate decrease in the quality of the sound played on the client machine. Because of the significant reduction in the amount of data to be sent across the wire, this conversion may reduce the host CPU utilization compared with the uncompressed version.

This setting is recommended for most LAN-based connections.

Figure 357. ICA Settings panel

4. Choose one of the audio quality modes on the ICA Settings panel:
   - Low audio quality causes any waveform data sent to the client to be compressed to a maximum of 16 Kbps before transmission.
   - Medium audio quality causes any waveform data sent to the client to be compressed to a maximum of 64 Kbps before transmission.
   - High audio quality allows clients to play any waveform data at its native data rate.

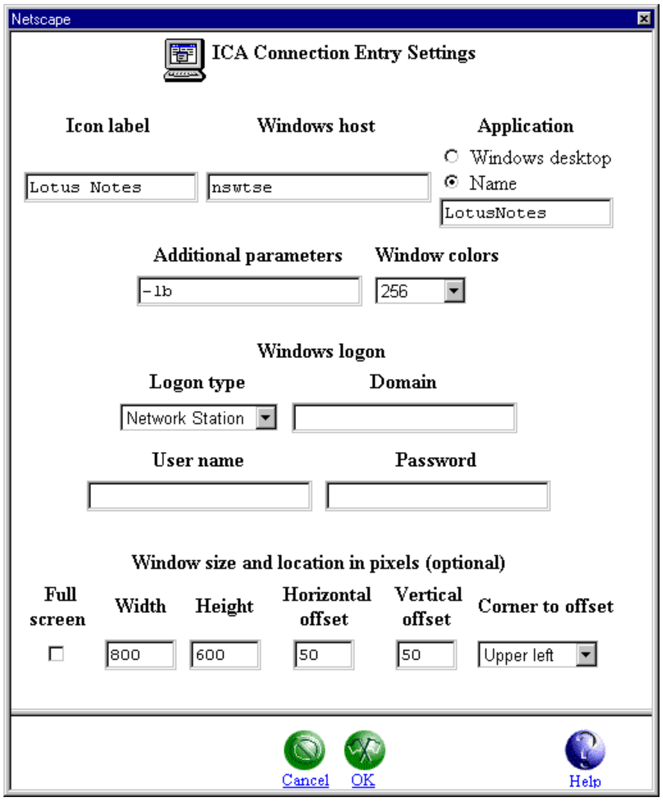
14.4.2 NSM configuration

Now that ICA parameters have been set up on the Windows NT multi-user server, we can configure Network Station ICA sessions from Network Station Manager.

14.4.2.1 ICA Remote Application Manager configuration

To define the ICA connections for use by the Network stations (refer back to Figure 347 on page 420), begin by creating the list of MetaFrame server connections shown by the ICA Remote Application Manager. To do this, complete these steps:

1. Log on to the NSM using a user name that is part of the NSMAdmin group.
2. Select the preference level.
3. Select **Applications->ICA Remote Application Manager**.
4. Click **Add** to configure a new ICA connection entry with the ICA Connection Entry Settings panel (Figure 358).



ICA Connection Entry Settings

Icon label: Lotus Notes

Windows host: nswtse

Application:
○ Windows desktop
● Name
LotusNotes

Additional parameters: -lb

Window colors: 256

Windows logon

Logon type: Network Station

Domain:

User name:

Password:

Window size and location in pixels (optional)

Full screen	Width	Height	Horizontal offset	Vertical offset	Corner to offset
□	800	600	50	50	Upper left

Figure 358. ICA Connection Entry Settings panel

5. The configuration shown defines a connection to the Lotus Notes Client Published Application on the server nswtse. Click **OK** to add your configuration to the ICA Remote Application Manager list.

The following list identifies and describes the fields for the ICA connection:

- **Icon label (Lotus Notes)**: The text in this field is the label that appears on the list of ICA connections provided by the ICA Remote Application Manager.
- **Windows host (nswtse)**: Type either the IP address or the host name of the Windows NT multi-user server on which you want to launch the Windows-based application.
- **Application (Name : LotusNotes)**: This field determines what the user sees after logon. The possible values are:
  - Windows desktop: The full Windows NT desktop
  - Name: An application

    You can type the name of a published application (same name as in Figure 348 on page 422) or the path and name of an application executable on the server.

    To access a published application, you must add the load balancing (-lb) parameter on the Additional Parameters field (even if the Load Balancing Services license is not installed on the server).

    To access an application executable, if any backslash (\) characters are used in any input fields, you need to use two.

For example, to access the Lotus Notes application executable, you should type:

```
d:\\Lotus\\Notes\\notes.exe
```

- **Additional parameters**: You can specify one or more command line parameters in this field. See 14.4.4.3, “Command line interface” on page 456, for full details.
- **Windows colors (256)**: The Window colors field determines the amount of color support. Possible values are 16 (default) and 256.
- **Windows logon (Network Station)**: You must choose one of the following logon types:
  - **Manual**: The PC server prompts the user for their login information (PC server user ID, password, and domain name) when the Windows-based session is launched at the Network Station.
  - **Automatic**: The PC server does not prompt the user for their login information when the Windows-based session is launched at the Network Station.

    You must complete the login information (domain, user name, and password) fields if you select Automatic. The login information specified will be passed to the PC server, and the user will automatically be logged in.
  - **Network Station**: The PC server does not prompt the user for their login information when the Windows-based session is launched at the Network Station. You may specify the domain name (optional) if you select Network Station. The user ID and password used to log into the network station will be passed to the PC server (along with the domain name if one was specified), and the user will automatically be logged in.

  The password is not stored or transmitted to the PC server in clear text.
- **Windows size and location in pixels (800x600)**: This function, if used, allows you to specify the size and location of the window for a Windows-based session. The following fields define the size of the window (width and height) and the window's position on the monitor (Horizontal and Vertical offset and Corner to offset from):
  - **Full screen (default)**: Selecting this box enables the Windows-based application to use the whole screen on the Network Station. Full screen does not include the Launch Bar area.
  - **Width**: This value determines the horizontal width of the window.
  - **Height**: This value determines the vertical height of the window.
  - **Horizontal offset**: This value determines the horizontal distance from whatever corner is specified as the Corner to offset value (for example, Upper left).
  - **Vertical offset**: This value determines the vertical distance from whatever corner is specified as the Corner to offset value (for example, Upper left).
  - **Corner to offset**: This value determines from which corner (Upper left, upper right, lower left, or lower right) the values from the Horizontal and Vertical offset fields are applied.

Once the new connection entry is saved, it is added to the ICA Connections Entries listed on the ICA Remote Applications Manager Settings panel are shown in (Figure 359).

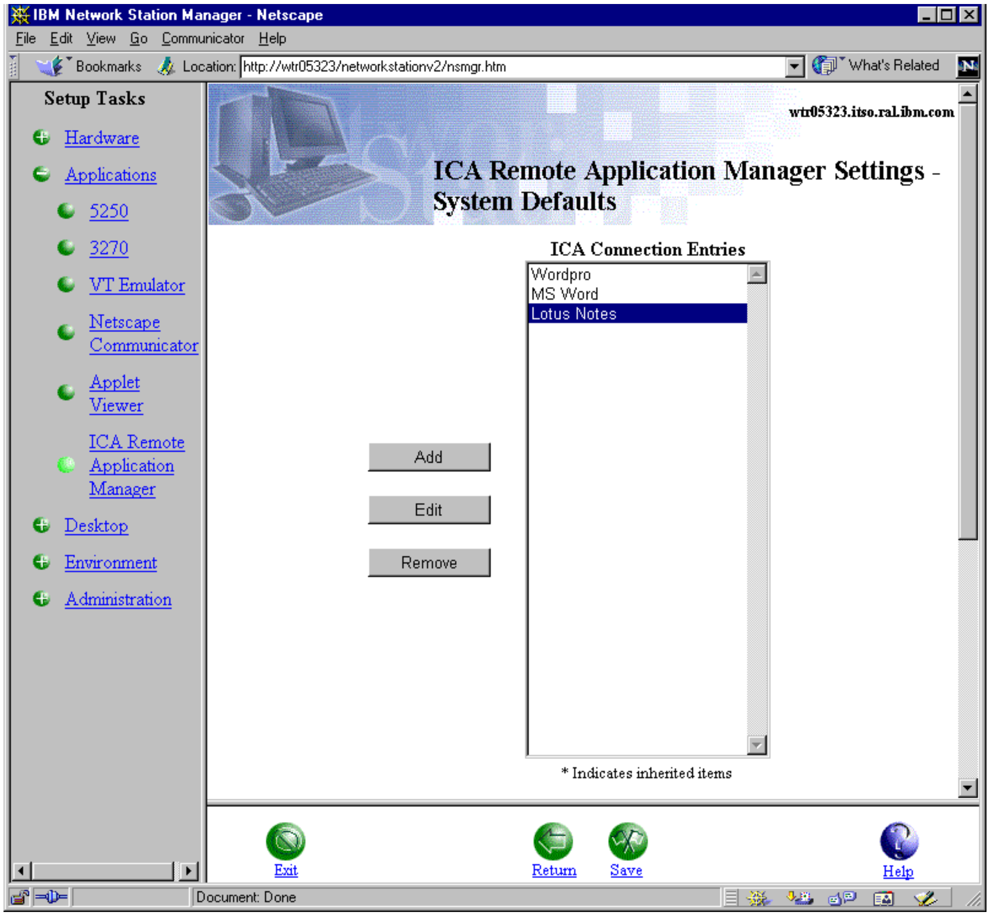
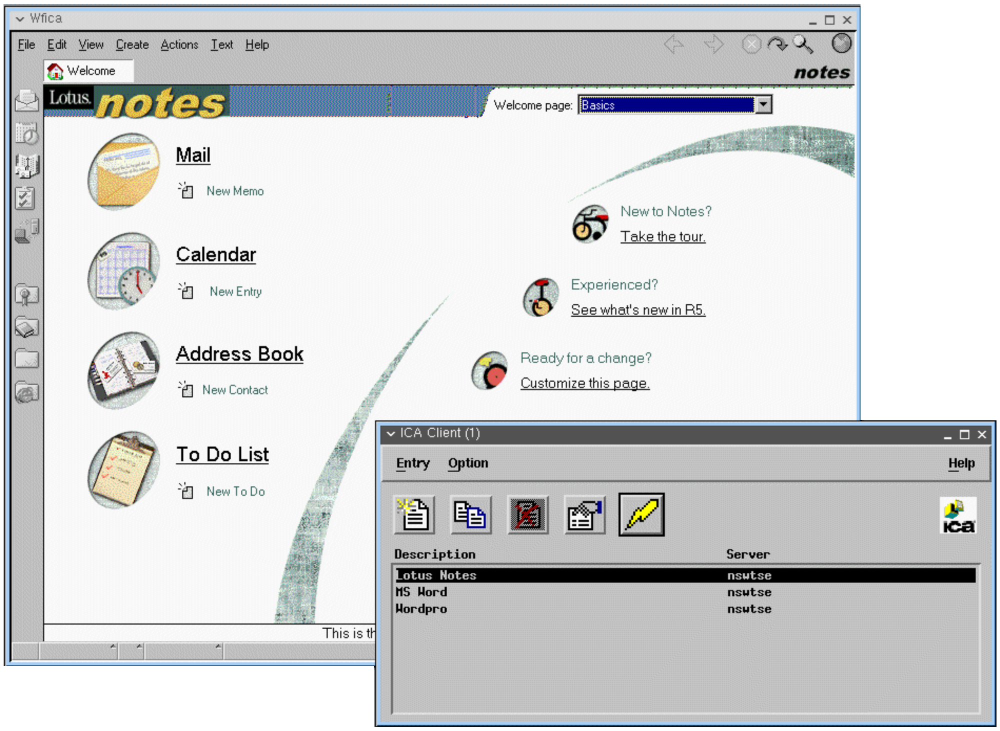

IBM Network Station Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://wtr05323/networkstationv2/nsmgr.htm
What's Related
Setup Tasks
Hardware
Applications
5250
3270
VT Emulator
Netscape Communicator
Applet Viewer
ICA Remote Application Manager
Desktop
Environment
Administration
wtr05323.itso.ral.ibm.com
ICA Remote Application Manager Settings - System Defaults
ICA Connection Entries
Wordpro
MS Word
Lotus Notes
Add
Edit
Remove
* Indicates inherited items
Exit
Return
Save
Help
Document: Done

Figure 359. ICA Remote Applications Manager Settings panel

Figure 360 on page 432 shows how the ICA Remote Application Manager and the Lotus Notes session look on the Network Station desktop.



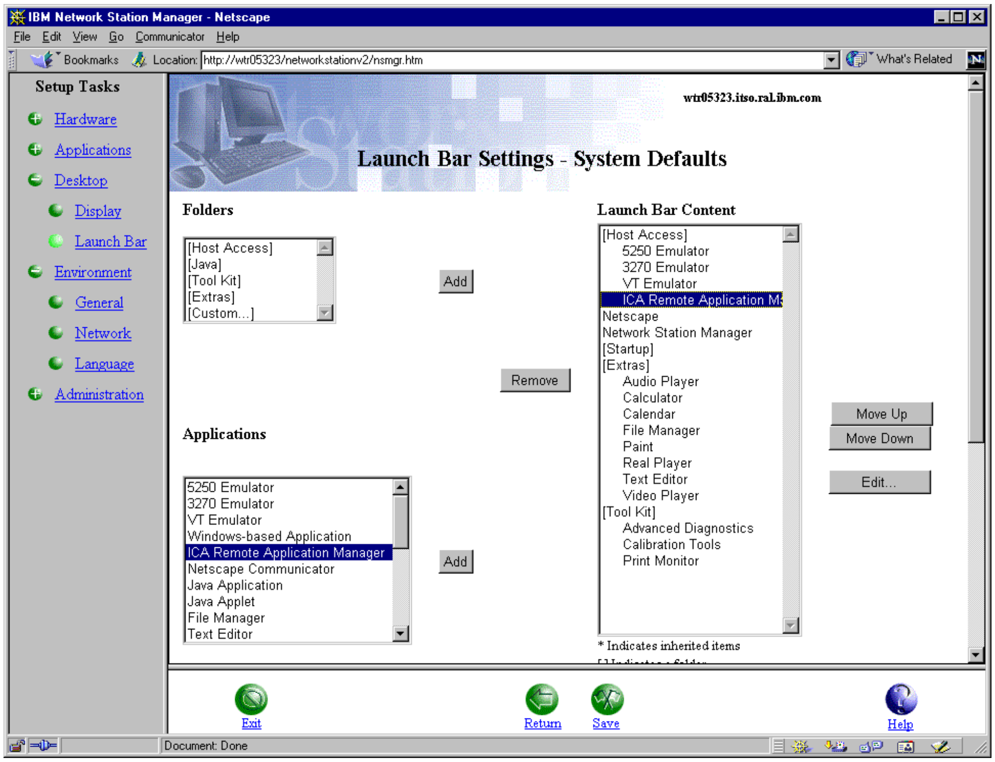
```
Description                                  Server
Lotus Notes                                  nswtse
MS Word                                      nswtse
Wordpro                                      nswtse
```

Figure 360. ICA Remote Application Manager and Lotus Notes ICA session on the Network Station

14.4.2.2 ICA Remote Application Manager Launch Bar icon

Next we have to add the ICA Remote Application Manager icon to the Network Station Launch Bar so the users can to be able to launch the ICA Remote Application Manager. Complete these steps:

1. Log on to the NSM using a user name that is part of the NSMAdmin group.
2. Select the preference level.
3. Select **Desktop->Launch Bar** (Figure 361).



Launch Bar Settings - System Defaults

Folders

[Host Access]
[Java]
[Tool Kit]
[Extras]
[Custom...]

Applications

5250 Emulator
3270 Emulator
VT Emulator
Windows-based Application
ICA Remote Application Manager
Netscape Communicator
Java Application
Java Applet
File Manager
Text Editor

Launch Bar Content

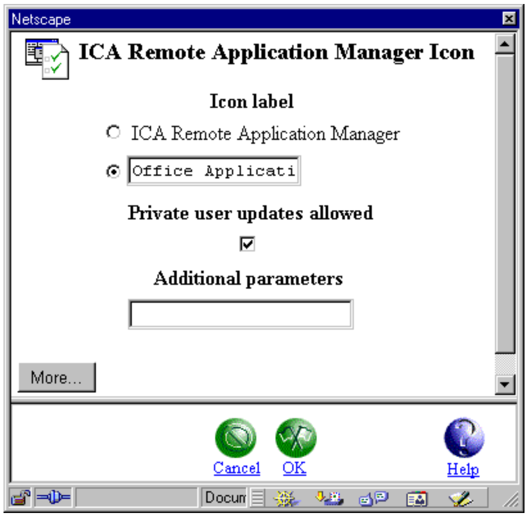
[Host Access]
 5250 Emulator
 3270 Emulator
 VT Emulator
 ICA Remote Application M
Netscape
Network Station Manager
[Startup]
[Extras]
 Audio Player
 Calculator
 Calendar
 File Manager
 Paint
 Real Player
 Text Editor
 Video Player
[Tool Kit]
 Advanced Diagnostics
 Calibration Tools
 Print Monitor

* Indicates inherited items

Figure 361. Launch Bar settings

4. From the Applications List Box, select **ICA Remote Application Manager**.
5. From the Launch Bar Content List Box, select the place where you want to insert the application you selected.
6. Click the **Add** button to add the ICA Remote Application Manager to the Launch Bar Content List box.

We can configure the ICA Remote Application Manager Launch Bar icon using the ICA Remote Application Manager Icon panel shown in Figure 362.



ICA Remote Application Manager Icon

Icon label

○ ICA Remote Application Manager

● Office Applicati

Private user updates allowed

☑

Additional parameters

Figure 362. ICA Remote Application Manager Icon

The procedure to access this panel is:

1. Select the **ICA Remote Application Manager** bar item from the Launch Bar Content List Box.
2. Click the **Edit** button.

The following list identifies and describes the fields for the ICA Remote Application Manager Icon:

- **Icon label (Office Applications)**: The text in this field is the label that appears under the icon when the icon is viewed in the Network Station's Launch Bar. You have two choices for the icon label:
  - ICA Remote Application Manager (the default)
  - Create your own label
- **Private user updates allowed**: This field allows users to create their own private connection entries when they use the ICA Remote Application Manager. Deselect the **Private user updates allowed** box if you do not want users to create their own ICA connection entries.
- **Additional parameters**: See 14.4.4.3, “Command line interface” on page 456, for details.

Figure 363 shows the Network Station launch bar including the Remote Application Manager labelled “Office Applications” in the Host Access folder.

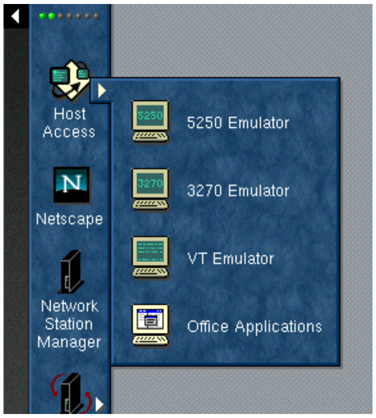


Figure 363. Network Station Launch Bar

14.4.2.3 Windows-based application Launch Bar icon

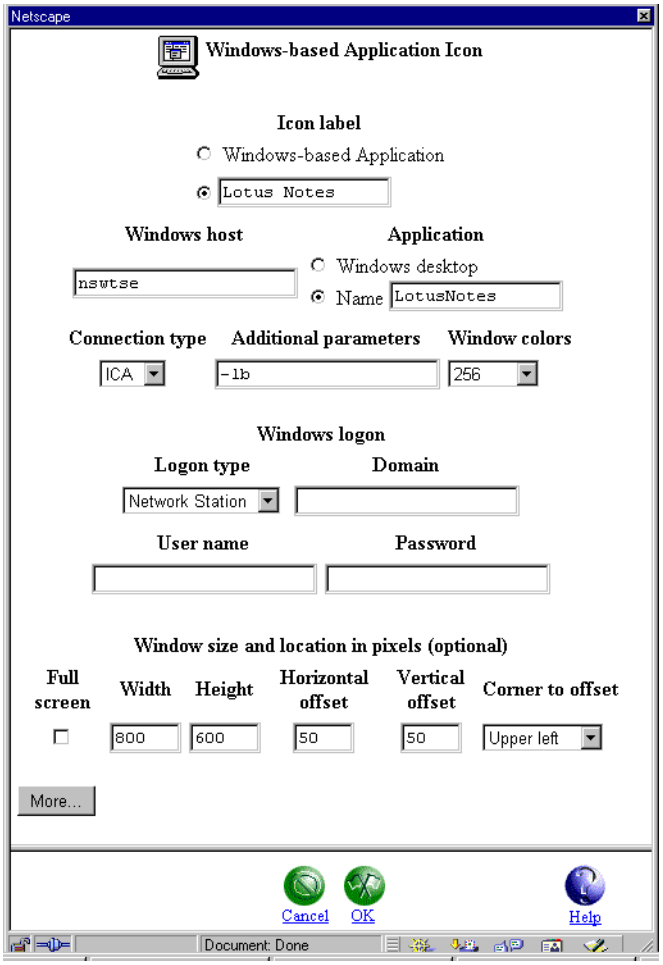
If you want to directly add an ICA connection entry icon to the Launch Bar instead of using the Remote Application Manager, use this method. You must first add a Windows-based Application Launch Bar item to the Launch Bar Content List Box. This is done the same way as when we added the ICA Remote Applications Manager Launch Bar item.

You then have to configure the Windows-based Application Launch Bar item using the Windows-based Application Icon panel.

Complete the following procedure to access this panel:

1. Select the Windows-based Application from the Launch Bar Content List Box (see Figure 361 on page 433).

2. Click the **Edit** button. See the display in Figure 364.



Netscape

Windows-based Application Icon

Icon label

○ Windows-based Application

● Lotus Notes

Windows host

nswtse

Application

○ Windows desktop

● Name LotusNotes

Connection type

ICA

Additional parameters

-lb

Window colors

256

Windows logon

Logon type

Network Station

Domain

User name

Password

Window size and location in pixels (optional)

Full screen	Width	Height	Horizontal offset	Vertical offset	Corner to offset
□	800	600	50	50	Upper left

Figure 364. Windows-based Application Icon panel

The configuration fields are the same as the ICA connection entry settings panel. There is only one additional field, *Connection type*. This field determines what protocol you want to use to connect to your PC server. The possible values are:

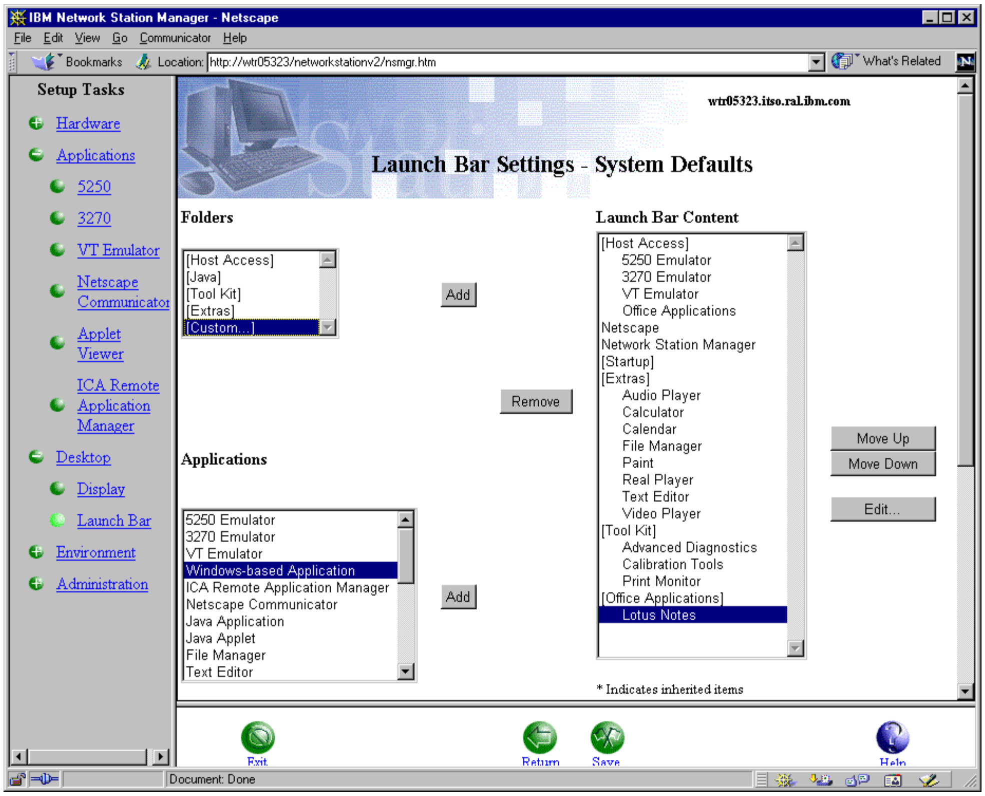
- **ICA**: Use the ICA protocol to connect to the MetaFrame server.
- **X11**: Use the X11 protocol to connect to a WinFrame server with WinCenterPro or a MetaFrame server with WinCenterPro for MetaFrame.

For the of X11 protocol, the ICA-related parameters introduced in the next section (such as -lb, -encryption) do not apply any more.

We have added the Windows-based Application item labelled Lotus Notes into a new folder called Office Applications. The modified Launch Bar Settings panel is shown in Figure 365.

To add a new folder on the Launch Bar, complete these tasks:

1. Select **Customize** in the Folders list, and click **Add**.
2. Enter a label for the new folder.



IBM Network Station Manager - Netscape

File Edit View Go Communicator Help

Bookmarks Location: http://wtr05323/networkstationv2/nsmgr.htm What's Related

Setup Tasks

- Hardware
- Applications
  - 5250
  - 3270
  - VT Emulator
  - Netscape Communicator
  - Applet Viewer
  - ICA Remote Application Manager
- Desktop
  - Display
  - Launch Bar
- Environment
- Administration

wtr05323.itso.ral.ibm.com

Launch Bar Settings - System Defaults

Folders

```
[Host Access]
[Java]
[Tool Kit]
[Extras]
[Custom...]
```

Applications

```
5250 Emulator
3270 Emulator
VT Emulator
Windows-based Application
ICA Remote Application Manager
Netscape Communicator
Java Application
Java Applet
File Manager
Text Editor
```

Launch Bar Content

```
[Host Access]
    5250 Emulator
    3270 Emulator
    VT Emulator
    Office Applications
Netscape
Network Station Manager
[Startup]
[Extras]
    Audio Player
    Calculator
    Calendar
    File Manager
    Paint
    Real Player
    Text Editor
    Video Player
[Tool Kit]
    Advanced Diagnostics
    Calibration Tools
    Print Monitor
[Office Applications]
    Lotus Notes
```

* Indicates inherited items

Document: Done

Figure 365. Launch Bar Settings panel

Figure 366 shows the Network Station Launch Bar including a Windows-based application icon Lotus Notes in the Office Applications folder.

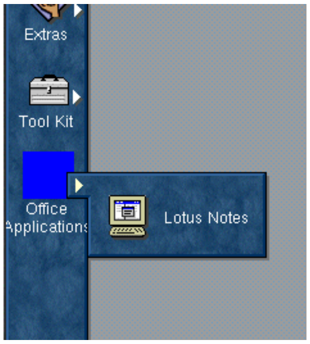


Figure 366. Network Station Launch Bar

14.4.3 Using the ICA Remote Application Manager

This section explains how to use and understand the ICA Remote Application Manager.

14.4.3.1 Quick start

To connect to a Citrix server, you need a user name and password set up for you on the server. You also need to know the name of the server and domain.

14.4.3.2 Starting the ICA Remote Application Manager

From the Launch Bar, select **Host Access->ICA Remote Application Manager**.

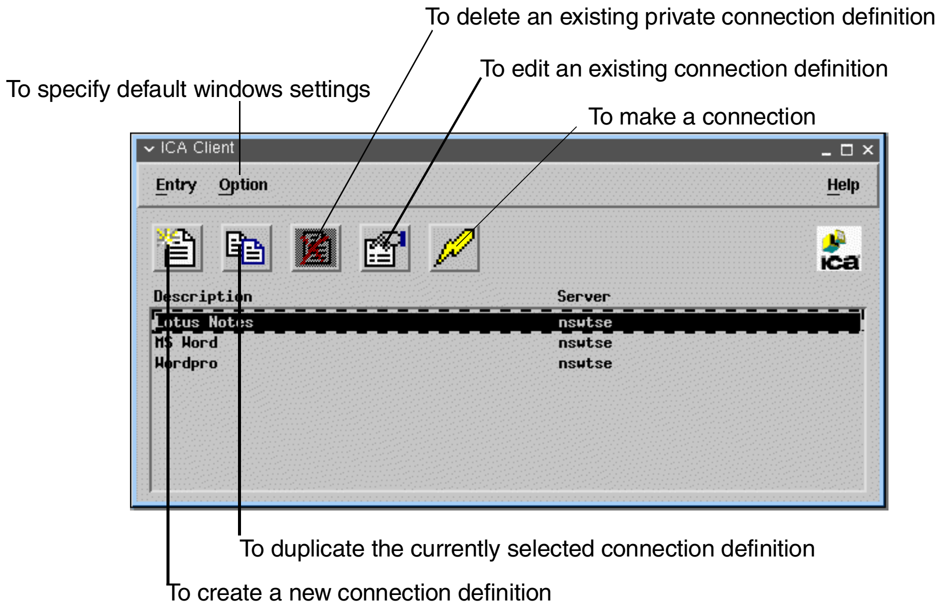
Or, from the command line, type the following command:

```
/usr/lib/ICAClient/wfcmgr
```

Here, `/usr/lib/ICAClient` is the directory in which you installed the ICA Remote Application Manager.

Note: If the ICA Remote Application Manager was not installed in the default installation directory, ensure that the environment variable ICAROOT is set to point to the actual installation directory.

The ICA Remote Application Manager window appears as shown in Figure 367.



Description	Server
Lotus Notes	nswtse
MS Word	nswtse
Wordpro	nswtse

To delete an existing private connection definition

To edit an existing connection definition

To specify default windows settings

To make a connection

To duplicate the currently selected connection definition

To create a new connection definition

Figure 367. ICA Remote Application Manager window

14.4.3.3 Defining a connection

Note: If Network Station Manager was used to define ICA connection entries, the entries will be displayed. You may go to the next section. To open a connection or continue with defining a new connection entry. To define a connection, follow these steps:

1. Choose **New...** from the Entry menu, or click the **New Entry** icon.
2. The Properties dialog box is displayed as shown in Figure 368 on page 438 to allow you to define a new connection.

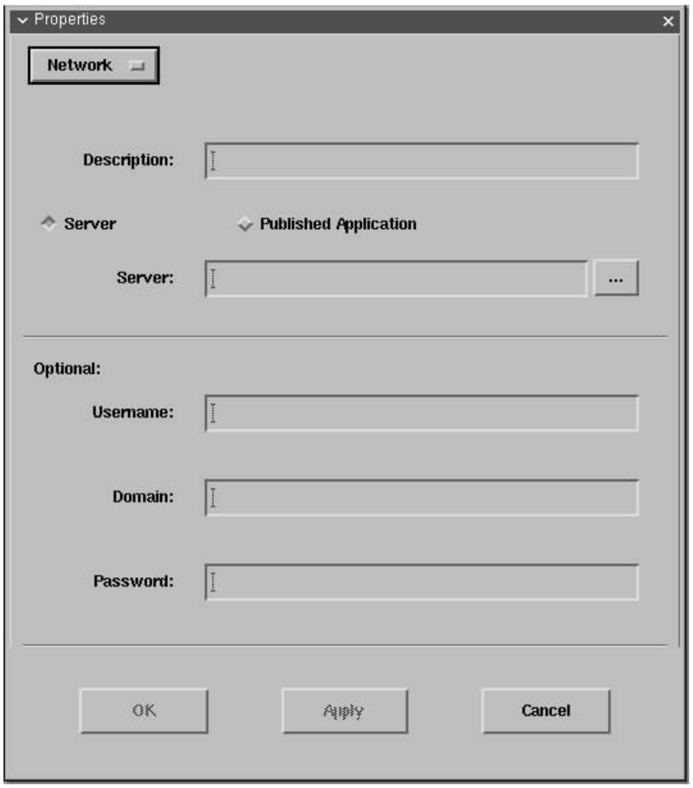


Figure 368. Properties dialog box

3. Edit the Description to describe the connection definition you are creating.

   The description is used to identify the connection definition in the ICA Remote Application Manager window.

4. Select to connect to a **Citrix Server** or to a **Published Application**. Then, choose a Citrix server or published application from the pull-down list.

5. If you want to log in as a specific user, enter the appropriate details in the Username, Domain, and Password fields.

   Alternatively, you can leave the fields blank, in which case you are prompted for them, if necessary, when you connect.

6. Click **OK** to create a connection definition containing the properties you specified.

The ICA Remote Application Manager window shows the connection definition you have created as shown in Figure 367 on page 437.

14.4.3.4 Opening a connection

Once you create a connection file with the appropriate network connection properties set up, you can connect to the Citrix server as explained here:

Double-click the name of the connection definition you want to open in the ICA Remote Application Manager window.

Alternatively, you can select the name of the connection definition and choose **Connect** from the Entry menu, or click the connect button (that looks like a lightning bolt).

This connects to the server specified in the connection file with the user name and password details you entered in the connection definition.

The following message tells you to which ICA server the ICA client is trying to connect:

```
Connecting to server <<server name>>
```

When the connection to the ICA server is complete, the following message is presented:

```
Connected to server <<server name>>
```

14.4.3.5 Connecting to Citrix MetaFrame servers

If you have not specified a user name or password in the connection file, you are prompted to enter them if they are required by the server as shown in Figure 369.

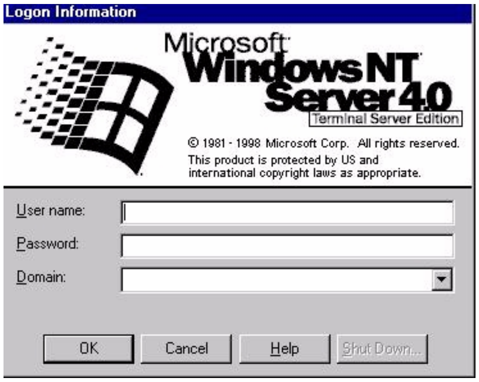

Logon Information
Microsoft Windows NT Server 4.0
Terminal Server Edition
© 1981 - 1998 Microsoft Corp. All rights reserved.
This product is protected by US and international copyright laws as appropriate.
User name:
Password:
Domain:
OK
Cancel
Help
Shut Down...

Figure 369. Citrix MetaFrame Log on Information

After a short delay, the Windows desktop is displayed in a window on your IBM Network Station as shown in Figure 370 on page 440.

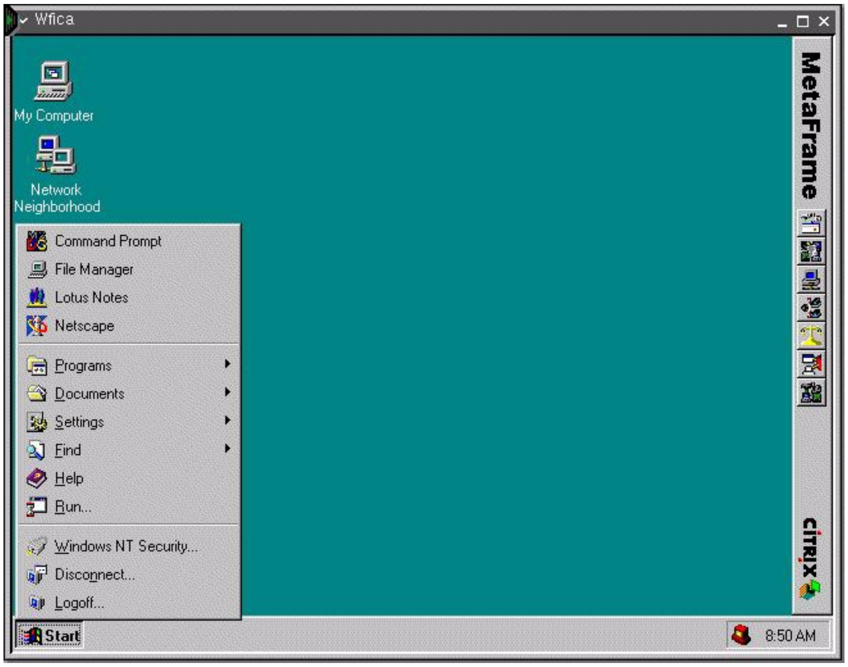


Figure 370. Windows desktop

Logging off from Windows

Choose **Logoff...** from the Windows **Start** menu. Or, if your connection is set up to run an application, select **Exit** from the application's **File** menu. These two methods close the ICA session and terminate the ICA client.

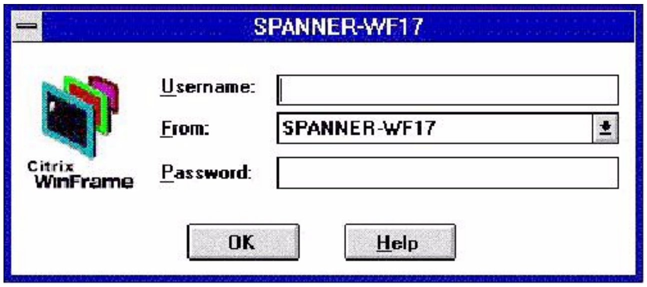
Disconnecting from Windows

Choose **Disconnect...** (if available) from the Windows **Start** menu. This leaves your session open on the Citrix server. You can resume work where you left off next time you log on to the server with the same user name and password.

When you reconnect, the server forces the ICA client window to be the same size and number of colors as in the original session.

14.4.3.6 Connecting to Citrix WinFrame servers

If you are connecting to a Citrix WinFrame server, then the login window (Figure 371) and desktop window (Figure 372) have a different appearance.


SPANNER-WF17

Username:

From: SPANNER-WF17

Password:

Figure 371. Citrix WinFrame server login window

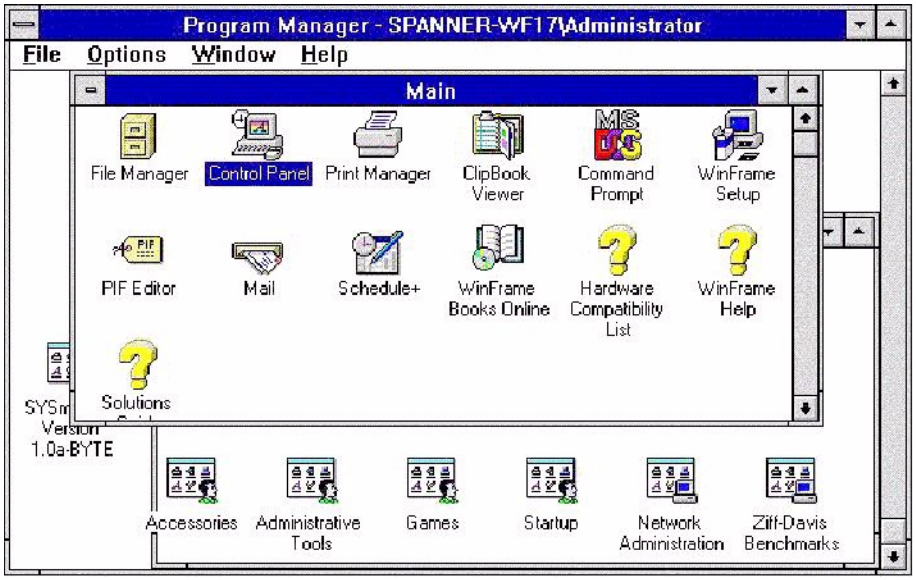


Figure 372. Desktop window appearance

Logging off from Windows

Choose **Log off...** from the Windows Program Manager **File** menu. Or, if your connection is set up to run an application, select **Exit** from the application's **File** menu. These two methods close the ICA session and terminates the ICA client.

Alternatively, choose **Close** (if available) from the Window menu. This leaves the ICA client application running so that you can open another session, if you want.

Disconnecting from Windows

Choose **Disconnect...** (if available) from the Windows Program Manager File menu.

14.4.3.7 Quitting from the ICA Remote Application Manager

Choose **Exit** from the **Entry** menu. This leaves any connections to Citrix servers open.

14.4.3.8 Editing an existing connection definition

You can edit existing connection definitions, or create new connection definitions, in the ICA Remote Application Manager window. When you create a new connection definition, the default window size and window color settings are those specified by Settings... on the Option menu.

To edit an existing connection definition, follow these steps:

1. Select the name of the connection you want to edit in the ICA Remote Application Manager window.
2. Select **Properties...** from the **Entry** menu, or click the **Properties** button.

   The Properties dialog box shows the current properties of the selected connection.

3. Edit the properties you want to change. Then, click **OK** to close the Properties window.

14.4.3.9 Properties dialog box

This section explains in detail how to use the ICA Remote Application Manager to create and edit connection definitions, giving you total control over your access to Citrix servers.

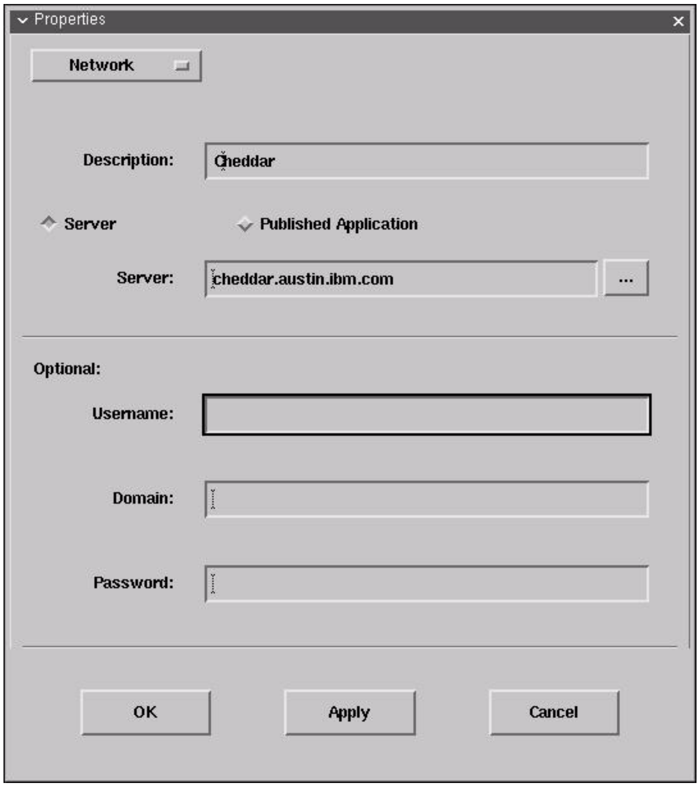
To display the connection properties, complete these tasks:

1. Select the name of the connection you want in the ICA Remote Application Manager window.
2. Choose **Properties...** from the **Entry** menu, or click the **Properties** button.

The Properties dialog box shows the current properties of the selected connection. Five panels contain all the information that you can select or change. They are Network, Connection, Window, Application, and Firewall.

Network

The Network panel (Figure 373) shows the current properties for description, server name, user name, password, and domain.



Description: Cheddar

◆ Server ◇ Published Application

Server: cheddar.austin.ibm.com

Optional:

Username:

Domain:

Password:

Figure 373. Properties: Network

The Description field identifies the connection definition. It is a required field. The characters ;, =, #, [,], and - are not allowed.

If the Server field is selected, enter the network name or address of the Citrix server. Selecting the **...** button brings up a list of available Citrix servers. This make take some time. The allowable characters are upper and lower case alphanumeric, plus the special characters period, underscore and dash. None of the special characters can be first or last.

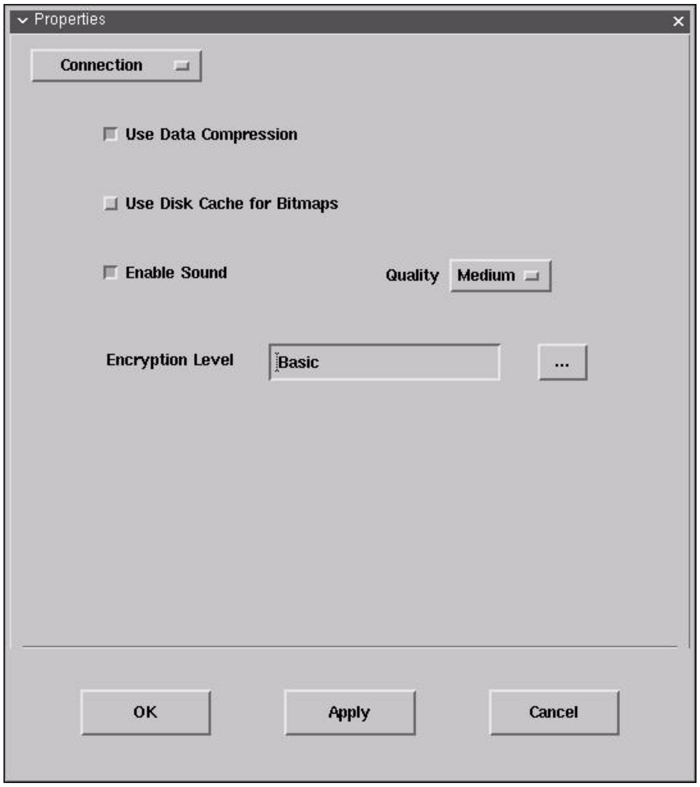
If the Published Application option is selected, enter the name of the published application. The characters ;, =, #, [,], and - are not allowed. Selecting the **...** button brings up a list of published applications. This may take some of time.

Either the Server name or the Published Application name is required.

The Username, Domain, and Password are used as login parameters and should match those set up on the specified Citrix server. If you do not provide these login parameters, you are prompted for them each time you connect.

Connection

The Connection panel (Figure 374) shows the current properties for compression, caching, sound, and encryption.



☑ Use Data Compression

□ Use Disk Cache for Bitmaps

☑ Enable Sound Quality Medium

Encryption Level Basic ...

Figure 374. Properties: Connection

Select **Use Data Compression** to reduce the amount of data transferred across the ICA session. This requires additional processor resources to compress and decompress the data, but can increase performance over bandwidth-limited connections.

Select **Use Disk Cache for Bitmaps** to enable persistent caching of frequently used icons and bitmaps. The persistent cache is always cleared when the IBM Network Station is re-booted. Internal caching is not affected by this option. Persistent caching must be enabled by following the ICA persistent caching directions in the /.profile file.

Select **Enable Sound** to enable sound support. Select **High**, **Medium**, or **Low** quality depending on the available bandwidth. The higher the sound quality is, the more bandwidth is used.

Select the **Encryption Level** for the ICA session. The default level is Basic. RSA encryption is available using RSA RC5 for 40-, 56-, and 128-bit session keys. Select RC5 128-bit Login Only to use encryption only during authentication. Selecting RC5 encryption disables automatic login to the Citrix server.

Window

The Window panel (Figure 375) shows the current properties for the number of colors, color mapping, and window size.

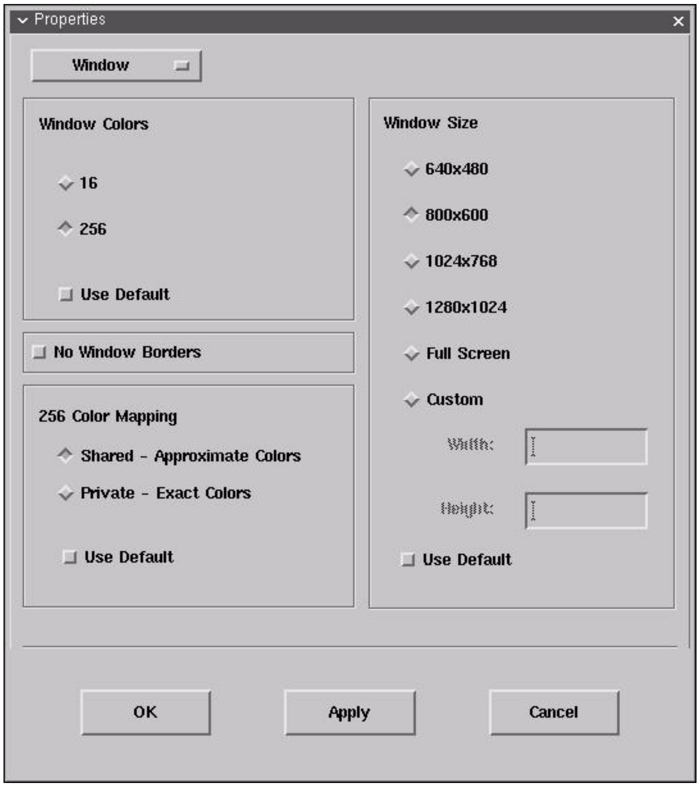


Figure 375. Properties: Window

Window Size allows you to select one of four standard window sizes, full screen, or a custom size. If custom is specified, then the width must be between 300 and 1280. If height is specified, it must be between 300 and 1024.

Window Colors allows you to set the number of windows colors to 16 or 256.

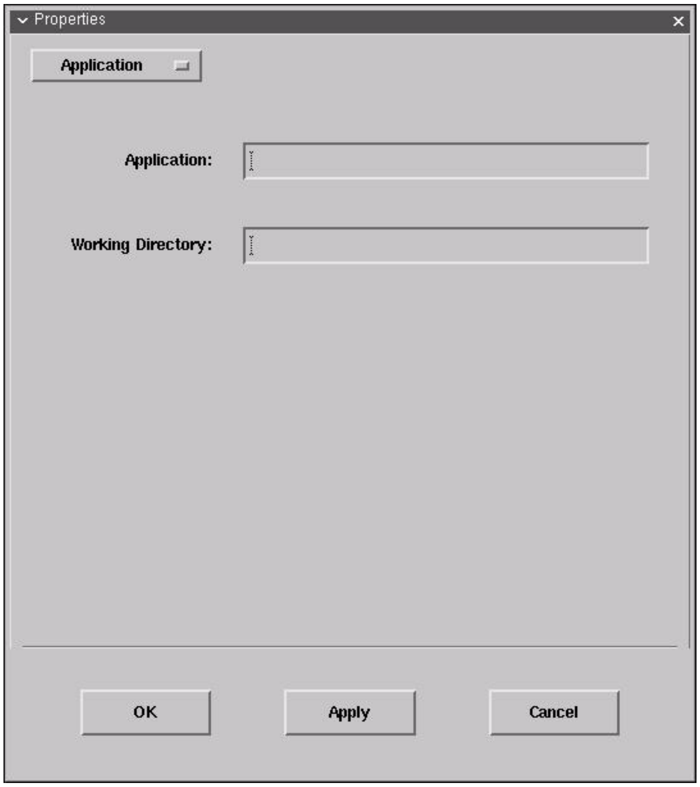
No Window Borders allows you to run the ICA client in a window without borders or a title bar. Typically, the window manager attaches borders and a title bar to windows that appear on the desktop.

256 Color Mapping allows you to set up 256 color sessions to use approximate or exact colors. Use Approximate Colors to eliminate color flashing when switching context. Note that if other applications have allocated all 256 colors, the client will fall back to using a private color map.

Select **Use Default** to use the default window size, window colors, or 256 color mapping setting specified with the Settings... command on the Option menu.

Application

The Application panel (Figure 376) shows the current properties for the application name and the working directory.



Application:

Working Directory:

Figure 376. Properties: Application

This panel allows you to specify the path name of an application to be run after connecting to the Citrix server. For example, to run Microsoft Word automatically after connecting to the Citrix server, you might enter:

```
C:\WINWORD\WINWORD.EXE
```

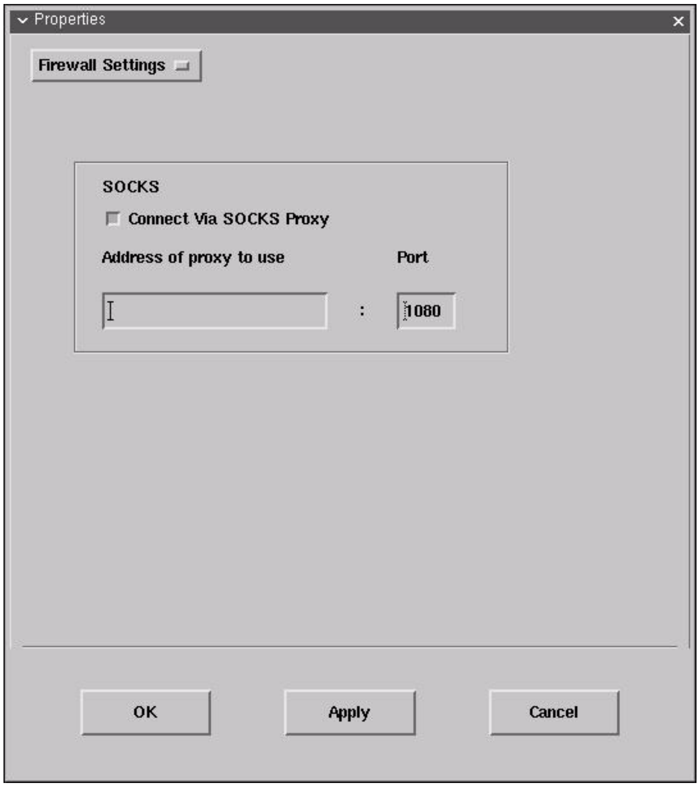
If you specify an application, you do not see the Windows desktop, and the connection is closed when you quit from the application.

The Working Directory allows you to specify the pathname of a working directory to be used with the application.

Note: If you selected to connect to a published application, the Application dialog box will not be available.

Firewall settings

The Firewall Settings panel (Figure 377 on page 446) shows the current properties for the SOCKS proxy.



SOCKS

□ Connect Via SOCKS Proxy

Address of proxy to use : Port 1080

Figure 377. Properties: Firewall

Selecting Connect Via SOCKS Proxy allows your ICA session to connect to an ICA Server via a SOCKS Proxy Server.

Specify the Address of proxy to use (network name or network address) and the Port number to use.

14.4.3.10 Settings dialog box

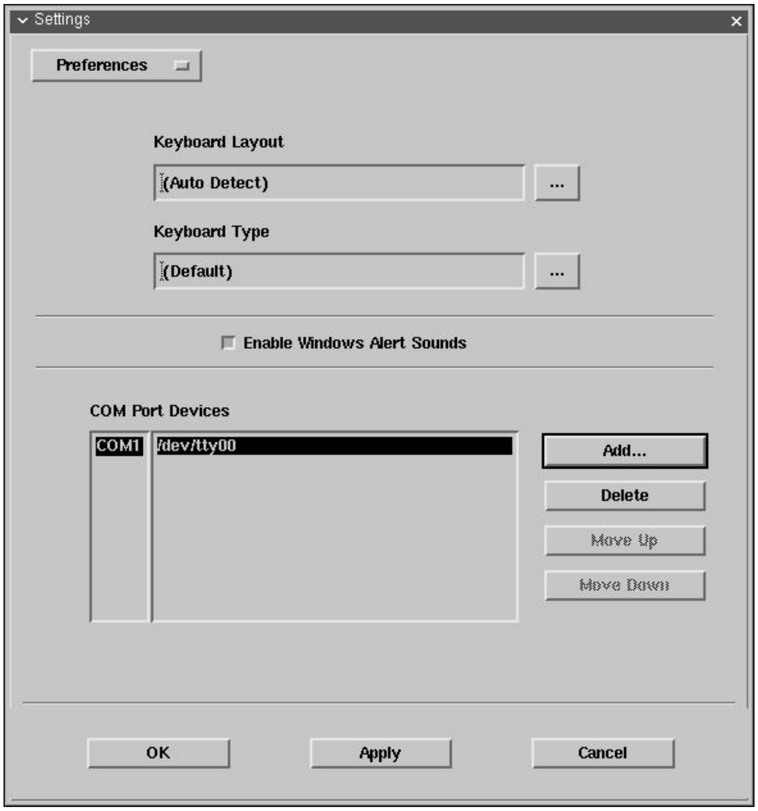
The Settings dialog box allows you to specify the default window settings used when you create a new connection file. It also allows you to enter a Citrix name server TCP/IP address.

To display the Settings dialog box, choose **Settings...** from the **Option** menu.

Six panels contain all the information that you can select or change. Each of these are explained are explained in the following sections.

Preferences

The Preferences panel (Figure 378) shows the current properties for keyboard type and layout, alert sounds, and com port devices.



Keyboard Layout: (Auto Detect)

Keyboard Type: (Default)

□ Enable Windows Alert Sounds

COM Port Devices

COM1	/dev/tty00

Figure 378. Settings: Preferences

Keyboard Layout specifies the keyboard layout used by the ICA client.

If (Auto Detect) is selected, the ICA client automatically detects and uses the keyboard layout configured by the IBM Network Station boot monitor.

If (User Profile) is selected, the Citrix server specifies the keyboard layout based on the user's Citrix server profile.

If neither of these options are suitable, one of the following explicit keyboard layouts can be selected:

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- Dutch (Belgian)
- English (UK)
- English (US)
- English (US ISO)
- Finnish
- French
- French (Belgian)
- French (Canadian 1988)
- French (Canadian 1992)
- French (Swiss)
- German

- German (Swiss)
- Greek
- Hungarian
- Icelandic
- Italian
- Italian (Swiss)
- Japanese (ATOK11)
- Japanese (MS-IME98)
- Norwegian
- Polish
- Polish (Programmer)
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovakian
- Slovenian
- Spanish
- Spanish (Latin American)
- Swedish
- Turkish (F)
- Turkish (Q)

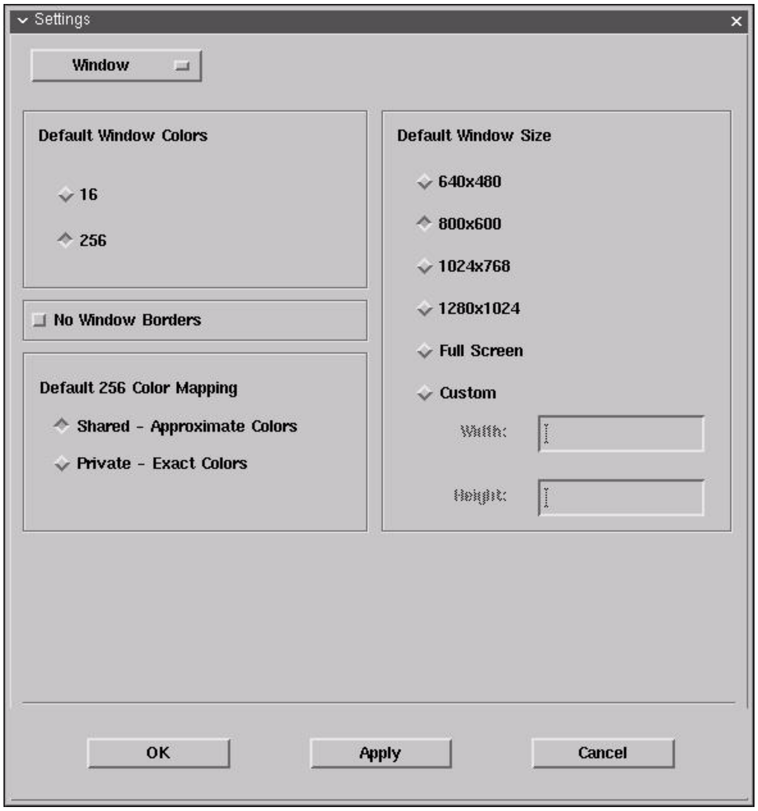
Keyboard Type specifies the keyboard type to be used with the ICA client. Select **(Default)**.

Enable Windows Alert Sounds, if selected, causes Windows alert sounds to be played using the IBM Network Station sound system.

COM Port Devices allows bi-directional mapping of IBM Network Station serial devices, for example, /dev/tty00, to Citrix Server COM ports.

Window

The Window panel (Figure 379) shows the current properties for default color and size choices. These settings are used as the default for all new connection files.



Settings

Window

Default Window Colors

○ 16

● 256

□ No Window Borders

Default 256 Color Mapping

● Shared - Approximate Colors

○ Private - Exact Colors

Default Window Size

○ 640x480

● 800x600

○ 1024x768

○ 1280x1024

○ Full Screen

○ Custom

Width:

Height:

Figure 379. Settings: Window

Window Size allows you to select one of four standard window sizes, full screen, or a custom size. If custom is specified, the width must be between 300 and 1280. If height is specified, it must be between 300 and 1024.

No Window Borders allows you to manage the window borders and title bar that surround an ICA session.

Window Colors allows you to set the number of windows colors to 16 or 256.

You can specify that your ICA window is one of four predefined window sizes, custom size or full screen.

256 Color Mapping allows you to setup 256 color sessions to use approximate or exact colors.

Server Location

The Server Location panel provides a more redundant method for locating the Master ICA Browser. The Master ICA Browser is queried to create a list of all Citrix servers and published applications on the network.

The Server Location panel (Figure 380 on page 450) shows the current properties for server groups and server lists.

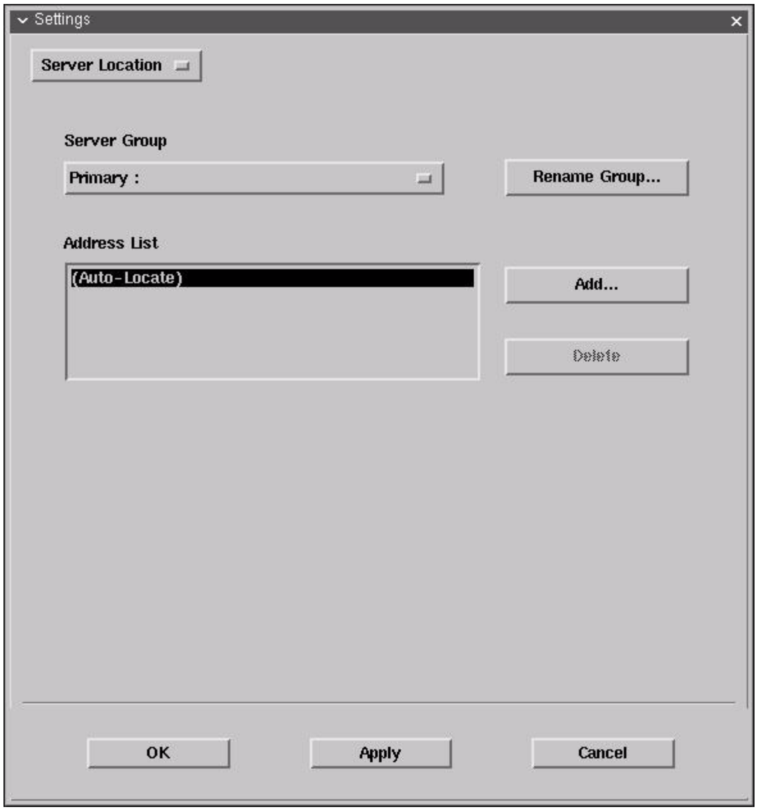


Figure 380. Settings: Server Location

If (Auto-Locate) is specified in the Address List box, the ICA client broadcasts a Get Nearest Citrix server packet. The first Citrix server to respond is queried for the address of the ICA Master Browser server.

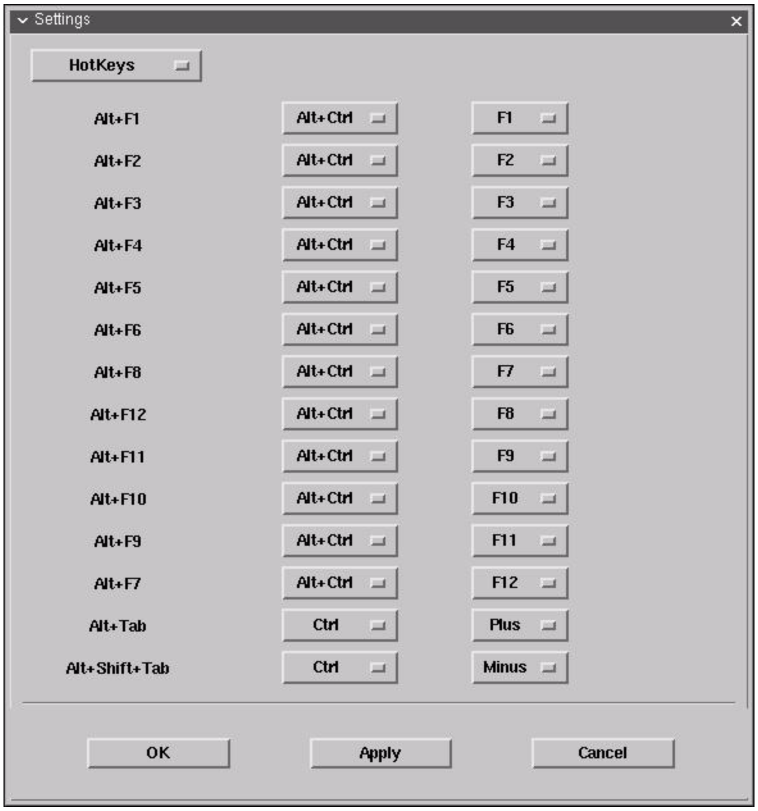
If Citrix servers are specified in the Address List box, the ICA client sends a request for the address of the Master ICA Browser to each of the servers listed in the Primary group. If there is no response, requests are sent to each of the servers listed in the Backup 1 group. If there is no response from the Backup 1 group, requests are sent to the servers listed in the Backup 2 group.

Some network configurations use routers or gateways to filter broadcast packets. Specifying Citrix servers allows the ICA Master Browser to be located on these types of networks.

Note: If the Master ICA Browser cannot be located, you can connect to Citrix servers directly by specifying the TCP/IP address as the server location.

HotKeys

The HotKeys panel (Figure 381) allows you to define alternative key combinations for the hot keys.



Alt+F1	Alt+Ctrl	F1
Alt+F2	Alt+Ctrl	F2
Alt+F3	Alt+Ctrl	F3
Alt+F4	Alt+Ctrl	F4
Alt+F5	Alt+Ctrl	F5
Alt+F6	Alt+Ctrl	F6
Alt+F8	Alt+Ctrl	F7
Alt+F12	Alt+Ctrl	F8
Alt+F11	Alt+Ctrl	F9
Alt+F10	Alt+Ctrl	F10
Alt+F9	Alt+Ctrl	F11
Alt+F7	Alt+Ctrl	F12
Alt+Tab	Ctrl	Plus
Alt+Shift+Tab	Ctrl	Minus

Figure 381. Settings: HotKeys

Table 61 shows the hot keys reserved for X Windows and the default alternative.

Table 61. Hot keys reserved for X windows

X Window hot key combination	Default alternative key combination
<Alt><F1> to <Alt><F12>	<Alt><Ctrl><F1> to <Alt><Ctrl><F12>
<Alt><Tab>	<Ctrl><Tab>
<Alt><Shift><Tab>	<Ctrl><Shift><Tab>

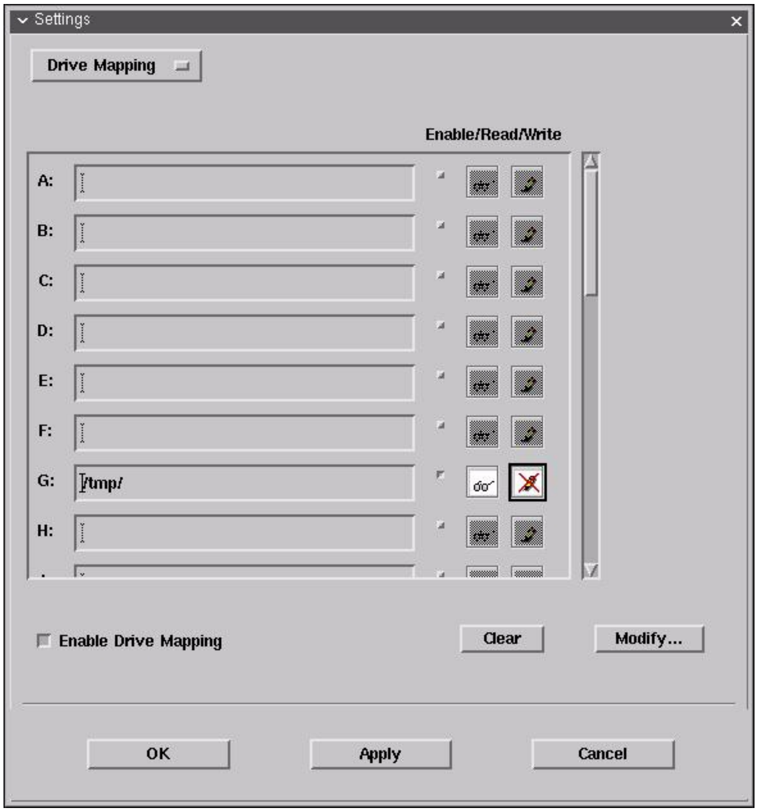
You can change the definitions by selecting alternative keys from the pop-up menus.

Any <Alt> key combinations not used by your X Window manager can be used as normal within your Citrix session.

In addition, the key combination <Ctrl><Alt><Enter> can be used to produce the PC key combination <Ctrl><Alt><Delete>.

Drive mapping

You can configure the ICA client so that you can access any directory mounted on your IBM Network Station, including CD-ROMs, from the Citrix server session as PC drive letters (Figure 382 on page 452).



G: /tmp/

Figure 382. Settings: Drive Mapping

After changing drive mapping settings, you need to log off and reconnect to the Citrix server for the changes to take effect. Simply disconnecting is not sufficient.

For each Windows NT drive letter, the Drive mapping list shows the disk or path name of the IBM Network Station directory mapped to the drive, and the Enable/Read/Write access.

To map a Citrix server drive to a directory on your IBM Network Station, follow this process:

1. Select the drive you want to map, for example G:.
2. If the drive you mapped is not available on the Citrix server, the directory you specified is mapped to another free drive letter.
3. Click **Modify** to change the drive mapping. A file selection dialog is displayed to allow you to select the IBM Network Station directory to map.
4. Select the directory (for example `/tmp`) you want to map to, and click **OK**. The directory is shown in the Drive mapping list.

To enable access to a specific drive, select the check box next to the corresponding drive. To change the access to a drive, click the appropriate read/write icons corresponding to the drive. Typically, only the $HOME and /tmp directories are writable.

To enable drive mapping, select **Enable Drive Mapping**. This enables drive mapping for all your connection definitions. Depending on the setup of the server, your mapped drives may be immediately available. They may also be mapped to different server drive letters than those you specified in the Drive Mapping panel, because the drives you specified have already been assigned by the server.

To find out the current status of your mapped drives for WinFrame, once connected to the Citrix server, open the **File Manager**. Click the drive letter pull-down menu in the top left of the File Manager window. This displays which local or client drives are mapped to which server drives. Client drives are shown in the format \\Client\drive, where *drive* is the drive letter specified in the Drive Mapping panel. If a drive you specified in the Drive Mapping panel is not shown in this list, you can connect it to a server driver letter as follows:

1. In the File Manager, select **Connect Network Drive?** from the **Disk** menu.
2. In the Connect Network Drive dialog box, select the server drive you want to map the client drive to in the **Drive** pull-down menu.
3. If you want to have this drive available to you each time you log into this server, ensure that the **Reconnect at Logon** box is selected.
4. Double-click the **Client Network** icon in the **Shared Directories** list. Then, click the appropriate client icon for your IBM Network Station directory. This displays a list of the available local drives, previously set up in the Drive Mapping panel.
5. Select the drive you want to map to the selected server drive, and click **OK**. Your local drive will now be available.

Repeat these steps for each of the local drives you want to attach to the server drives.

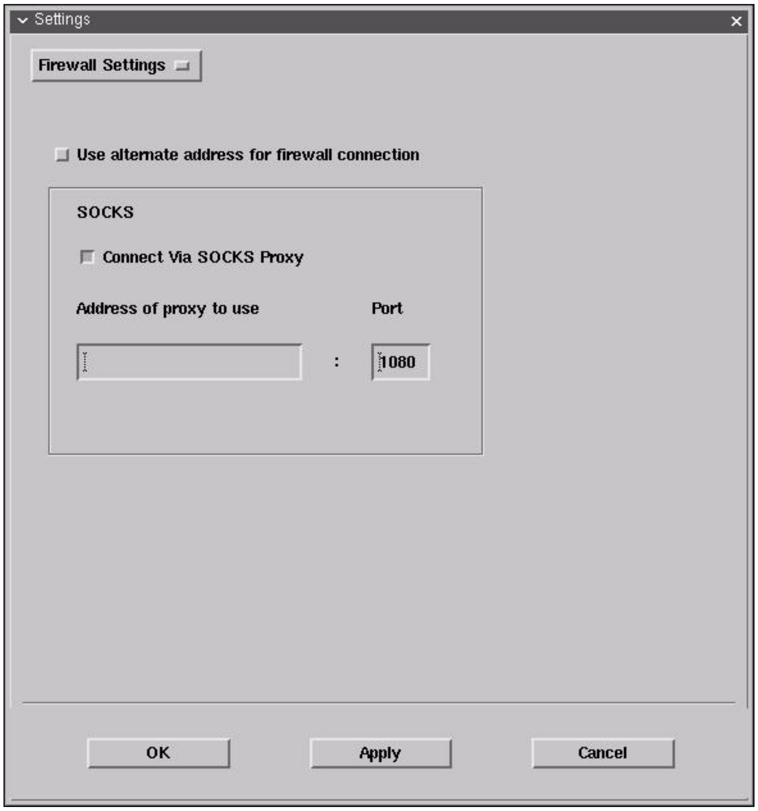
To find out the current status of your mapped drives for MetaFrame, once connected to the Citrix server, open the Windows NT Explorer. Client drives are shown in the format `<drive>$ on 'Client'(<drive>:)`, where <drive> is the drive letter specified in the Drive Mapping panel.

File naming conventions

Because UNIX is a case-sensitive file system and Windows NT is case insensitive, problems may occur if you use UNIX files within the ICA client session whose names are identical except for their case, for example, ReadMe and README. In such circumstances, although Windows NT displays the names correctly in a file listing, when a file is referred to, for example as a link in an HTML file, the first file found is used. We recommend that you give unique names to any files you intend to use within the ICA client session.

Firewall Settings

The Firewall Settings panel (Figure 383 on page 454) allows you to enable an alternate network address and SOCKS proxy server.



Settings

Firewall Settings

□ Use alternate address for firewall connection

SOCKS

□ Connect Via SOCKS Proxy

Address of proxy to use : Port 1080

Figure 383. Settings: Firewall Settings

The Use alternate address for firewall connection feature is used to browse for Citrix servers or published applications that are inside a firewall from a client machine that is outside the firewall. The firewall and the Citrix servers must be configured to map the internal network addresses of Citrix servers to external Internet addresses. Enter the external Internet addresses in the Address List.

Do not use the Use alternate address for firewall connection check box except on the advice of your network administrator.

Selecting Connect Via SOCKS Proxy allows your ICA session to connect to an ICA Server via a SOCKS Proxy Server.

Specify the Address of proxy to use (network name or network address) and the Port number to use.

14.4.4 Advanced configuration

The following sections deal with some advance configuration concerns.

14.4.4.1 Network Station's ICA client default values

The default settings used by the Network Station's ICA client are listed in Table 62. Some of the default values can be modified by the user from the Remote

Application Manager on the Network Station if the NSM administrator authorizes it. The modifiable settings are indicated by an asterisk (*).

Table 62. Default settings for ICA clients

Settings	Default values
Audio support	Enabled
Audio quality level	Medium
Color*	256
256 color mapping*	Shared (approximate color)

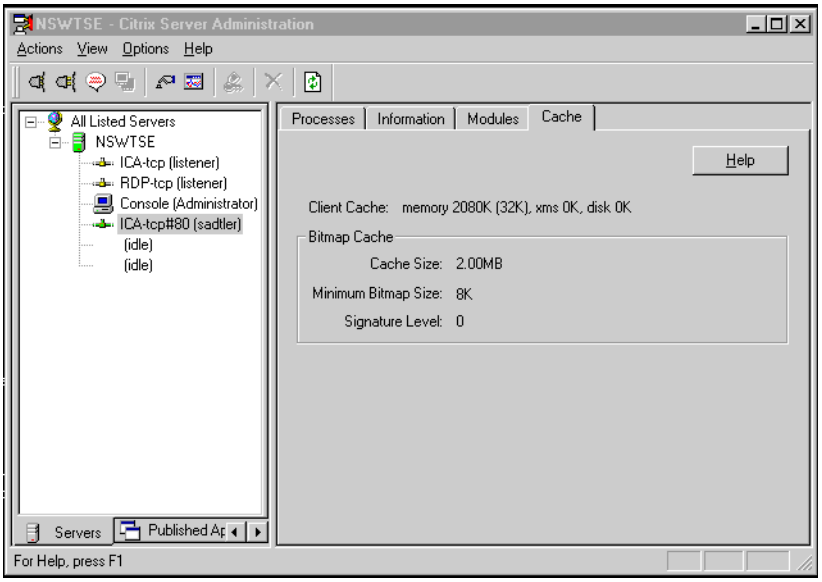
Video resolution	for NSM connection configuration: Full screen.
	for User connection configuration: 640 x 480.

Data compression	Enabled
Bitmap caching	0 KB
Encryption	Basic

14.4.4.2 ICA client cache

The procedure to access the client cache information on a MetaFrame server is described in the following list. You can adjust the ICA client cache with the -cache <n> parameter, where <n> is the number of KB. By default, it is 2 MB.

1. From a MetaFrame session, click the **Start** button on your desktop.
2. Click **Programs**.
3. Click **MetaFrame Tools (Common)**.
4. Click **Citrix Server Administration**. The Citrix Server Administration panel appears.
5. In the left frame, click your **NT user ID**.
6. Click the **Cache** tab to see information about the ICA client bitmap caching (Figure 384 on page 456).



Client Cache: memory 2080K (32K), xms 0K, disk 0K

Bitmap Cache

Cache Size: 2.00MB

Minimum Bitmap Size: 8K

Signature Level: 0

Figure 384. Citrix Server Administration panel: Client bitmap cache information

14.4.4.3 Command line interface

This section is intended for administrators who went to start the Network Station's ICA client or the ICA Remote Application Manager using the command line interface on a Network Station. This may be useful in debugging situations.

To launch the command line interface on the Network Station, from the Network Station launch bar, select the Tool Kit folder and launch the **Advanced Diagnostics** application. Here, you have a choice of two executable programs in the IBM Network Station ICA package.

The ICA client program, `wfica`, connects to a Citrix application server and establishes a session. The application window is presented within an X11 window on the Network Station as explained in the following section.

The ICA Remote Application Manager program, wfcmgr, is a graphical user interface for selecting ICA servers or Windows applications to which to connect. It presents connection records that it creates and connection records created by Network Station Manager. When a connection is initiated, the ICA client program is forked and executed as explained in the following section.

wfcmgr: ICA Remote Application Manager

The ICA Remote Application Manager can be launched from the Advanced Diagnostics window by typing:

```
wfcmgr <options>
```

There is a small set of command line parameters for the ICA Remote Application Manager. The -description, -icaroot and -file parameters came with the Citrix source code. The others have been added to provide additional value to the IBM Network Station. See Table 63 for a list of the available options.

Table 63. ICA Remote Application Manager command line parameters

Parameters	Values	Description
-help		The usage text is sent to the console.
-noupdate		When this option is specified, updates to the connection file or the configuration file are not allowed.
-description	<text>	The full text from the Description field of the connection definition dialog. If this argument is not specified, then the first description in the [ApplicationServers] section of the appsrv.ini file will be used.
-file	<name>	The fully qualified file name of the file that contains the connection description to be used. If the HOME environment variable is defined, the default file name is $HOME/.ICAClient/appsrv.ini. Otherwise, the default file name is /usr/lib/ICAClient/config/appsrv.ini.
-icaroot	<directory>	The fully qualified directory where the ICA client package was installed. If not specified, the ICAROOT environment variable is accessed to get the directory. If neither the -icaroot argument nor the ICAROOT environment variable are used to define the installation directory, then by default, it is /usr/lib/ICAClient.
-geometry	<WxH±X±Y>	The X11 window Width, Height, X offset, and Y offset. All values are in pixels. Positive X offsets are from the top of the screen and negative from the bottom. Positive Y offsets are from the left side of the screen and negative from the right. Variations of this specification include <WxH> and <±X±Y>. By default, the wfcmgr window is centered on the screen. To position the wfcmgr window in the upper left corner of the screen, specify `-geometry +0+0`.
-UseFullScreen	[<bool>]	When this option is set to True, the wfcmgr window must be the size of the full screen. Allowable values are True and False. Default value is False.
-NoWindowManager	[<bool>]	When this option is set to True, the wfcmgr window will not have borders nor a title bar. Allowable values are True and False. Default value is False.
-log		Enables ASSERT logging. ASSERTs are program sanity tests that wfcmgr can make. Typically these test are not enabled because they tend to impact performance.

wfica: ICA Network Station client

The Network Station's ICA client can be launched from the Advanced Diagnostics window by typing:

```
wfica [ica_options] [ns_options [-- <application>]]
```

Note: The Version 1 Release 3.0 ICA command line parameters will continue to be supported. This allows for Version 1 Release 3.0 ICA migration. The command line parameters have precedence over the .ini files.

Table 64 lists the available parameters for `[ica_options]`. For more information regarding the `[ns_options [-- <application>]]` options, see Table 65 on page 459.

Note: NS Options cannot be combined with the -description parameter.

Table 64. wfica: ICA Network Station client command line parameters ica_options

Parameters	Values	Description
-help		The usage text is sent to the console.

-version		The following message is sent to the console:
		`IBM Network Station ICA client`
		`Version 2.0 (Build dd/mm/yyyy - hh:mm:ss)`
		`Copyright International Business Machines Corp. 1999`
		`All rights reserved`
		`Citrix ICA client for Unix`
		`Version 3.00.15`
		`Copyright 1998-1999 Citrix Systems, Inc.`
		`All rights reserved`

-quiet		Connection dialogs will not be presented to the user. By default, the ICA client will present a “connecting to” dialog followed by a “connected to” dialog. Both of these dialogs are informational and require no response by the user.
-description	<text>	The full text from the Description field of the connection definition dialog. Either -description or -server or -- <application> must be specified. If neither of these parameters are specified, the user will be prompted for a server name.
-file	Path and file name	The fully qualified file name of the file that contains the connection description to be used. If the HOME environment variable is defined, the default file name is $HOME/.ICAClient/appsrv.ini. Otherwise, the default file name is /usr/lib/ICAClient/config/appsrv.ini.
-protocolfile	<name>	The fully qualified file name of the file that contains the protocols supported by the ICA client. By default, the file name is /usr/lib/ICAClient/config/module.ini. This is a system configuration file and not meant to be modified.
-clientfile	<name>	The fully qualified file name of the file that contains the options and defaults for all connection descriptions. If the HOME environment variable is defined, the default file name is $HOME/.ICAClient/wfclient.ini. Otherwise, the default file name is /usr/lib/ICAClient/config/wfclient.ini.
-icaroot	<directory>	The fully qualified directory where the ICA client package was installed. If not specified, the ICAROOT environment variable is accessed to get the directory. If neither the -icaroot argument nor the ICAROOT environment variable are used to define the installation directory, then by default, it is /usr/lib/ICAClient.

Table 65. wfica: ICA Network Station client command line parameters ns_options

Parameters	Values	Description
-server	<name>	Specifies the ICA application server to which to connect. The name can be a fully qualified network host name, an abbreviated network host name, or a dotted decimal network address. Either -description or -server or -- <application> must be specified. If neither of these parameters are specified, the user will be prompted for a server name. -server and -browser are mutually exclusive.
-browser	<namelist>	Specifies the name of a master browser. The master browser is an ICA server that tells the ICA client which ICA application server to connect to and which application to run on that server. A colon (:) separated list of master browsers can be specified. Each name can be a fully qualified network host name, an abbreviated network host name, or a dotted decimal network address. If neither -server nor -browser is specified and -- <application> is specified, the ICA client will broadcast (typically to the local subnet) to get a master browser name. Either -description or -server or -- <application> must be specified. -server and -browser are mutually exclusive. Example: `-browser johnsimpson:0.0.0.0:xxx`
-username	<name>	Specifies the Windows NT server login user name.

Parameters	Values	Description

-password	[<password>]	Specifies the Windows NT server login password. The following password formats are supported:
		NSM Format: The NSM format is checked first. This is a repeating sequence of the % character followed by two hexadecimal characters. For example, the following is an NSM encrypted password:
		`%B2%86%C8%78`
		ICA Format: The ICA format is checked second. This is a string of hexadecimal decimal characters. The first four characters specify the number of bytes required to contain the binary form of the remaining hexadecimal characters. For example, the following is an ICA encrypted password:
		`0005a986568f51`
		In-the-clear: If the password is neither an NSM password nor an ICA password, it is assumed to be an unencrypted password. For example, the following is neither an NSM nor an ICA encrypted password. Therefore, it is an unencrypted password:
		`mypw`
		If -password is specified without a <password>, an NSM formatted password is requested from the actlogind daemon.

-domain	<name>	Specifies the Windows NT server domain name.
-name	<clientname>	Specifies the client name to be used by the ICA application server. If the client name is longer than 20 characters (an ICA protocol limitation), it is truncated to 20 characters. If -name is specified but is not followed by a host name, the fully qualified host name will be obtained from the system and converted to a simple host name. A simple host name is defined to be the first name in a fully qualified dotted name string. In other words, everything is truncated after the first decimal point. If the resulting string is longer than 20 bytes (an ICA protocol limitation), it is truncated to 20 bytes. If -name is not specified, the fully qualified host name is obtained from the system. If it is longer than 20 characters (an ICA protocol limitation), the dotted decimal IP address string will be used.
-color	16 256	Specifies the number of colors that the ICA application server should use to generate application graphics. Allowable values are 16 and 256.

Parameters	Values	Description
-encryption	basic login 40 56 128	Specifies the level of encryption to be used between the ICA client and the ICA application server. Supported encryption levels are: **basic:** Simple encryption (this is the default) **login:** 128-bit RSA encryption for login only **40:** 40-bit RSA encryption **56:** 56-bit RSA encryption **128:** 128-bit RSA encryption If any level of encryption is specified other than basic, any client side specification of username, password, or domain, whether from the command line or from an INI file, will not be used. The intent here is to insure the user logs into the Windows NT server via the Windows NT login dialog.)
-WorkingDirectory	<path>	Specifies the Windows NT working directory path.
-geometry	<WxH±X±Y>	The X11 window Width, Height, X offset, and Y offset. All values are in pixels. Positive X offsets are from the top of the screen and negative from the bottom. Positive Y offsets are from the left side of the screen and negative from the right. Variations of this specification include <WxH> and <±X±Y>. Window size allows you to select one of four standard window sizes, full screen, or a custom size. If custom is specified, width must be between 300 and 1280 and height must be between 300 and 1024. By default, the wfica window is centered on the screen. To position the wfica window in the upper left corner of the screen, specify: `-geometry +0+0`
-UseFullScreen	[<bool>]	When this option is set to True, the wfica window should be the size of the full screen. Allowable values are True and False. Default value is False.
-NoWindowManager	[<bool>]	When this option is set to True, the wfica window will not have borders or a title bar. Allowable values are True and False. Default value is False.
-title	<text>	Puts the specified text into the X11 window title bar.
-cache	<size>	Size in kilobytes of the internal ICA client transient cache.
-shm	<size>	Size in kilobytes of shared memory to be allocated. If size is greater than zero, the X11 Shared Memory extension is enabled.
-log		Enables ASSERT logging. ASSERTs are program sanity tests that wfica can make. Typically these test are not enabled because they tend to impact performance.

Parameters	Values	Description
-<keyword>	<value>	Any unrecognized arguments will be analyzed to see if they qualify as a command line keyword=value pair. Any such keyword=value pairs are assumed to be valid .INI file entries and will be concatenated with the keyword=value pairs extracted from the INI files. <keyword>=<value> pairs are not checked for validity. Therefore, the ability for the ICA client to detect and report command line errors is limited.
--	<application>	Specifies the program that the ICA application server should run if the -server argument is also specified. Otherwise, it specifies a published application, and a master browser will be contacted to get both the program to run and the ICA application server to run it on. This parameter must be last. Either -description or -server or -- <application> must be specified. If neither of these parameters are specified, the user will be prompted for a server name. If -- <application> is not specified, a default description must exist in an accessible connection file.

The following V1R3 command line arguments can still be used in the V1R3-to-V2R1 migration strategy, but they should not be used beyond that. You should not use these if at all possible:

- -host <name> same as -server <name> if -lb is not specified. If -lb is specified, it is the same as -browser <name>.
- -lb governs how the -host parameter will work.
- -restart ignored.
- -geometry fullscreen is the same as < max_screen_width x max_screen_height + 0 + 0 >

Flash boot support

When booting the IBM Network Station from a flash card, several boot monitor fields may be available. In particular, one of the three Boot Host fields can be used to specify the IP address of an ICA server or ICA master browser.

Additional unused boot monitor (text) fields may be also used to specify ICA command line parameters. The boot monitor storage for these additional ICA command line parameters is limited.

The ICA client supports the additional command line parameters shown in Table 66 to support flash boot.

Table 66. ICA Remote Application Manager command line parameters

Parameters	Values	Description
-server1		Indirectly specifies the -server parameter where the server <name> comes from the First Boot Host parameter in NVRAM.
-server2		Indirectly specifies the -server parameter where the server <name> comes from the Second Boot Host parameter in NVRAM.

Parameters	Values	Description
-server3		Indirectly specifies the -server parameter where the server <name> comes from the Third Boot Host parameter in NVRAM.
-browser1		Indirectly specifies the -browser parameter where the browser <namelist> comes from the First Boot Host parameter in NVRAM.
-browser2		Indirectly specifies the -browser parameter where the browser <namelist> comes from the Second Boot Host parameter in NVRAM.
-browser3		Indirectly specifies the -browser parameter where the browser <namelist> comes from the Third Boot Host parameter in NVRAM.
-nvram	<fieldname>	Specifies the name of a text field in nvram. The text field will be analyzed and, if the first non-blank character is a dash (-), then the text will be used to replace the -nvram <fieldname> specification. Use the boot monitor to enter text in selected fields. See Table 67.

Table 67 gives the NVRAM filed name for selected boot monitor fields which *may* be available.

Table 67. NVRAM field names for selected boot monitor fields

boot monitor field name	NVRAM field name
Series 2200, 2800: Boot file server directory and file name (second)	second-boot-path
Series 2200, 2800: Boot file server directory and file name (third)	third-boot-path
Series 2200, 2800: Workstation directory (second)	config-unix-directory2
Series 300, 1000: Configuration file	config-custom-file

For example, to specify multiple ICA browsers on a Series 2800, the following text could be entered in the Boot Monitor field called `Boot file server dir and file name (third)`:

```
-b 9.8.7.201:9.8.7.104:server2 -- MyApplication
```

Then, the command:

```
wfica -nvram third-boot-path
```

will actually be interpreted as:

```
wfica -b 9.8.7.201:9.8.7.104:server2 -- MyApplication
```

The -server1, -server2, -server3, -browser1 , -browser2, and -browser3 arguments are mutually exclusive.

Locking keys

By default, the operator controls the locking state of the keyboard on the Network Station. When the operator presses a locking key (CapsLock or NumLock), the keyboard goes into the appropriate lock state. If the active window is the ICA client, the locking key is sent to the active Windows application on the ICA server.

Typically, this synchronizes the locking state and the LEDs between the Network Station and the ICA server.

However, a few Windows applications (notably VT100 emulators) process the NumLock key as a function key. As a result, the NumLock state of the ICA server is not changed and NumLock synchronization between the ICA server and the Network Station does not end until the NumLock key is pressed again.

To help control this situation, the ICA client (wfica) supports the following command line option:

```
-NumLockSync <bool>
```

When this option is set to false, the ICA server controls the NumLock state of the wfica window. The default value is true.

The keyboard locking state will always be in sync with the active window. In effect, each Network Station window, including the window that ICA is running in, will perceive that the keyboard is in the correct lock state. However, the Network Station windowing system (X11) always toggles the NumLock LED every time the NumLock key is pressed. As a result, the NumLock LED may not always reflect the NumLock state of the ICA window if -NumLockSync False is specified.

14.5 Java ICA client configuration

As mentioned before, the Java ICA client is usually not the preferred client on the Network Station to access a Windows NT multi-user environment. It does not offer as many features as the Network Station's ICA client, cannot be centrally customized from Network Station Manager, and requires more RAM memory on the Network Station.

However, there may be instances where this is the desired method. We show you how easy a Windows application can be added to a Web page and accessed from Netscape Communicator on a Network Station.

The Java ICA client features will certainly be improved in the future. We think that it is important to keep your attention in this direction. Using the Java ICA client as an applet on a browser is indeed a step further in the utilization of a single-user interface. Figure 385 shows and overview of the ICA Java client applet configuration.

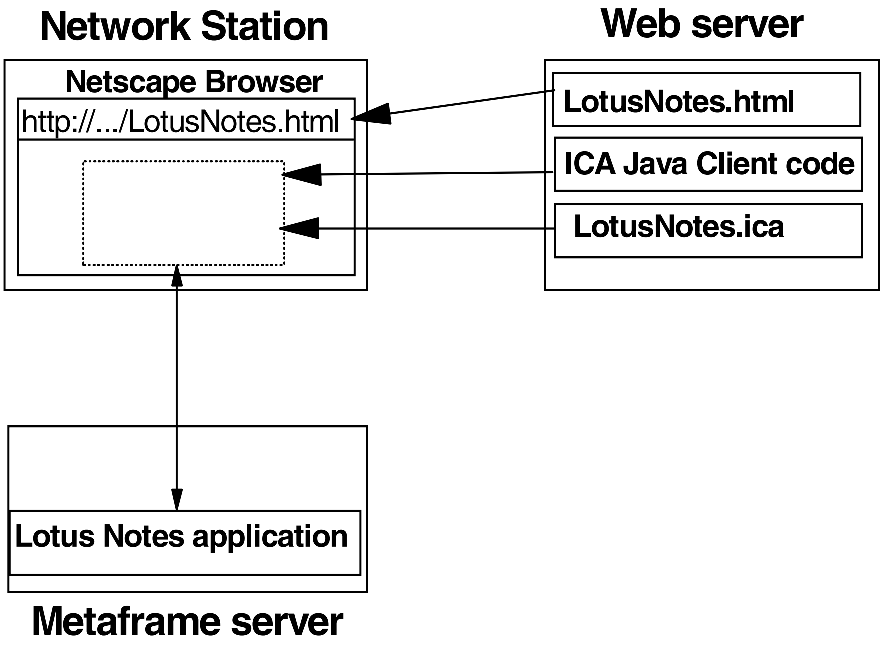


Figure 385. ICA Java client applet configuration overview

Once again, we use the example of a connection to a published Lotus Notes application on a Windows NT multi-user to illustrate the configuration procedure. The procedure consists of four steps:

1. Installing and publishing an application
2. Creating an ICA file
3. Creating a Web page with a link to the ICA file and the ICA Java Client code
4. Web server configuration consisting of copying the ICA file, the Web page and the Java ICA client code to a Web server

14.5.1 Application installation and publishing

Refer to 14.4.1, “Windows NT multi-user server set up” on page 421, for information on the installation and publishing of Lotus Notes client 5.0.

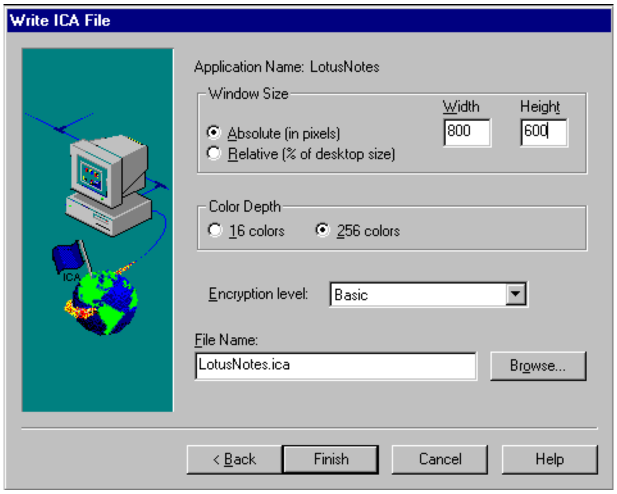
14.5.1.1 ICA file

ICA files are text files containing a series of command tags. These tags define the attributes of the session to be launched on the MetaFrame server. The Web browser downloads the ICA file and passes it to the ICA Java client, which then initiates the ICA session on the MetaFrame server.

The procedure to create an ICA file from a Published Application on a MetaFrame server is explained here:

1. Log on to the MetaFrame server using a user name that is part of the Administrator group.
2. Select **Start->Programs->MetaFrame Tools->Published Application Manager**.
3. Select the Lotus Notes published application we created previously.

4. Select **Application->Write ICA file** (Figure 386). Then, select **Not much. I have done this before**, and click **Next**.



Write ICA File

Application Name: LotusNotes

Window Size

● Absolute (in pixels)
○ Relative (% of desktop size)

Width: 800
Height: 600

Color Depth

○ 16 colors ● 256 colors

Encryption level: Basic

File Name: LotusNotes.ica

Figure 386. Published Application Manager: Write ICA File panel

5. Enter the Window size, color depth, encryption level, and file name in the Write ICA file panel. Click **Finish**.

The ICA file is saved in the c:\wtsrv\system32\ directory by default.

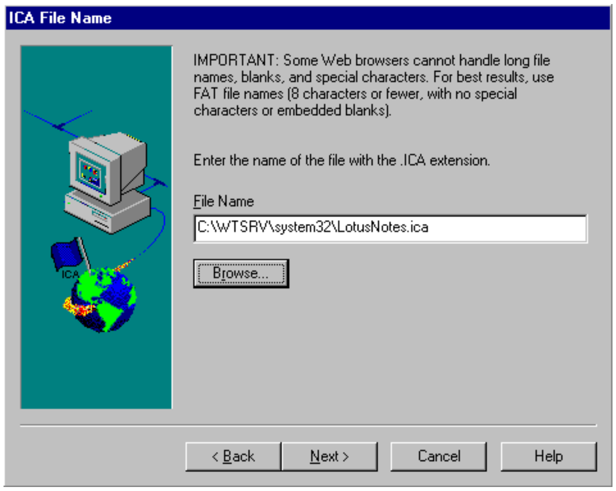
14.5.2 HTML page

The HTML page we create is a template Web page for the published Lotus Notes application that Web users can visit to connect to the application. This Web page contains a link to download the Java ICA client as an applet and the ICA file from the Web server.

The procedure to create an HTML file from a Published Application on a MetaFrame server is described here:

1. Log on to the MetaFrame server using a user name that is part of the Administrator group.
2. Select **Start->Programs->MetaFrame Tools->Published Application Manager**.
3. Select the Lotus Notes published application we created previously.
4. Select **Application->Write HTML file**. Then, select **Not much. I have done this before**, and click **Next**.
5. On the Create New ICA File? panel, select **Use an existing ICA file**, and click **Next**.

   Actually, you can create the ICA and HTML file in one step.
6. Enter the same ICA file name shown in Figure 386. This step is shown in Figure 387. Click **Next**.



ICA File Name

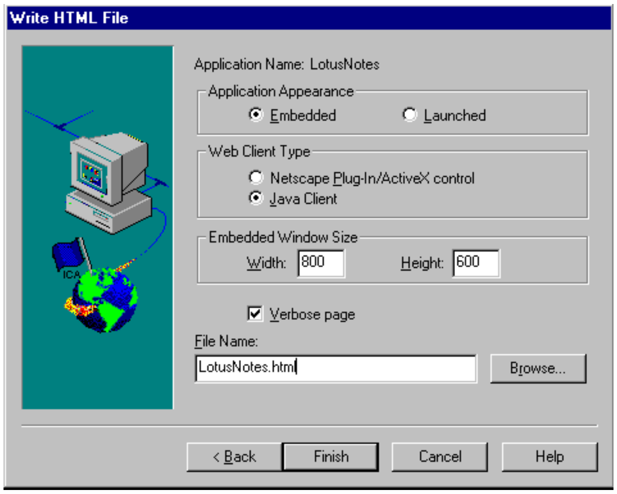
IMPORTANT: Some Web browsers cannot handle long file names, blanks, and special characters. For best results, use FAT file names (8 characters or fewer, with no special characters or embedded blanks).

Enter the name of the file with the .ICA extension.

File Name: C:\WTSRV\system32\LotusNotes.ica

Figure 387. Published Application Manager: ICA File Name panel

7. Enter the Application Appearance, Web Client Type, Embedded Windows Size and File Name in the Write HTML file panel (Figure 388). Click **Finish**.



Write HTML File

Application Name: LotusNotes

Application Appearance: ● Embedded ○ Launched

Web Client Type: ○ Netscape Plug-In/ActiveX control ● Java Client

Embedded Window Size: Width: 800 Height: 600

☑ Verbose page

File Name: LotusNotes.html

Figure 388. Published Application Manager: Write HTML File panel

The HTML file is saved in the c:\wtsrv\system32\ directory by default.

14.5.3 Web server configuration

We used Lotus Domino 5.0 server as the Web server.

The first step of the configuration is copying of the ICA file, the HTML file, and the Java ICA client code to the root directory of the Web server. For Domino 5.0, the root directory is drive:\Lotus\Domino\Data\Domino\html.

The ICA file and the HTML file created previously are located on the c:\wtsrv\system32\ directory on the MetaFrame server. Copy them to the Web root directory (or, make them accessible to the Web server).

You can download the Java ICA client code from the Citrix Web site at:
`http://www.citrix.com`

We downloaded the compressed file for Windows platform because the Domino server is installed on a Windows NT 4.0 server.

You must decompress the file. The ICA Java client is available in three formats: JICAEngJ.jar, JICAEngN.jar, JICAEngM.cab, depending on which browser you will use to access it. The *JICAEngN.jar* format is a signed .jar file containing the ICA Java client class files signed with Netscape's authentication method. This is the file we must copy on the root directory of the Domino Web server.

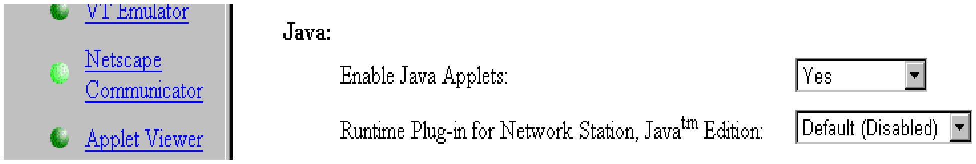
The second step of the configuration is the registration of ICA as an application MIME type on the Web server. This is a default for a Lotus Domino Web server. There is nothing more that needs to be done.

14.5.4 Java ICA client access from the Network Station

In our example, we have used the Java ICA client as an applet from Netscape Communicator. Therefore, the NSM administrator must enable the Java applet support for Netscape Communicator.

This is done by using these steps:

1. Log on to the NSM using a user name that is part of the NSMAdmin group.
2. Select the System preferences level.
3. Select **Applications->Netscape Communicator**.
4. Scroll down to the Java Settings section and Enable Java Applets (Figure 389).



Java:

Enable Java Applets: Yes

Runtime Plug-in for Network Station, Java^{tm} Edition: Default (Disabled)

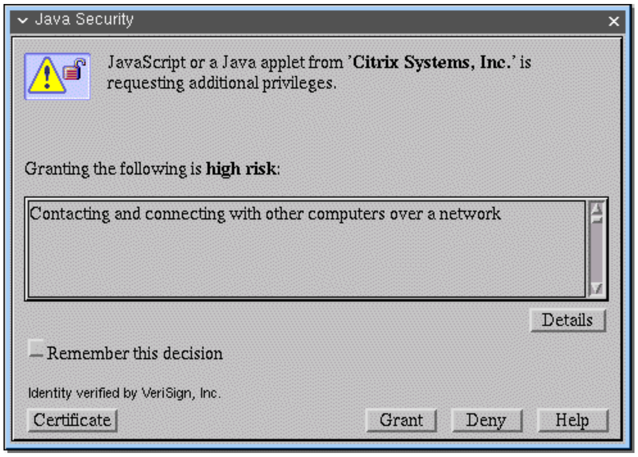
Figure 389. Enable Java Applets: Yes

To start a session to the MetaFrame server, simply enter the URL in the location toolbar of the browser:

```
http://DominoWebServerName/LotusNotes.html
```

When the HTML page we created is accessed from the browser, the browser downloads the ICA Java Client code and the ICA file from the Web server to the Network Station. It passes the ICA file to the ICA Java client, which then initiates the ICA session on the MetaFrame server.

The first time the ICA Java Client makes a connection to the Windows NT multi-user server, the user will have to grant access to the server. The window that the user will see is shown in Figure 390.



JavaScript or a Java applet from '**Citrix Systems, Inc.**' is requesting additional privileges.

Granting the following is **high risk**:

Contacting and connecting with other computers over a network

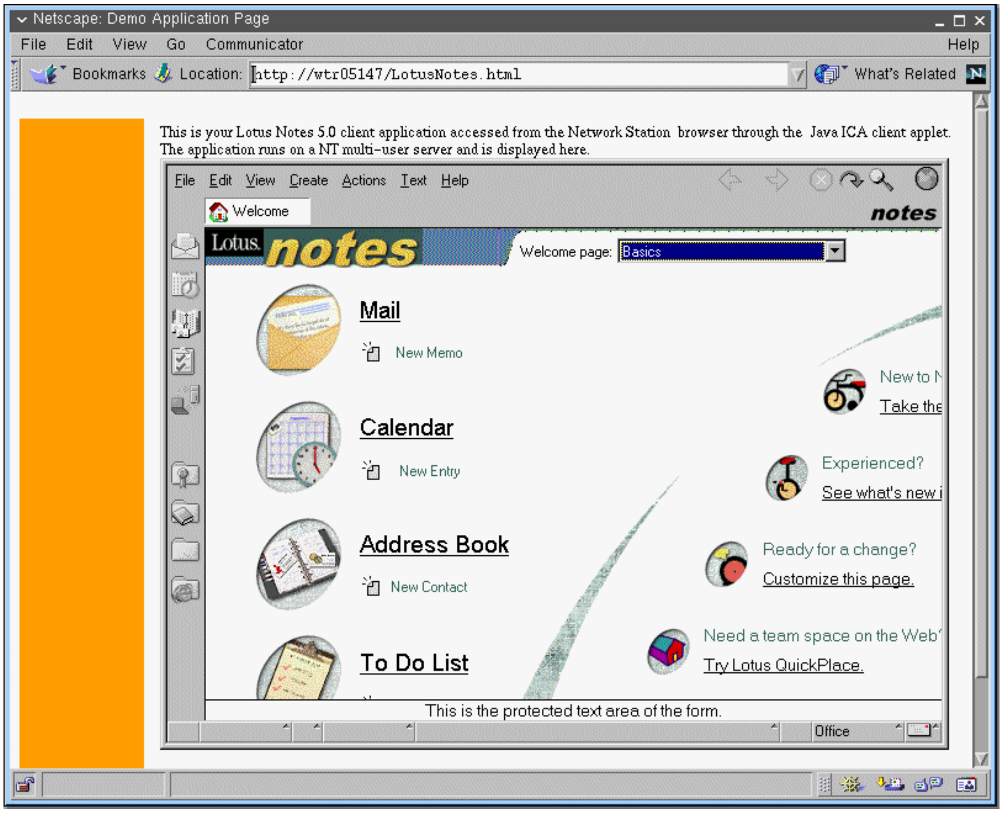
□ Remember this decision

Identity verified by VeriSign, Inc.

Figure 390. Java Security window

Grant the Java ICA client access to your Network Station by clicking the **Grant** button.

Figure 391 shows the published Lotus Notes application accessed from the ICA Java Client running as an applet in the Netscape Communicator browser of the Network Station.



Location: http://wtr05147/LotusNotes.html

This is your Lotus Notes 5.0 client application accessed from the Network Station browser through the Java ICA client applet. The application runs on a NT multi-user server and is displayed here.

This is the protected text area of the form.

Figure 391. Published Lotus Notes application accessed from the ICA Java Client

14.6 QuickOn for Running Windows with NSM V1R3

The QuickOn for Running Windows flash card allows a Network Station to function like a Windows-based Terminal. When you use QuickOn for Running Windows, you *do not need* an NSM server. The Network Station boots from a flash memory card in the PC Card drive (PCMCIA) that contains the operating system, minimal configuration information and the ICA client application.

The ICA client is configured to automatically start when the Network Station is powered on. It provides a single, full screen Windows NT desktop. The desktop is automatically restarted when you logoff from Windows NT. It can boot to a MetaFrame logon screen in as little as 28 seconds. Figure 392 shows an overview for QuickOn for Running Windows.

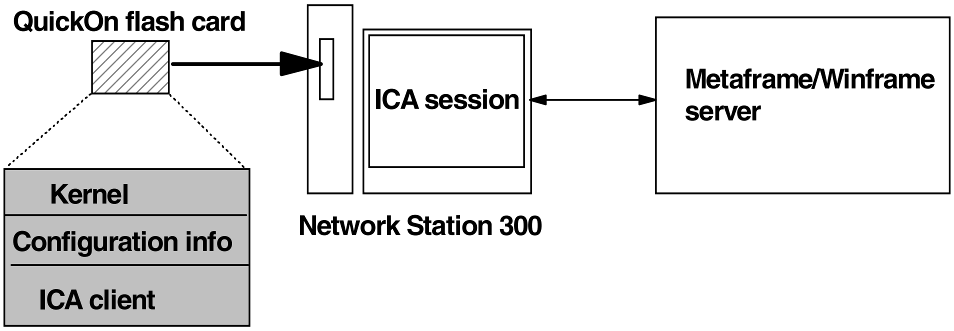


Figure 392. QuickOn for Running Windows overview

14.6.1 QuickOn for Running a Windows environment

This section helps you understand some of the issues related to QuickOn.

System requirements

The QuickOn for Running Windows flash card is an 8 MB PC card. The card is designed for a Series 300 Network Station Ethernet or Token-Ring model. The code installed on the card is NSM V1R3 based. A minimum of 16 MB of memory is required on the Network Station.

Keyboard and locales

The QuickOn for Running Windows flash card contains keyboard setup information files and other setup information for the locales in English US, English UK, French, French Canadian, German, Italian, Spanish, and Swedish. Others keyboard setup information files are provided on the card, but they are not supported.

Load balancing

The QuickOn for Running Windows flash card is configured to automatically connect to a single published application when load balancing is used. This published application is the *desktop*, which is the familiar Windows NT desktop. You need to publish the name *desktop* (case sensitive) before you can use QuickOn for Running Windows and load balancing.

Print

You can print using printers attached to the Windows NT multi-user server, Network printers, or printers attached to Network Stations. See the *IBM Network*

Station Printing Guide, SG24-5212, for additional information on printing with your Network Station.

The queue names on the Network Station are always PARALLEL1 and SERIAL1. You can send ASCII, PCL, or PostScript data streams.

14.6.2 Peer booting

You can use one QuickOn for Running Windows flash card to boot multiple Network Stations. To do this, you peer boot multiple Series 300 Network Stations from one QuickOn for Running Windows flash card that is installed in a Network Station. All of the Network Stations must be on a local area network and run the NFS protocol for peer booting.

The number of Network Stations that boot from a single Network Station installed with a QuickOn for Running Windows flash card depends on the environment. LAN traffic and peer boot timing are the major performance factors. One flash card can “buddy boot” approximately ten other Network Stations.

The QuickOn for Running Windows flash card is pre-configured to allow peer booting.

Setting up Network Station to use QuickOn for Running Windows

The setup of a Network Station using the QuickOn for Running Windows flash card is done through the Network Station NVRAM. The configuration is very simple and quick.

You only need to perform the following instructions once for each Network Station. After you configure the system, the Network Station NVRAM saves the configuration parameters for future use.

14.6.2.1 Network configuration information

You need the following information to boot a Network Station with QuickOn for Running Windows:

- The IP address of the Network Station
- The IP address of the MetaFrame, WinFrame, or WinCenter server
- The subnet mask, gateway, and other network setup parameters

14.6.2.2 Boot monitor

If the Network Station boot monitor is below V3.0.7.3, the QuickOn for Running Windows flash card automatically updates the boot monitor to V3.0.7.3.

14.6.2.3 Installing the flash card

Before you power on the Network Station, insert the QuickOn for Running Windows flash card into the PC Card drive. Do not insert the flash card when the Network Station is powered on.

14.6.2.4 Clearing NVRAM

You need to clear NVRAM the first time that you boot from the QuickOn for Windows flash card. This clears any residual setting in the Network Station NVRAM. Complete these steps:

1. Power off your Network Station.
2. Power on your Network Station.

3. Press the Esc key when you see the `Search for Host System...` message. You should now be at the Setup Utility screen.
4. Use <LeftCtrl>+<LeftAlt>+<LeftShift>+F1 to enter the boot monitor. The boot monitor responds with:

```
IBM Network Station model xxxx-xxx 8-bit Color Boot Monitor
>
```

5. Enter the following commands, in order, to reset the NVRAM settings to their factory defaults:

   a. > nv
   b. ->> l
   c. ->> s
   d. Are you sure? y
   e. ->> q
   f. > se

The Setup Utility screen appears.

14.6.2.5 Booting using NVRAM

This section explains the procedure for booting using NVRAM.

Setting NVRAM for boot monitors 3.0 and above

From the Setup Utility, complete the fields shown Table 68. The boot parameters are different for a Network Station containing the flash card and a Network Station that uses the peer boot.

Table 68. Setting NVRAM for boot monitors 3.0 and above

Keys	Fields	Values for NS containing the flash card	Values for peer booting NS
F2	PCMCIA Card entry	Verify that the card has been successfully configured.	
F3	IP Addressed from	NVRAM	NVRAM
	Network Station IP Address	Your NS IP address	Your NS IP address
	Boot Host IP Address: First Host Second Host Third Host	 0.0.0.0 0.0.0.0 Your MetaFrame or WinFrame server IP address	 IP address of the NS with card 0.0.0.0 Your MetaFrame or WinFrame server IP address
	Configuration Host IP Address	0.0.0.0	0.0.0.0
	Gateway	Your Gateway IP address	Your Gateway IP address
	Subnet Mask	Your subnet mask	Your subnet mask
	Broadcast IP Address	Your broadcast IP address	Your broadcast IP address
F4	Boot file		
	TFTP Boot Directory		
	NFS Boot Directory		/peerboot/

Keys	Fields	Values for NS containing the flash card	Values for peer booting NS
	Boot Host Protocol: TFTP order NFS order Local Order	 Disabled Disabled 1	 Disabled 1 Disabled
F5	Configuration File	flash.nsm or flashlb.nsm (load balancing with direct connection) or flashbc.nsm(load balancing with broadcast capability)	peer.nsm or peerlb.nsm (load balancing with direct connection) or peerbc.nsm(load balancing with broadcast capability)
	Configuration Directory First	/local/configs/	/peerboot/configs/
	Configuration Host Protocol: First Second	 Default Default	 Default Default
F7	F2 Select a keyboard language		

Setting NVRAM for boot monitors prior to 3.0

From the Setup Utility, complete the fields shown in Table 69. The boot parameters are different for a Network Station containing the flash card and a Network Station that uses the peer boot.

Table 69. Setting NVRAM for boot monitors prior to 3.0

Key	Field	Value for NS containing the flash card	Value for peer booting NS
F4	PCMCIA Card entry	Verify that the card has been successfully configured.	
F5	IP Addressed from	NVRAM	NVRAM
	Network Station IP Address	Your NS IP address	Your NS IP address
	Boot Host IP Address: First Host Second Host Third Host	 0.0.0.0 0.0.0.0 Your MetaFrame or WinFrame server IP address	 IP address of the NS with card 0.0.0.0 Your MetaFrame or WinFrame server IP address
	Gateway	Your Gateway IP address	Your Gateway IP address
	Subnet Mask	Your subnet mask	Your subnet mask
	Broadcast IP Address	Your broadcast IP address	Your broadcast IP address
F6	Boot file		
	TFTP Boot Directory		
	NFS Boot Directory		/peerboot/
	Boot Host Protocol: TFTP order NFS order MOP order Local Order	 Disabled Disabled Disabled 1	 Disabled 1 Disabled Disabled

Key	Field	Value for NS containing the flash card	Value for peer booting NS
	Configuration File	flash.nsm or flashlb.nsm (load balancing with direct connection) or flashbc.nsm(load balancing with broadcast capability)	peer.nsm or peerlb.nsm (load balancing with direct connection) or peerbc.nsm(load balancing with broadcast capability)
	Configuration Directory		/peerboot/configs/

14.6.2.6 Booting using DHCP

There is no DHCP option to pass the Third Boot Host parameter, which is what the ICA client uses to determine to which MetaFrame, WinFrame, or WinCenter server to connect. You must set this value in NVRAM.

Set up the Network Station as described for NVRAM booting. Select **DHCP** from the F3 or F5= Set Network Parameters menu.

There is also no option to pass in the Configuration File value. Again, you must set this option (flash.nsm,flashlb.nsm, flashbc.nsm, peer.nsm, peerlb.nsm, or peerbc.nsm) directly in NVRAM.

DHCP provides a Network Station that boots from the QuickOn for Running Windows flash card with an IP address and other limited DHCP options. These DHCP options, when entered correctly, do not interfere with QuickOn for Running Windows.

These options include:

- Option 1: Subnet Mask
- Option 3: Router
- Option 6: DNS Server
- Option 15: Default Domain

Do not set any other options at the MAC, class, subnet, or system level for a Network Station that boots from the QuickOn for Running Windows flash card.

14.6.2.7 Peer booting using DHCP

If you choose to peer boot your Network Stations and if you use DHCP, the Network Stations with the QuickOn for Running Windows flash card must have fixed IP addresses.

Set up the Network Stations and the DHCP server as described in the previous section. For the peer booting Network Stations, you must also add DHCP Option 66, TFTP Server, with the IP Address of the Network Station with the flash card.

If you have multiple Network Stations with flash cards in a given subnet, you have two choices. You may define Option 66 at the MAC level for every Network Station, or you may create multiple scopes in a given subnet, and group the scopes.

14.6.2.8 Network Station boot with the new parameters

If the boot monitor is down-level, a screen that indicates a boot monitor refresh appears. *Do not touch the system during the boot monitor update*. The Network Station automatically reboots when the update completes.

You may see one of these messages in red:

- `NS0830 Boot from PCMCIA card failed`
- `NS0830 NFS failed file 'kernel.Z' not found`

Ignore these messages.

After the reboot, if you get a blue screen with the Console window, something has been set up incorrectly. Check the Configuration Directory settings by pressing F5 on the Setup Utility, or clear NVRAM and re-enter the configuration information.

14.7 Advanced miscellaneous ICA topics

This section contains helpful tips on some advanced ICA topics.

14.7.1 Precedence order for ICA connection records

The current schema for precedence of ICA connection records in the ICA Remote Application Manager is: NSM (NC Registry) first, then user's appsrv.ini file if it exists, or if it does not exist, the system appsrv.ini file. This precedence information is important for understanding what connection records will appear in the Remote Application Manager (wfcmgr). Since the ICA code was designed to use the connection description as the unique field, two records cannot be added with the same description.

A problem can occur if or when NSM has a connection record with a description that is the same as one found in either of the appsrv.ini files. Currently the NSM connection record takes precedence and the duplicate will not be shown to the user.

Another problem can occur since NSM doesn't guarantee unique names for each connection record. It is possible for two records to exist in NSM with the same description. In this case, only the first record encountered will be shown to the user.

14.7.2 Copying and pasting text and graphics

The ICA client automatically transfers simple text, RTF text and DIB/BMP graphics between the X Windows and Windows clipboards. This way, you can copy or cut and paste freely between X Windows and Windows applications or between Windows applications on the same or different Citrix servers.

- RTF Rich Text Format (Both sending and receiving applications must use the same code page)
- DIB Windows Device Independent Bitmap
- BMP Windows Bitmap

All applications involved with the copy and paste operations must be capable of handling the data formats involved. The ICA client does not do data conversions.

To copy text or graphics from Windows to X Windows, follow these steps:

1. Select the text or graphic you want to copy from the Windows application.

2. Select **Copy** from the Windows application's **Edit** menu. The text or graphic is copied to the Windows clipboard.
3. Switch to the X application you want to use.
4. Choose the appropriate command from the X application to paste in the text or graphic you copied.

To copy text or graphics from X Windows to Windows, follow these steps:

1. Select the text or graphics you want to copy.
2. Choose the appropriate command from the X application to copy the text or graphics. The text or graphic is copied to the Windows clipboard.
3. Switch to the ICA client.
4. Select **Paste** or **Paste Special...** from the **Edit** menu of the Windows application to paste the text or graphic.

14.7.3 Connecting to local printers

With the ICA client you can print to any spooled printer available from your IBM Network Station. Such printers may be connected to the parallel port or the serial port. Printers can be connected automatically or manually.

14.7.3.1 Automatic connection

Using Network Station manager (NSM), local printers need only to be set up once to enable automatic connection to ICA sessions.

To automatically connect printers during the ICA logon, two actions need to happen. First, the ICA client needs to be able to provide the ICA server with the Windows NT printer driver name for each of the Network Station printers. Second, the Windows NT printer driver must be installed on the ICA server. The correct printer driver name can be found by using the Printer Wizard on the ICA server (see the following steps for determining the correct printer driver value). The Network Station ICA client takes the Windows NT printer driver name from the Network Station Manager (NSM) description field of the printer. The printer driver name is entered into the description field via the NSM printer configuration screens.

Once the printer driver name has been added via NSM and the Network Station in question has been rebooted, you can log in to the ICA server and bring up the **Control Panel-> Printers** window. You can see the printers that were auto created. If you do not see the printers, you should bring up the **Programs->MetaFrame Tools->Client Printer Configuration** screen and make sure that the data they entered was correct and available to the ICA server.

The steps for determining the correct Windows NT printer driver name are listed here:

1. On the ICA server computer, click **Start->Settings->Printers**.
2. Double-click the **Add Printer** icon. Select **My Computer**, and then click **Next**.
3. In the Available Ports list box, select **LPT1**, and then click **Next**.
4. In the left pane, select the **Manufacturer** of the printer you installed on your Network Station. In the right panel, scroll to the model of the Printer you want the Terminal Server to load as the printer driver.

This is the server printer driver name that you want to use. Write this name down. This exact name will be entered via NSM into the description field of the printer you are configuring.

14.7.3.2 Manual connection

Manual connections to local printers must be done each time an ICA session is established.

To print to a local printer in WinFrame, follow these steps:

1. In the Main program group, double-click the **Print Manager** icon.
2. In the Printer Manager window, you should see an icon or open dialog box for a network printer with a name similar to **workstation#printer**. Here, *workstation* is the IBM Network Station name, and *printer* is the IBM Network Station name for the printer.
3. If no client printer is available, select **Connect to Printer?** from the Printer menu.
4. Double-click the **Client Network** icon in the Shared Printer list.
5. Double-click the **Client** icon.
6. Select the client printer icon that has a name similar to **workstation#printer**, and click **OK**.
7. If you want this printer to be your default printer select, it in the Default menu at the top of the Printers window.

To print to a local printer in MetaFrame, follow these steps:

1. Click **Start** on the task bar, point to **Settings**, and click **Printers** on the submenu.
2. In the Printers window, you should see an icon for a network printer with a name similar to **workstation#printer**. Here, *workstation* is the IBM Network Station name, and *printer* is the IBM Network Station name for the printer.
3. If no client printer is available, double-click the **Add Printer** icon in the Printers window to run the **Add Printer Wizard**.
4. Click the **Network** printer server. Then, click **Next**.
5. Double-click **Client Network**, and double-click **Client**.
6. Select the printer from the list displayed, and click **OK**.
7. Spooled printers available on the IBM Network Station have a name similar to **workstation#printer**.
8. If you want this printer to be your default printer, click **Yes**, and then click **Next**.
9. Click **Finish** to complete the process.

Note: The ICA client printer support is not bi-directional. This means that the printer cannot answer or originate messages.

14.7.4 Connecting to local serial devices

With the ICA client, you can use serial devices attached to any of the COM ports on your IBM Network Station. COM port mapping does not happen automatically. To map a client COM port, follow these steps:

1. Start the ICA client and logon to the Citrix server.
2. Start a DOS command prompt.
3. At the prompt, type: `net use comX: \\client\comZ:`

   Here, *X* is the number of the COM port on the server (ports 1 through 9 are available for mapping), and *Z* is the number of the client COM port to which you want to map. Press Enter.
4. To confirm the operation, type `net use` at the prompt. The list that appears contains mapped drives, LPT ports, and mapped COM ports.

To use this COM port in a session on a Citrix server, install your device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session on the server. Use this mapped COM port as you would a COM port on the client computer. The IBM Network Station ICA client can map any of the four virtual serial ports (com1 through com4) to any of the defined tty ports (/dev/tty00 through /dev/ttynn) on the Series 300, Series 1000, and Series 2800 Network Stations.

On the Series 2200 Network Station, there are USB ports, not serial ports. However, USB to serial port boxes can be used and any of the four virtual serial ports (com1 through com4) can be mapped to any of the defined USB/tty ports (/dev/utty00 through /dev/uttynn).

Series 300 and Series 1000
/dev/tty00 base serial port on the planar board
/dev/tty01 A plug on the multiport serial card
/dev/tty02 B plug on the multiport serial card
/dev/tty03 C plug on the multiport serial card
/dev/tty04 D plug on the multiport serial card

Series 2200
/dev/utty00A plug on USB to serial port box
/dev/utty01B plug on USB to serial port box
...

Series 2800
/dev/tty00 serial port 1 on the planar board
/dev/tty01 serial port 2 on the planar board
/dev/tty02 A plug on the multiport serial card
/dev/tty03 B plug on the multiport serial card
/dev/tty04 C plug on the multiport serial card
/dev/tty05 D plug on the multiport serial card

Note: COM port mapping is not TAPI compatible. TAPI devices cannot be mapped to client COM ports.

14.7.5 Low bandwidth considerations

The ICA client has several performance tuning options that can be set, most of which address network traffic reduction. Network topologies vary greatly as does the instantaneous load they bear. You may need to experiment with the following tuning options to see how they best work in your network.

14.7.5.1 Number of colors

The ICA protocol supports 16 and 256 colors. Selecting 16 colors produces less network traffic than 256 colors. Operating the ICA server in the same color mode (16 or 256 colors) saves a color conversion on the server side. On the IBM Network Station, 16-color image data takes more processing power than 256 colors.

The default is 256 colors.

14.7.5.2 TCP buffering

If your network topology involves any low bandwidth segments and you notice slow performance due to the large number of ica packets being sent over the wire, you can configure the ICA connection to use a low bandwidth optimization algorithm for small packet transmissions. This decreases the overall number of packets sent on the wire, which in some low bandwidth situations may improve the overall performance. This should not be used in high bandwidth environments since it can actually slow down the user interface performance.

To enable the low bandwidth optimization algorithm, add the following option to the extra options section of your connection in NSM. Or, add it to your command line parameters if you are creating your own ICA client commands:

```
-TcpNoDelay No
```

The default is `-TcpNoDelay Yes`.

14.7.5.3 Audio quality levels

There are three selectable audio quality levels: low, medium, and high. These levels also represent the amount of network traffic that audio requires. For example, low audio quality produces less network traffic than high audio quality.

The default is medium.

14.7.5.4 Persistent caching

Persistent caching only helps in very low bandwidth situations, for example, connecting through a modem. In high bandwidth networks, persistent caching may actually decrease performance.

The default is no persistent caching.

14.7.5.5 Compression

ICA protocol compression results in reduced network traffic at the expense of processing power required to run the compression algorithms.

The default is compression on.

Chapter 15. Accessing Lotus Domino from the Network Station

This chapter focuses on the different ways you can access a Lotus Domino environment from an IBM Network Station. It also has examples of installing a Windows application on Windows NT Terminal Server Edition and the configuration of Netscape Communicator (Navigator, Messenger, Address Book, and News).

eSuite has been withdrawn from marketing

After a long evaluation and careful assessment of business priorities, Lotus has decided to realign the marketing and development resources that currently support the eSuite offering. A core eSuite development team will be maintained to provide support for current eSuite customers and to evaluate options for integrating eSuite technologies into the Lotus Domino and Notes platforms, and into IBM WebSphere.

Lotus eSuite is not supported for V2R1 of the Network Station. If you are currently using eSuite with your V1R3 Network Station, visit the Lotus Web site at: `http://www.lotus.com/home.nsf/welcome/esuite1`

15.1 Lotus Domino

Lotus Domino is an integrated messaging and Web application software platform. With Domino, you can develop and deliver secure, interactive Web applications and take advantage of a rock solid infrastructure for messaging and collaboration. Domino integrates in a single product, messaging, security, systems management, data distribution, replication, and application development.

Refer to the Lotus Web site `http://www.lotus.com` for more information about Lotus Domino.

Domino refers to the server part of the product. Different clients can access a Domino server in different ways:

- **Notes clients**: Can access Notes applications on the server using Notes protocol. They can access mail using Notes protocol, POP3, or IMAP. And, they can access news groups and discussion databases using Notes protocol or NNTP.
- **Web clients**: Access Notes applications and mail on the server using HTTP and send mail to the server using SMTP.
- **POP3 clients**: Access mail on the server using POP3 and send mail to the server using SMTP.
- **IMAP clients**: Access mail on the server using IMAP and send mail to the server using SMTP.
- **LDAP clients**: Access directory (for example, the address book) on the server using LDAP.
- **NNTP clients**: Access news groups and discussions databases on the server using NNTP.

15.1.1 Domino and Network Station integration

The Domino environment to which we have connected the Network Station, is a *Lotus Domino Server Release 5.0*. Release 4.6 of the product could have been used as well although some advanced features would not be available, especially for the Web client.

15.1.1.1 Domino clients on the Network Station

All client types are available from the Network Station environment. Table 70 indicates the Network Station applications corresponding to the Domino clients.

Table 70. Network Station applications corresponding to Domino clients

Domino clients	Network Station applications
Notes client	ICA session to a Windows NT multi-user server with Lotus Notes client
Web client	Netscape Navigator 4.5
POP3 client	Netscape Messenger 4.5
IMAP client	Netscape Messenger 4.5
LDAP client	Netscape Address Book 4.5
NNTP client	Netscape News 4.5

Figure 393 shows an overview of the connections of the different Network Station applications to the Domino server and the required Domino services.

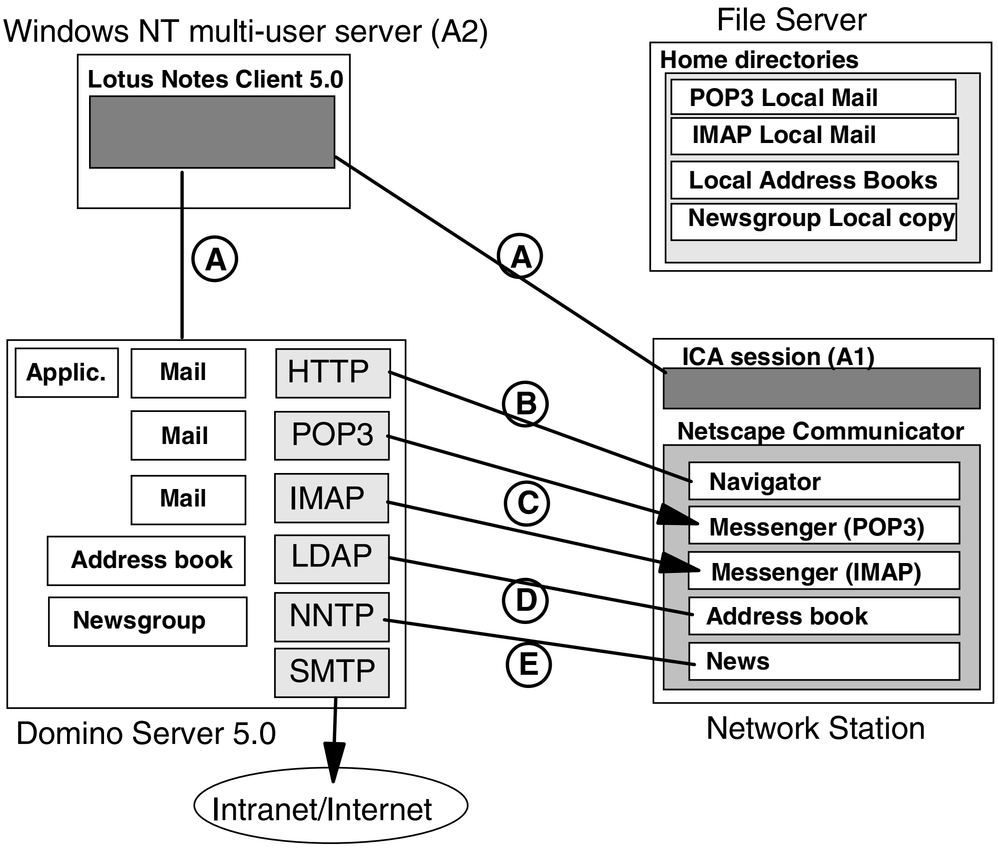


Figure 393. Domino environment

In Figure 393, the following connections are shown:

- An ICA session connection to a Windows NT multi-user server running the Lotus Notes client application. The Lotus Notes client connects to the Domino server using Notes protocol (A).
- A Netscape Navigator connection using HTTP (B).
- A Netscape Messenger connection using POP3, IMAP, and SMTP (C).
- A Netscape Address Book connection using LDAP (D).
- A Netscape News connection using NNTP (E).

The configuration of the Domino services that we implement to access Domino from the Network Station, is almost identical between Release 5.0 and Release 4.6 of the product, except for the SMTP service.

Each Network Station Domino client and Domino service setup is explained in the following sections. First, we indicate how these clients differentiate from each other.

15.1.1.2 Domino clients comparison

The Domino clients are compared in Table 71 in terms of accessibility to a Domino server.

Table 71. Domino clients accessibility comparison

Domino clients on the Network Station	Domino applications & and databases	Notes mail and calendar	POP3 mail	IMAP mail	Address Book	NewsGroup
Notes client	Yes	Yes	Yes	Yes	Yes	Yes
Netscape Navigator	Yes	Yes			Yes	Yes
Netscape Messenger (POP3)			Yes			
Netscape Messenger (IMAP)				Yes		
Netscape Address Book					Yes	
Netscape News						Yes

Within a Lotus Domino/Notes environment, the best Network Station solutions are to use *Netscape Navigator* to provide Web browser access to Domino, or to use the *Lotus Notes client* on a Windows NT multi-user server. Netscape Navigator provides access to most Notes facilities, where the Lotus Notes client provides full access to Notes, but requires the additional expense of a Windows NT multi-user system and software. Both solutions let you access Notes mail and calendar, address book, newsgroup, and other Domino applications or databases.

With Lotus Domino Release 5, there is now greater similarity of use between a Notes 5 client on Windows and Netscape Navigator on the Network Station. Lotus Domino Release 5 has indeed added more Notes functions for browsers. The Windows Lotus Notes 5 client user interface is much more like the Internet Explorer 4 Web interface.

Even though the user interface has become similar, the Web client (Network Station Netscape Navigator) doesn't implement some of the Notes features like full rich-text input, security based on a Notes ID file, signed and encrypted data, input of graphical data, and database local replication.

The Netscape mail and news clients provide other approaches to access mail files and newsgroups on a Domino server, which may sometimes be beneficial in particular environments.

15.1.1.3 Domino mail comparison

First, we look at the characteristics of the types of mail Domino can handle.

Electronic mail application

Let's start first with a review of the electronic mail evolution.

On the Internet, the *Simple Mail Transfer Protocol (SMTP)* has been in use for many years, as a means of transporting mail. It was originally limited to basic "flat" unformatted text only, but later the *Multipurpose Internet Mail Extensions (MIME)* allowed other data formats, including binary attachments, to be added to the flat text. These allow formatted word processor documents to be sent, but require the recipient to have the same or compatible word processor software. There have been no agreed standards to carry "rich text". More recently, some mail systems have been adding a MIME attachment in Hypertext Markup Language (HTML) format, containing a rich text version, together with a flat text version for older mailers. This can convey richer formatting. But, again, there is only limited support in mailers, and recent developments in Extensible Markup Language (XML) may change it again.

The SMTP protocol only specifies how mail is transferred, not what the sender or receiver can do with the mail. It expects to be able to deliver the mail to the recipient's computer using store-and-forward techniques if that computer is temporarily unavailable.

Increasing demand for mobile access from many locations led to the development of other mail protocols, in particular the protocols *Post Office Protocol (POP3)* or *Internet Message Access Protocol (IMAP4).* With these protocols, a central mail server is used to hold mail being sent to a user, in their own personal mailbox. The mail server receives this mail using standard SMTP. Then, the user can log into the server and download the mail using POP3 or IMAP4 protocols. Because those protocols are only used to receive mail, a different method is required for sending mail. Outgoing mail is transmitted by SMTP to a mail server, usually the same mail server holding the user's mailbox, but sometimes to a different SMTP server. POP3 and IMAP4 both allow users to download mail and then work offline. This is of limited use to LAN-based Network Stations.

A recent development is to use *HTTP Web-based mail servers* (not to be confused with the HTML MIME attachments). A Web browser is used to access the mail server, which then returns mail items as Web pages. Depending on the Web server, mail can be saved in different folders and may allow the rich text format for incoming mail. When a message needs to be sent, an HTML form is sent by the Web server. The user can fill in the message, and then send the form to the server, which converts it into normal SMTP format. This outgoing mail content is limited to the flat text that can be entered into an HTML form, although some systems allow limited rich text (using Java applets) and formatted attachments to be included as well. There may be additional limits on the total amount of text that can be sent.

Because of the limitations of content or facilities in each of the mail services above, more proprietary mail services such as *cc:Mail* or *Lotus Notes* mail have become popular. These services provide many more facilities for handling the mail and creating rich text content. To preserve all the mail properties, they require both the sender and recipient to have the same or compatible mail systems, and generally require special mail client software on each user's computer. Therefore, they are commonly used within corporate intranets. These systems are usually provided with mail gateways to SMTP mail, but any extra formatting and facilities, such as notification of delivery, are lost when passing through the gateway, even if the destination runs the same mail software.

Storing mail

Most mail users require a way of storing and organizing their mail. The mail could be stored on the mail server itself, or on the client, or copies could be kept on both. The advantages of each method are highlighted here:

- Storing mail at the server allows users to see the same mail items regardless of the workstation from which they access it. However, they need an online connection to view the mail.
- Storing mail on the client allows offline access to mail. But, it is difficult to use on more than one client workstation, since each client would save a separate set of messages.
- Storing mail at both the server and client potentially allows both online and offline access. Mail clients may provide synchronization facilities such as Lotus Notes' replication. In this case, the implementation needs to be investigated to ensure that if more than one client workstation is used, it supports the server and multiple local clients being kept in step.

Network Stations add another variant. They can provide a “local” client mail file, which is actually a directory on the server supporting the Network Station. This may be on the same system as the mail server or on a completely different system. This means that a user moving between several Network Station clients can see the same client mailboxes, without needing to keep a synchronized copy on the mail server.

To add to the confusion, the various mail protocols provide different server storage facilities:

- POP3 allows the user to keep mail on the mail server in a *single* mailbox, or to move mail to the local mail client, and to selectively delete messages. POP3 clients may choose to delete messages automatically as they are copied or leave the server copy alone, until it is explicitly deleted. POP3 clients may implement multiple folders, but these are always local to the client. The protocol does not allow a client to store modified messages on the server.
- IMAP4 adds multiple server mailbox folders. IMAP4 clients may work entirely with these server folders, or work with a local copy of mail while leaving the original on the mail server. Clients may also implement local folders, which may be synchronized with the server, or may have a totally different structure. Clients may store messages back to the IMAP4 server. Therefore, IMAP4 can provide many of the replication facilities found in Lotus Notes.

- HTTP Web-based mail (where the mail is rendered into HTML pages and viewed on a browser) always keeps the mail on the mail server and may provide multiple server mailbox folders.
- Lotus Notes mail allows you to work with multiple server mailbox folders or allows you to replicate these folders to the Notes client. The replication facilities guarantee that server and client views will be kept synchronized.

Domino mail on the Network Station

As we have seen, Lotus Domino provides all the above types of mail service, including POP3/SMTP, IMAP/SMTP, HTTP/HTML, and Lotus Notes access. The Network Station supports the Domino clients that can access these mail services, Lotus Notes client, Netscape Navigator, and Netscape Messenger.

Table 72 shows the mail functions that are provided by each Domino client on the Network Station.

Table 72. Mail functions of a Domino mail client on a Network Station

	Rich text		**Attachment**		**Server folders**	**Client folders**	**Calendar**	**Address Book**
	Received	**Sent**	**Received**	**Sent**				
Notes Client R5 Notes mail and calendar access using Notes protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Netscape Navigator Notes mail and calendar access using HTTP	Yes	Yes[1]	Yes	Yes	Yes	**No**	Yes	Yes
Netscape Messenger POP3 mail access using POP3 protocol	Yes HTML[2]	Yes HTML[3]	Yes	Yes (file/URL)	**No**	Yes	**No**	Yes LDAP
Netscape Messenger IMAP mail access using IMAP protocol	Yes HTML[2]	Yes HTML[3]	Yes	Yes (file/URL)	Yes	Yes (not synch'd)	**No**	Yes LDAP

Notes:

1. A rich-text applet allows the user to create limited rich-text mail content.
2. The POP3/IMAP mail clients support rich text as an HTML/MIME attachment. However, the Domino server does not convert Notes rich text into this format, so it can only be viewed as flat text.
3. The POP3/IMAP mail clients optionally send rich text as an HTML attachment, together with a flat-text version. The attachment is not converted to Domino rich text by the server, or can it be displayed in rich text when received.

As mentioned previously, the best solutions are to use Netscape Navigator to access Domino using HTTP or to use the Lotus Notes client on a Windows NT multi-user server.

Under most circumstances, IMAP and POP3 mail access offer no real advantages over the previously mentioned methods. POP3 cannot access all Notes mail folders, which may prevent its deployment. Domino does not automatically convert between rich-text Notes mail and rich-text HTML attachments. If you need to integrate other (non-Notes) mail systems, especially those using HTML formatted mail, then IMAP or POP3 may have some advantages.

The following section studies the setup of each Domino client on the Network Station and the configuration of the required services on the Domino server.

15.1.2 Lotus Notes Client Release 5.0

The Lotus Notes client can be used from the Network Station through an ICA session (A1 in Figure 393 on page 482) that connects to a Windows NT multi-user server supporting the ICA protocol (A2). The Windows NT multi-user server can be a WinFrame server or a Windows NT Terminal Server Edition server with the MetaFrame add-on product. ICA sessions and the Windows NT multi-user server are potential elements of a Network Station environment that are thoroughly covered in Chapter 14, “Windows application access (ICA)” on page 403.

A Windows NT multi-user server is a Windows NT server with a multi-user server core that provides the ability to host multiple, simultaneous client sessions on the Windows NT server. Applications are installed and run on the server and only screen updates, keystrokes, mouse clicks, and audio commands pass between the session running on the user platform, which is the Network Station here, and the server.

To access a Domino R5.0 server with a Notes client R5.0 from a Network Station, perform the following steps.

1. Install and set up a MetaFrame (or WinFrame) server.
2. Install Lotus Notes Client R5.0 (shared installation) on the MetaFrame (or WinFrame) server.
3. Set up the Lotus Notes Client R5.0 for a template user. Automatic template files are copied to a user home directory at the first logon.
4. Set up the correct Windows NT permissions on the Notes directories.
5. Perform Notes administration and migration aspects.
6. Configure the Network Station Manager.

15.1.2.1 MetaFrame (or WinFrame) server installation and setup

See Chapter 14, “Windows application access (ICA)” on page 403, for information on installing and setting up a MetaFrame server.

In our example, the PC server used as the Windows NT multi-user server has the following configuration:

- IBM Netfinity 3000 (128 MB RAM, 380 MHz, 4 GB hard drive)
- Windows NT 4.0 Server Terminal Server Edition
- MetaFrame 1.8
- Service Pack 4 for Windows NT Terminal Server Edition

The hard disk has two partitions: one with the operating system (c:\ 2GB) and the other with the application code and user data (d:\2 GB).

Lotus Notes Client Release 5.0 requires on the server:

- 90 MB disk space
- 32 MB RAM for the application code and about 2.5 MB additional RAM per active Notes user

15.1.2.2 Lotus Notes Client Release 5.0 shared installation

To install the Lotus Domino client 5.0, complete these steps:

1. Log on to the MetaFrame server as Administrator.
2. Open a command prompt, and enter:

   ```
   Change user /install
   ```

   This command indicates to the system that the application installation must be handled in a multi-user way.
3. From the Notes CD autorun panel, select **Install->Clients->Lotus Notes->Custom Install** or launch **drive:\Clients\w32intel\setup.exe** directly from the CD.
4. Check the shared installation on the third window of the Notes Installation. You are also prompted for a name and company name on this screen.
5. On the next screen, make sure that the destination folder for the Notes code is the drive and directory corresponding to the application code (for example, d:\Lotus\Notes).
6. Deselect **Common data**, **Modem Command Script**, **Readme**, and **Optional Data files** in the Data files list. This only installs the required data from the Data files list because the other elements are available on the Domino server.
7. Notes Installation now copies all the files to your hard disk.
8. Click **Finish** when the `Successful Installation` message appears.

15.1.2.3 Setting up Lotus Notes Client R5.0 for a template user

To set up a Lotus Notes client at release 5.0 or a template user, complete these steps:

1. Create a directory as shown in this example: d:\TemplateUser.
2. Assign this physical directory to a virtual drive by substituting a directory (h:, for example, or any letter you want to use as the home drive for all your users) to the d:\TemplateUser directory. To do this, open a command prompt, and enter:

   ```
   subst h: d:\TemplateUser
   ```
3. Launch the Lotus Notes Shared setup by running:

   ```
   d:\Lotus\Notes\setup.exe
   ```
4. On the third window of the Lotus Notes Shared setup, when prompted for a name and company, do not enter a person’s name in the Name field since all users will get this setting. We recommend that you enter the company name in this field.
5. Specify `h:\Lotus\Notes\data` as the destination folder. The h: drive corresponds currently to the d:\TemplateUser directory (see step 2). In a Windows NT user session, it will correspond to their home directory on the server.

   Notes Shared setup now copies some files to the TemplateUser directory.

6. Click **Finish** when the `Successful Installation` message appears. Do not launch Notes now.
7. Move the **notes.ini** file from c:\wtsrv to h:\Lotus\Notes.
8. Edit the notes.ini file, and add the following line:

   ```
   WinNTIconPath=d:\Lotus\Notes\Data\W32
   ```

   It should appear as shown in the following example:

   ```
   [Notes]
   Directory=h:\Lotus\Notes\Data
   KitType=1
   InstallType=2
   WinNTIconPath=d:\Lotus\Notes\Data\W32
   ```

9. Move the **W32** directory from d:\TemplateUser\Lotus\notes\data to d:\Lotus\Notes\data. You will have to create the data directory.
10. Delete the d:\TemplateUser\Lotus\Notes\data\Help directory
11. Delete the MAIL50.NTF file in the d:\TemplateUser\Lotus\Notes\data directory.
12. Open a command prompt, and enter:

    ```
    Change user /execute
    ```

You now have two directories with Notes files installed:

- d:\Lotus\Notes is the Notes application code directory.
- d:\TemplateUser\Lotus\Notes\data is the Notes data directory for the template user.

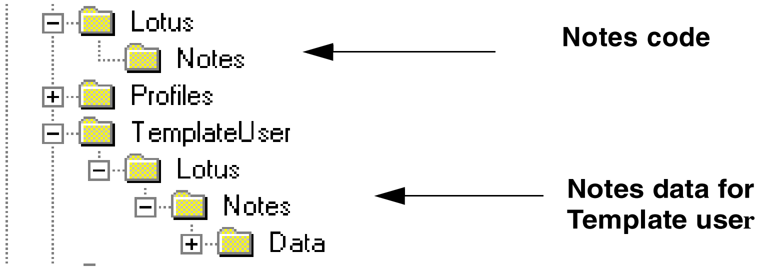


Figure 394. Lotus Notes Client installation directory structure

The “template” files are copied by a login script to each user’s home directory the first time they log on the server. By removing some files, you have limited the size of this directory to 6.53 MB.

15.1.2.4 Automatic copying template files to a user’s home directory

The procedure to implement the automatic copy of the template files to a user home directory at their first logon is described here:

1. Define a home directory for each user in User Managers for Domains. Select **Start->Programs->Administrative Tools->User Manager for Domains->User Properties->Profile**. In the Terminal Server Home Directory section, enter a home directory path for the user in the local path field, for example, `d:\users\%username%`

2. Define the H: drive as the substitution drive for each user's home directory. To do this, run the chkroot.cmd batch in the directory c:\wtsrv\Application Compatibility Scripts\. Enter `H:` as the RootDrive.

   The chkroot.cmd is normally launched the first time an administrator uses one of the compatibility scripts provided by Microsoft for installing standard Microsoft applications. By configuring the substitution drive for Lotus Notes in the same place, we are sure not to interfere with subsequent application installation.

   Refer to the Release Notes document on the Windows NT Terminal Server Edition CD for more information about the compatibility scripts.

3. Create a batch file called nclogin.bat in the c:\wtsrv\system32\repl\import\scripts\ directory that contains the following lines:

   ```
   if not exist h:\notes md h:\lotus
   if not exist h:\lotus\notes md h:\lotus\notes
   if not exist h:\lotus\notes\data md h:\lotus\notes\data
   if not exist h:\windows\notes.ini copy
   "d:\TemplateUser\Lotus\Notes\data\*.*" "h:\lotus\notes\data"
   if not exist h:\windows\notes.ini copy
   "d:\TemplateUser\Lotus\Notes\notes.ini" "h:\windows\notes.ini"
   ```

4. Assign the login script to all users in User Manager for Domains. Click **Start->Programs->Administrative Tools->User Manager for Domains**. While holding down the Ctrl key, click on all the users who will be using Notes. Once all desired users are selected, click **User->Properties**. Select **Profile**, and enter `nclogin.bat` in the login Script field.

5. Create a Common icon for all users to run Lotus Notes. Right-click the Start button, and select **Explore All Users**. Under **Profiles->All Users->Desktop**, click **File->New->Shortcut**. Enter `d:\Lotus\Notes\notes.exe` for the command line, and click **Next**. Enter `Lotus Notes` for the description, and click **Finish**.

6. Right-click the newly created Lotus Notes Shortcut. Select **Properties**. Click the **Shortcut** tab, and change the Start In field to:

   ```
   h:\lotus\notes\data
   ```

You can also configure a Lotus Notes published application to take advantage of the Load Balancing services. See Chapter 14, “Windows application access (ICA)” on page 403, for more information about Load Balancing Services and how to configure Lotus Notes as a published application.

Now when a user logs on the next time, their user directory will be automatically mapped to h:\. Also, the Lotus Notes client will be set up as an application in their directory (Figure 395).

The first time Notes is started, it will use the default notes.ini file copied by the login script, nclogin.bat, from the Template directory to the user home directory. The user will have to specify their name and mail server or to provide their Notes ID file on the first window to connect to the Domino server.

The next time, Lotus Notes will look for the Notes configuration files (notes.ini, desktop configuration, and so on) and application (local mail file, and so on) in the user home directory.

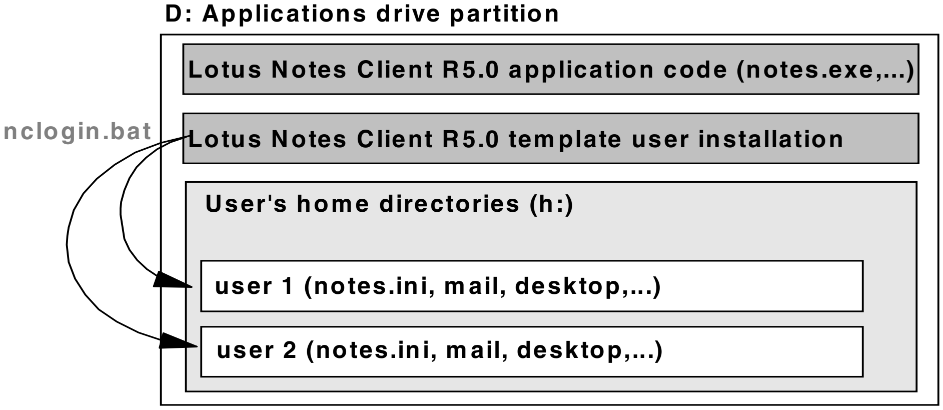

D: Applications drive partition
Lotus Notes Client R5.0 application code (notes.exe,...)
nclogin.bat
Lotus Notes Client R5.0 template user installation
User's home directories (h:)
user 1 (notes.ini, mail, desktop,...)
user 2 (notes.ini, mail, desktop,...)

Figure 395. Automatic template files copy

15.1.2.5 Windows NT permissions setup on the Notes directories

The Windows NT multi-user server will be accessed by all users. Therefore, it is important to correctly set the access permissions on each directory we created. You would not want, for example, a user to delete the Notes application code or access another user home directory.

The permissions should be set as shown in Table 73.

Table 73. Directories permissions setup

Description	Directory	Permissions
Lotus Notes Client R5.0 application code	d:\Lotus\Notes	Administrators: Full Control Everyone: Read(RX)(RX)
Lotus Notes Client R5.0 template user installation	d:\TemplateUser\Lotus\Notes	Administrators: Full Control Everyone: Special Access (R)(RX)
User’s home directory	d:\Users\%username%	Username: FullControl (Default)

15.1.2.6 Notes administration and migration aspect

The only issue remaining is how to distribute the Notes ID files and the migration of existing Lotus Notes user’s settings. However, this issue is a standard Lotus Notes administration issue that will be left to the Lotus Notes experts.

15.1.2.7 Network Station Manager configuration

To allow a user to start an ICA session pointing to the server where the Lotus Notes application resides, you need to add and configure an ICA session button on the Network Station desktop launch bar. This is done with Network Station Manager.

Such a configuration to access Lotus Notes as a published application, is thoroughly explained in Chapter 14, “Windows application access (ICA)” on page 403.

15.1.3 Web browser client

The Web browser client shipped with the Network Station is Netscape Navigator 4.5. This covers the configuration of a Domino server and Network Station

Manager to access Domino applications and the Mail and Calendar database from the browser. To set this up, you need to perform the following steps (Figure 396):

1. Configure the Domino server HTTP settings, and start the HTTP service.
2. Give the users mail databases, and assign an Internet password for the user.
3. Give the Network Station users access to Netscape Navigator.
4. Enable Java support for the Netscape application.

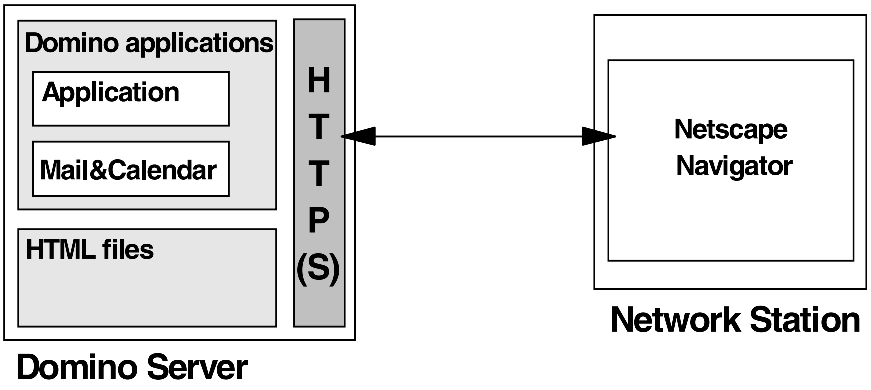


Figure 396. Domino HTTP service

15.1.3.1 Domino HTTP service configuration

Domino can act as a Web application server. It can serve pages to Web browsers that are stored in either the file system or in a Domino database.

When a Web browser requests a page from a Domino application, Domino translates the document into HTML. When a Web browser requests a page in an HTML file, Domino reads the file directly from the file system. Then the Web server uses the HTTP protocol to transfer the information to the Web browser.

HTTP service startup

To start the Domino Web server service, type the following server command on the Domino console:

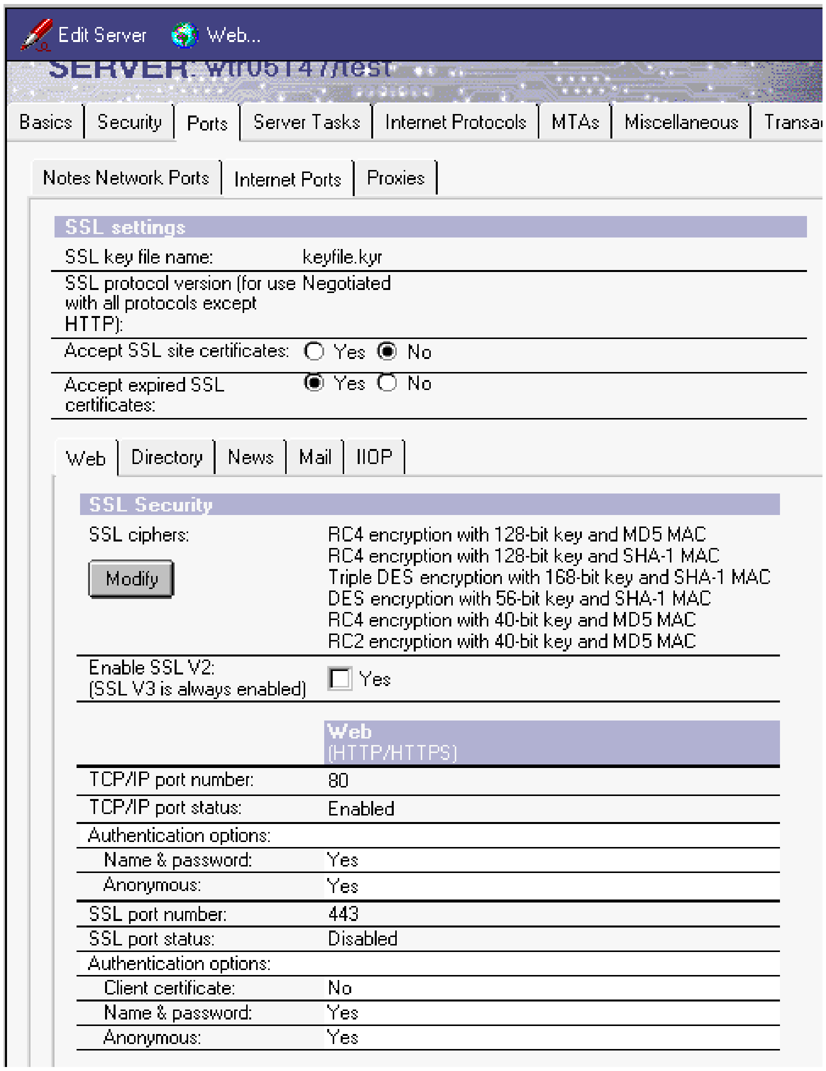
```
load http
```

Security setup

A Web user must authenticate with the Domino server before they can access a Domino application from a browser unless anonymous access to the application is authorized. Domino supports basic user name and password authentication and Secure Sockets Layer (SSL) authentication as well as SSL encryption. The HTTP default security configuration is the basic user name and password authentication.

To modify the default HTTP configuration (TCPIP port, security), from the Lotus Domino Administrator client, perform these steps:

1. Select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab. Then, open the server document for the server that runs the HTTP service
4. Click these tabs in order: **Ports->Internet Ports->Web** (Figure 397).



SSL settings

SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL certificates:	● Yes ○ No

SSL Security

SSL ciphers:	RC4 encryption with 128-bit key and MD5 MAC RC4 encryption with 128-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC DES encryption with 56-bit key and SHA-1 MAC RC4 encryption with 40-bit key and MD5 MAC RC2 encryption with 40-bit key and MD5 MAC
Enable SSL V2: (SSL V3 is always enabled)	□ Yes

	Web (HTTP/HTTPS)
TCP/IP port number:	80
TCP/IP port status:	Enabled
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	443
SSL port status:	Disabled
Authentication options:	
Client certificate:	No
Name & password:	Yes
Anonymous:	Yes

Figure 397. Web Configuration

Notes mail and calendar database

The standard Notes mail and calendar database is an example of a Domino application that can be accessed from a browser (Web client) and from the Notes client. A mail database is automatically created by Domino once an administrator registers a new Notes user.

To register a Notes user, from the Lotus Domino Administrator client, complete these steps:

1. Select **File->Open server**.
2. Select a server to administer.
3. Click the **people & groups** tab.
4. Expand the **Tools** list and **People** List.
5. Click **Register** and complete the fields.

We have created a Notes user called Carla Sadtler on the server *wtr05147/test*, belonging to the *testdomain* Notes domain, with the following parameters:

- Basic tab

  First name: Carla
  Last Name: Sadtler
  User Name: Carla Sadtler/test, Carla Sadtler
  Short name: csadtler
  Internet password: A password of your choice

- Mail tab

  Mail system: Notes
  Domain: testdomain
  Mail server: wtr05147/test
  Mail file: mail\csadtler
  Internet address: CarlaSadtler@nstation.com

15.1.3.2 Netscape Navigator configuration through NSM

Next, make sure the users have the Netscape Navigator available on the Launch Bar and that Java support is enabled.

Netscape Communicator icon on the Network Station Launch Bar

To enable access to the Web client from any Network Station, the NSM administrator must ensure that Netscape Communicator is included in the Launch Bar of the Network Station desktop (this is the default).

To do this, complete these tasks:

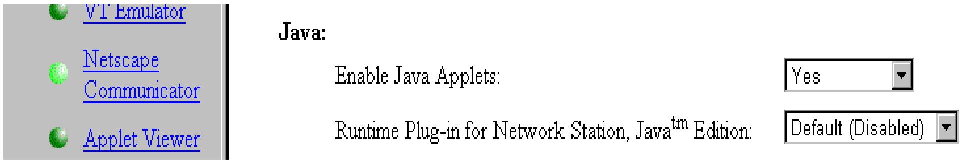
1. Log on to NSM using a user name that is part of the NSMAdmin group.
2. Select the **System** preferences level.
3. Select **Desktop->Launch Bar**
4. Verify that the Launch Bar Content list box contains Netscape Communicator. If not, select Netscape Communicator from the application list box, and add it to the Launch Bar Content list box.

Java support

The Notes mail file, when accessed from a browser, will use some Java applets (view applet, navigator applet, rich-text applet). Therefore, the NSM administrator must enable Java applet support for Netscape Communicator.

To do this, complete these steps:

1. Log on to the NSM using a user name that is part of the NSMAdmin group.
2. Select the **System** preferences level.
3. Select **Applications->Netscape Communicator**.
4. Scroll down to the Java Settings section and Enable Java Applets (Figure 398).



Java:

Enable Java Applets: Yes

Runtime Plug-in for Network Station, Java^{tm} Edition: Default (Disabled)

Figure 398. Enable Java Applets: Yes

15.1.3.3 Domino application access from the Network Station

To access a Domino application from the Network Station browser using a basic user name and authentication, complete these tasks:

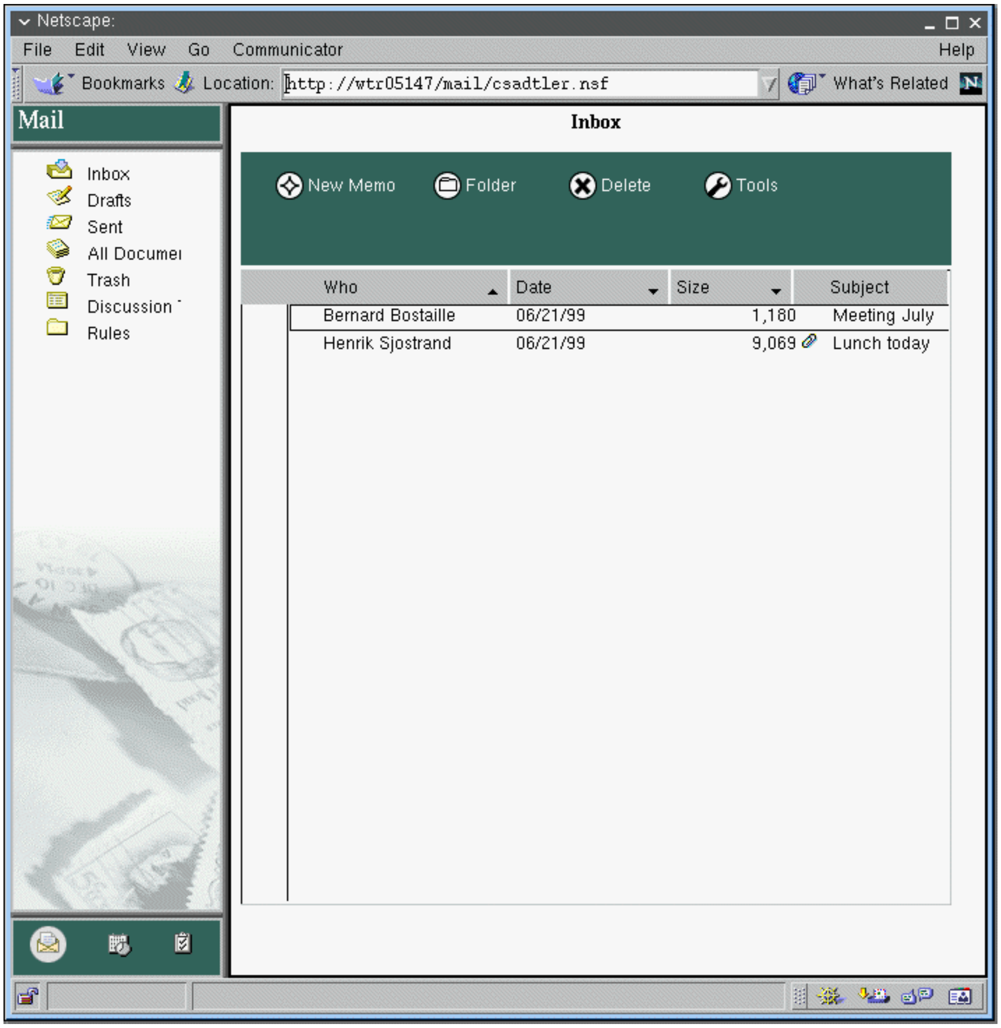
1. Click the **Netscape Communicator** icon to launch the program.
2. Type a URL with the following syntax in the browser location toolbar:

   ```
   http://DominoServerName/ApplicationName.nsf
   ```

   To access, for example, the standard Notes mail and calendar database of the user Carla Sadtler, type:

   ```
   http://wtr05147/mail/csadtler.nsf
   ```

3. Log on with the user name (for example, csadtler or Carla Sadtler) and the Internet password (Figure 399).



Location: http://wtr05147/mail/csadtler.nsf

Inbox

Who	Date	Size	Subject
Bernard Bostaille	06/21/99	1,180	Meeting July
Henrik Sjostrand	06/21/99	9,069	Lunch today

Figure 399. Notes Mail client from the Network Station browser

15.1.4 POP3 and IMAP Internet mail client

Internet mail clients can use Netscape Messenger from a Network Station to access their mail residing on a POP3 or IMAP server like Domino. The following list and Figure 400 on page 496 shows the elements of such a configuration.

- A Domino server running POP3, IMAP, and SMTP services
- A Network Station with Netscape Messenger
- A file server

The file server, as shown in Figure 400, is by default the Network Station boot server, where the user home directories reside.

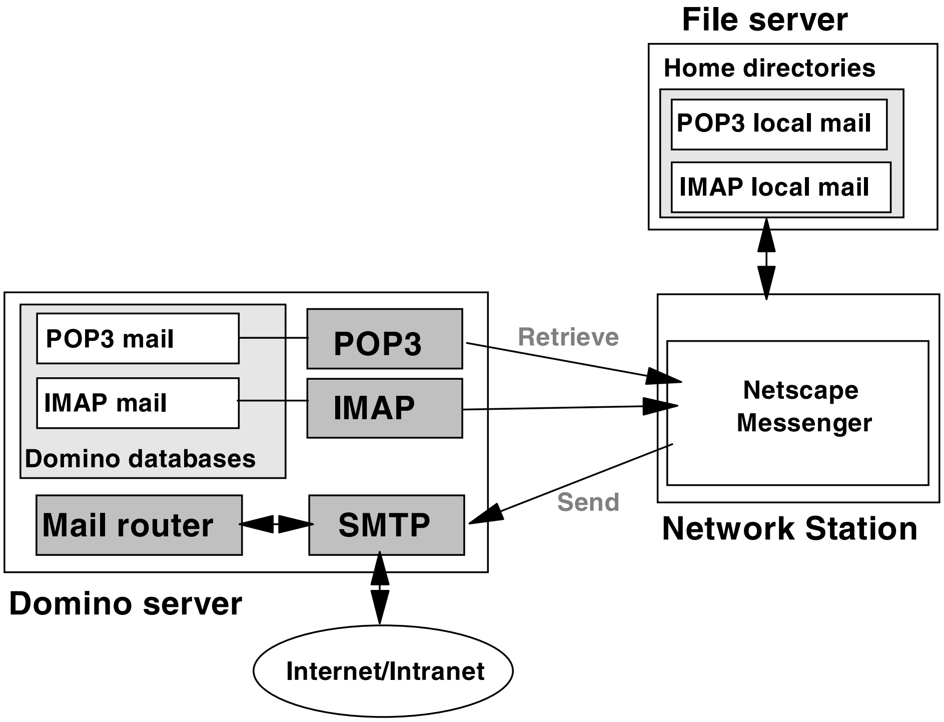


Figure 400. Network Station Internet mail client and Domino

Setting up for POP3 or IMAP access to a Domino server from a Network Station involves the following steps:

1. Define the users to the Domino server and define their mail system as POP or IMAP.
2. Create mail databases for the users.
3. Configure the Domino server Internet mail parameters.
4. Set up the SMTP service on the Domino server.
5. Use NSM to configure the launch bar for the users to include Netscape.
6. Use NSM to configure the mail environment for the users and to set the mail server type for the Netscape application.
7. Perform any advanced configuration for Netscape Messenger.

15.1.4.1 POP3 protocol

Post Office Protocol Version 3 (POP3) is an Internet mail protocol that allows POP3 clients to retrieve mail from a POP3 server and store them locally. In the case of a Network Station, the “local” mail files reside on a file server (boot server by default).

15.1.4.2 IMAP protocol

Internet Mail Access Protocol (IMAP) is an Internet mail protocol that allows for manipulation of mail in different modes. IMAP clients can:

- Retrieve messages from an IMAP server and store them locally (similar to a POP3 client)
- Access messages directly from the server
- Copy messages for offline use and then later synchronize them with mail on the server (however, synchronization is *not* available with the Network Station Netscape Messenger 4.5)

> **Note**
>
> In Netscape, normally you would see this option by right-clicking the folder (for example, New folder) and choosing Property folders. Clicking on the "download options" tab gives you the choice to download the folder.

IMAP clients can also share mailboxes that are equivalent to a Notes mail folder.

15.1.4.3 Domino POP3 and IMAP service configuration

A Domino POP3 server only stores and enables the retrieval of mail received by POP3 clients. A Domino IMAP server enables IMAP clients to access their messages directly on the server or to retrieve them.

None of the configuration tasks for POP3 and IMAP are involved with sending and delivering messages. These functions are handled by the Domino SMTP service and Domino mail routing. The configuration of the Domino SMTP service is covered in 15.1.4.4, "Domino SMTP service configuration" on page 499.

POP3 and IMAP services startup

To start the POP3 or IMAP server task while the Domino server is running, type one of the following server commands on the Domino console:

- POP3 server task: `load POP3`
- IMAP server task: `load IMAP`

POP3 and IMAP client setup

The setup of a POP3 or IMAP client on the Domino server involves the creation of a Person document and a mail file.

In the following steps, you create a Person document for a POP3 or IMAP user called *Bernard Bostaille* on the server *Mailserver.ibm.com/NstationCert* belonging to the *Nstationdomain* Notes domain. from the Lotus Domino Administrator client, perform these steps:

1. Select **File->Open server**.
2. Select a server to administer.
3. Click the **People & Groups** tab, and click **Add Person**.
4. Complete the **Basics** section:

   First name: Bernard
   Last Name: Bostaille
   User Name: Bernard Bostaille

Short name: bbostaille
Internet password: A password of your choice

5. Complete the **Mail** section

   Mail system: POP or IMAP
   Domain: testdomain
   Mail server: wtr05147/test
   Mail file: mail\bbostail
   Internet Address: BernardBostaille@nstation.com

6. Save the Person document.

To create the mail file for the POP3 or IMAP user *Bernard Bostaille*, follow these steps:

1. Choose **File->Database->New**
2. In the server field, select the **wtr05147/test** Domino server.
3. In the title field, enter:

   ```
   Bernard Bostaille's Mail
   ```

4. In the field name, enter:

   ```
   mail\bbostail.nsf
   ```

5. Select the template named **MAIL50.NTF**.
6. Click **OK**.
7. Choose **File->Database->Access Control List** (ACL), and give the user Bernard Bostaille Manager, with delete documents, access in the mail file ACL. Remove your name from the ACL.

For the IMAP client, in addition to the previous steps, the mail file must be enabled for IMAP access. This is done by typing the following server command on the Domino console:

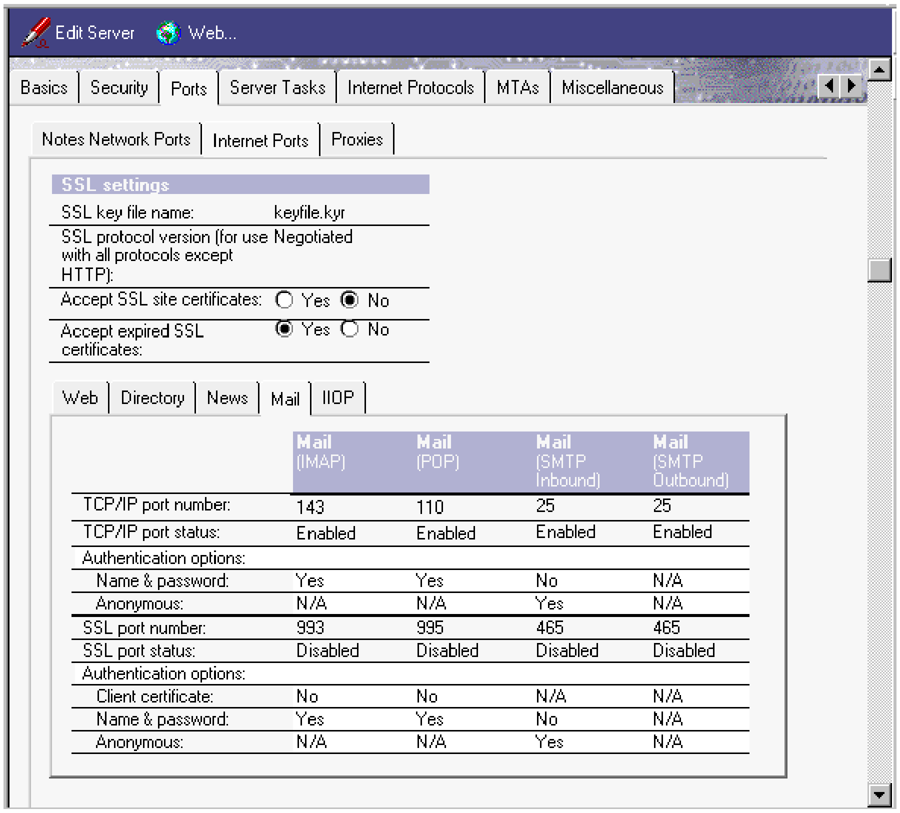
```
load convert -m mail\bbostail.nsf
```

Security setup

Internet mail clients must authenticate with the POP3 or IMAP server before they can access mail. Domino supports basic username and password authentication and Secure Sockets Layer (SSL) authentication as well as SSL encryption. The POP3 and IMAP default security configuration is the basic username and password authentication.

To modify the default POP3 or IMAP configuration (TCPIP port, security), from the Lotus Domino Administrator client, follow these steps:

1. Select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab. Then open the server document for the server that runs the POP3 or IMAP service.
4. Click the following tabs in order: **Ports->Internet Ports->Mail** tab. See Figure 401.



SSL settings

SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL certificates:	● Yes ○ No

	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
TCP/IP port number:	143	110	25	25
TCP/IP port status:	Enabled	Enabled	Enabled	Enabled
Authentication options:				
Name & password:	Yes	Yes	No	N/A
Anonymous:	N/A	N/A	Yes	N/A
SSL port number:	993	995	465	465
SSL port status:	Disabled	Disabled	Disabled	Disabled
Authentication options:				
Client certificate:	No	No	N/A	N/A
Name & password:	Yes	Yes	No	N/A
Anonymous:	N/A	N/A	Yes	N/A

Figure 401. Domino Server Configuration for Internet mail

15.1.4.4 Domino SMTP service configuration

Simple Message Transfer Protocol (SMTP) provides for message transfer with SMTP networks (Internet and intranets). A complete mail system installation for Internet mail clients (POP3 and IMAP) requires the Domino SMTP service and the Domino Mail Router task for sending and delivering messages to the Internet and to POP3 or IMAP client mail files on a Domino server.

The SMTP service configuration is different between Domino 4.6 and Domino 5.0. In Domino 4.6, the SMTP service is provided by a Message Transfer Agent (SMTP/MTA) separately from the Domino Mail Router. In Domino 5.0, the Domino Router implements a native SMTP protocol to transport Internet or intranet messages, along with Notes mail routing protocols for compatibility with previous releases. The SMTP MTA is no longer needed.

Lotus Domino Server Release 4.6

To run the Domino SMTP/MIME MTA task on your server, the *SMTP support* code must have been installed with the Domino server 4.6 code (this is the default installation). If this is not the case, you have to run the Domino server 4.6 code installation process again, and select it on the Manual Domino installation panel.

Once the SMTP support is installed on your Domino server, you must create or edit the following documents in the Public Address Book. If the Domino administrator selects the SMTP service during the setup of the Domino server, Domino automatically creates default documents and starts the SMTP service.

- Server document

  Routing tasks: Mail routing, SMTP Mail routing. In the Internet Message Transfer Agent (SMTP MTA) section:

  – Global domain name: GlobalDomain
  – Fully qualified Internet host name: MailServer.ibm.com

- The Global Domain document (Server-Domains view)

  – Domain type: Global Domain
  – Global domain name: GlobalDomain
  – Global domain role: SMTP MTA
  – Internet Domain Suffix: nstation.com
  – Notes domain(s) included: None

- The Foreign SMTP Domain document (Server-Domains view)

  – Domain type: Foreign SMTP Domain
  – Message Addressed to Internet Domain: *.*
  – Should be routed to Domain name: TheInternet

- The Server Connection document (Server-Connections view)

  – Connection type: SMTP
  – Source server: MailServer.ibm.com/NstationCert
  – Destination domain: TheInternet
  – Relay host: Your SMTP relay host if applicable

Figure 402 outlines the SMTP configuration with Domino server 4.6.

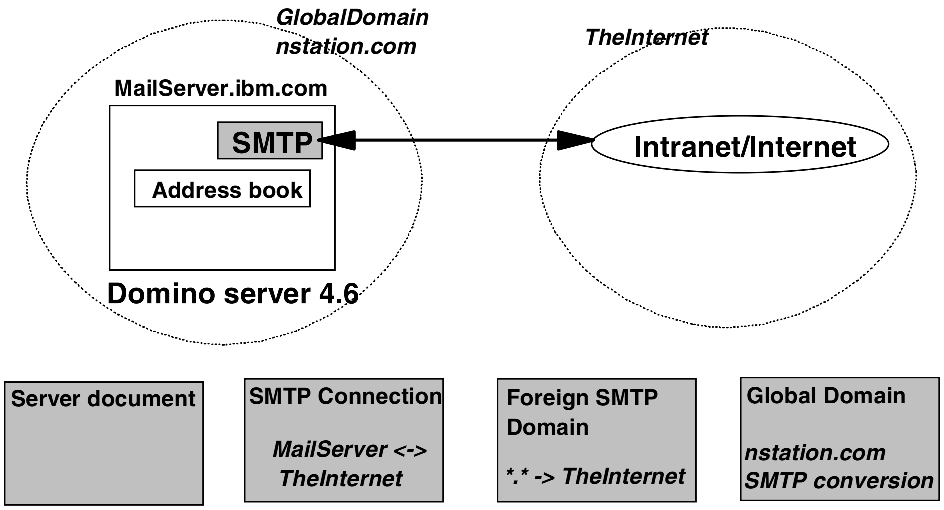


Figure 402. SMTP configuration overview with Domino 4.6

Make sure that the TCP/IP DNS server in your environment is set up to include all the Internet domain names that your company uses (for example, nstation.com).

To start the SMTP MTA server task while the Domino server is running, type the following server command on the Domino console:

```
load SMTPMTA
```

Lotus Domino Server Release 5.0

The SMTP support is native and, therefore, automatically installed with Lotus Domino server 5.0. Only two documents are involved in the SMTP configuration. If the Domino administrator selects the SMTP service during the setup of the Domino server, Domino automatically creates default entries for these documents and starts the SMTP service.

Figure 403 outlines the SMTP configuration with Domino server 5.0.

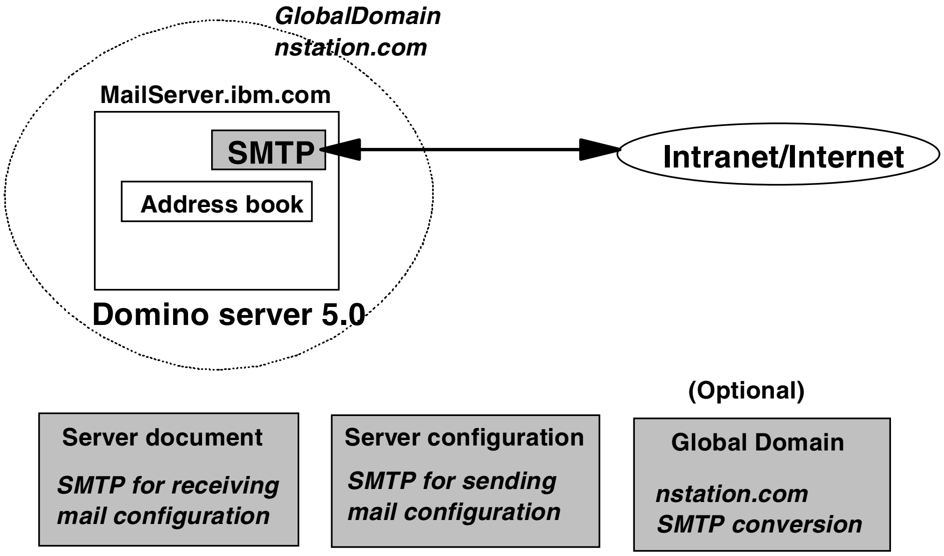
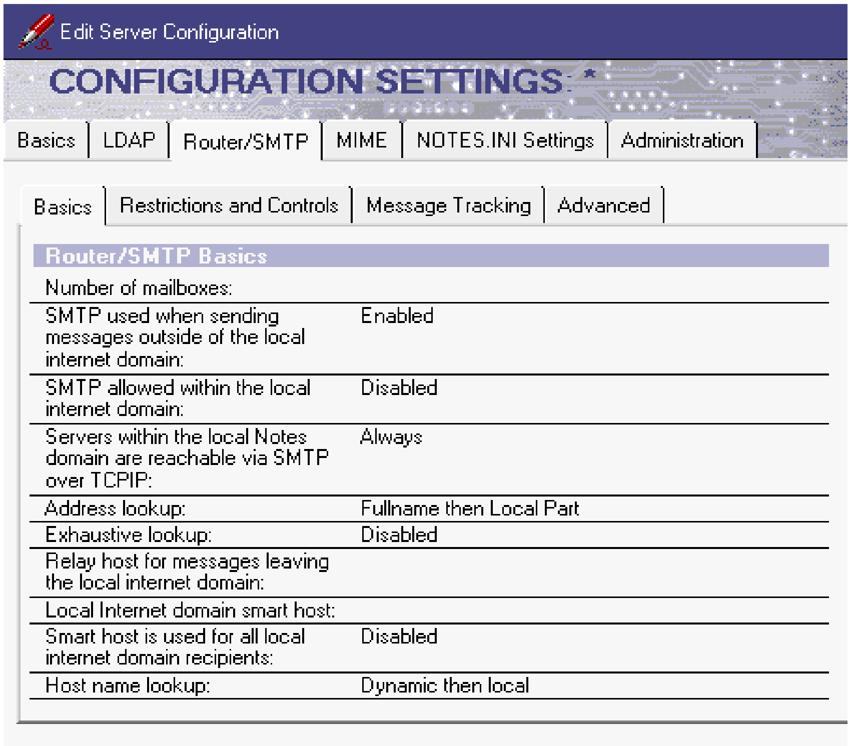


Figure 403. SMTP configuration overview with Domino 5.0

To configure *SMTP for sending mail* on the Router/SMTP-Basics tab of the Server Configuration document, follow this process:

1. From the Lotus Domino Administrator client, select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab. Then expand the **Messaging** section.
4. Choose **Configurations**.
5. Click **Add Configuration** to create a new Configuration Settings document or edit the existing one.
6. Click the **Router/SMTP** tab.
7. Complete the fields and save the document.

The Router/SMTP basic configuration is shown in Figure 404 on page 502.



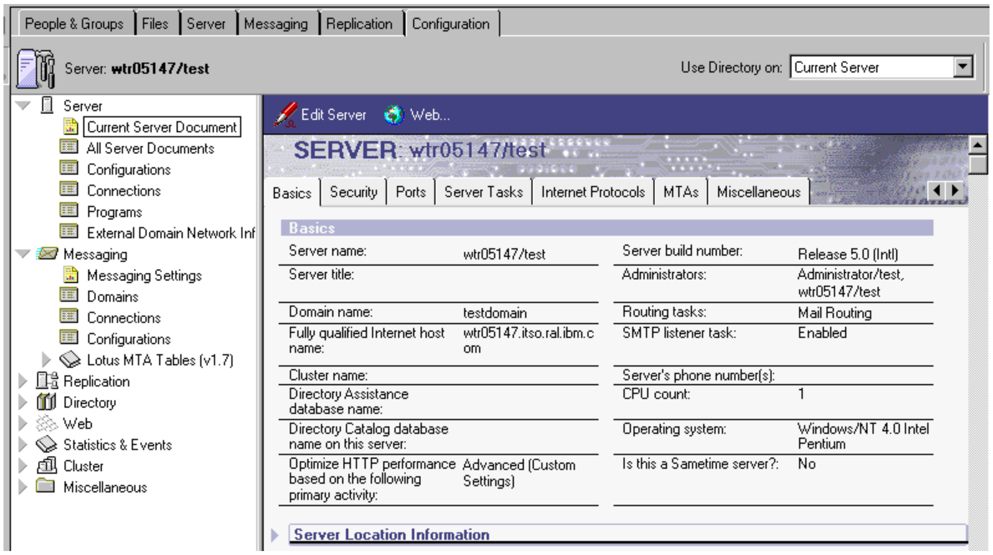
Router/SMTP Basics

Number of mailboxes:	
SMTP used when sending messages outside of the local internet domain:	Enabled
SMTP allowed within the local internet domain:	Disabled
Servers within the local Notes domain are reachable via SMTP over TCPIP:	Always
Address lookup:	Fullname then Local Part
Exhaustive lookup:	Disabled
Relay host for messages leaving the local internet domain:	
Local Internet domain smart host:	
Smart host is used for all local internet domain recipients:	Disabled
Host name lookup:	Dynamic then local

Figure 404. Router/SMTP: Basics configuration

Configure *SMTP for receiving mail* on the Basics tab of the Server document by performing these tasks:

1. From the Lotus Domino Administrator client, select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab. Then, expand the **Server** section.
4. Choose **Current Server** document.
5. Edit the server document for the server that runs the SMTP service.
6. Click the **Basics** tab.
7. Complete the Fully qualified Internet host name field, enable the SMTP listener task, and then save the document.



Server: **wtr05147/test**

Use Directory on: Current Server

SERVER: wtr05147/test

Basics

Server name:	wtr05147/test	Server build number:	Release 5.0 (Intl)
Server title:		Administrators:	Administrator/test, wtr05147/test
Domain name:	testdomain	Routing tasks:	Mail Routing
Fully qualified Internet host name:	wtr05147.itso.ral.ibm.com	SMTP listener task:	Enabled
Cluster name:		Server's phone number(s):	
Directory Assistance database name:		CPU count:	1
Directory Catalog database name on this server:		Operating system:	Windows/NT 4.0 Intel Pentium
Optimize HTTP performance based on the following primary activity:	Advanced (Custom Settings)	Is this a Sametime server?:	No

Figure 405. Server Configuration for SMTP

The domain of the Domino server’s host name (for example, itso.ral.ibm.com) may be different that your Internet domain (for example, nstation.com). In this case, you must create a Global Domain document to specify your primary and alternate Internet domains. The procedure to do this is as follows:

1. From the Lotus Domino Administrator client, select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab. Then, expand the **Messaging** section.
4. Select **Domains**, and then click **Add Domain**.
5. On the **Basics** tab, complete these fields:

   Domain type: Global Domain
   Global domain name: GlobalDomain
   Global domain role: R5 Internet Domain or R4.x SMTP MTA

6. Click the **Conversions** tab, complete these fields, and then save the local primary Internet domain document (for example, nstation.com).

   You can also change the way Domino converts a Notes address to an Internet address.

Make sure that the TCP/IP domain name services (DNS) server in your environment is set up to include all the Internet domain names that your company uses (for example, nstation.com).

To start the SMTP service while the Domino server is running, type the following server command on the Domino console:

```
load SMTP
```

15.1.4.5 Netscape Messenger configuration through NSM

To enable access to Netscape Messenger from any Network Station, the NSM administrator must ensure that Netscape Communicator is included in the launch bar of the Network Station desktop (this is the default).

Next, set up the Internet mail clients. You need the following information to configure a Network Station Internet mail client.

- The fully qualified domain name of the Domino SMTP server
- The fully qualified domain name of the Domino POP3 or IMAP server
- The Internet Mail type
- The Internet Mail client user name
- The user's name
- The e-mail address

For example, assume that you want to configure the Internet mail client for the user Bernard Bostaille. The data for this user is:

- The SMTP server: wtr055147.itso.ral.ibm.com
- The POP3 or IMAP server: wtr05147.itso.ral.ibm.com
- The Internet Mail type: POP3 or IMAP
- The POP3 or IMAP client user name: bbostaille or Bernard Bostaille
- The user's name: Bernard Bostaille
- The e-mail address: BernardBostaille@nstation.com

The SMTP server, the POP3 or IMAP server, the Internet Mail type, the user's name, and the e-mail address can be configured with Network Station Manager. The client can also configure settings using the Netscape preferences.

When using NSM, these elements can be configured at the system preferences level. The configuration tasks are fairly simple if we assume that only one of the Internet mail protocols is implemented for all users and that we can take advantage of the ${USER} variable to pass the user name from the Network Station login to the mail settings. To implement this, the name used by a user to log on a Network Station must be the same as their Internet mail client user name.

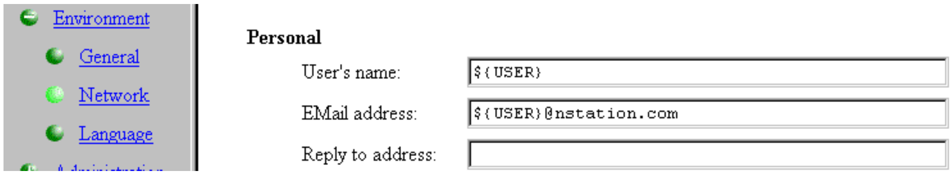
For example, we register the user "BernardBostaille" in the NSMUser group on the Network Station boot server. This user will log on the Network Station as "BernardBostaille". The login name will be passed to the Internet mail settings to build the mail user name "BernardBostaille" and the e-mail address "BernardBostaille@nstation.com".

Note

Windows NT lets you define a user with a space in the name, but the Network Station login will fail if the user name has a blank space, for example, Bernard Bostaille.

The procedure to configure the mail client from NSM is explained here:

1. Log on to the NSM using a user name that is part of the NSMAdmin group.
2. Select the **System** preferences level.
3. Select **Environment->Network**.
4. Scroll down to the Personal Settings section. Complete the two fields as illustrated in Figure 406.



Personal

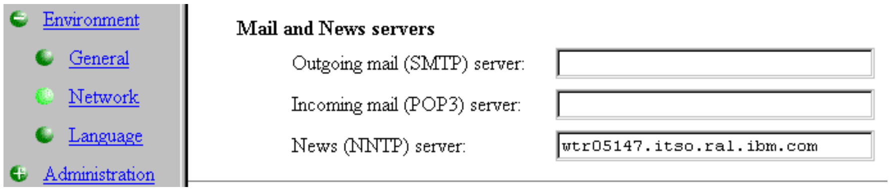
User's name: ${USER}

EMail address: ${USER}@nstation.com

Reply to address:

Figure 406. Configure mail client: Personal settings

5. Scroll down to the Mail and News server section. Complete the names of the SMTP and POP3 servers.



Mail and News servers

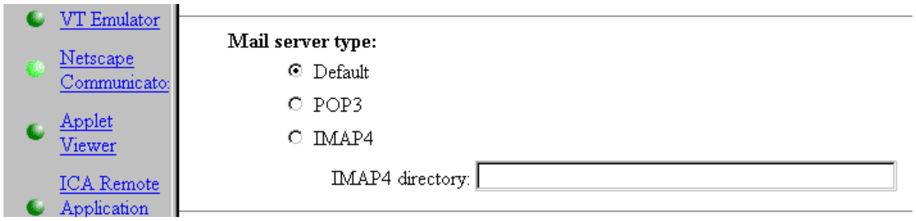
Outgoing mail (SMTP) server:

Incoming mail (POP3) server:

News (NNTP) server: wtr05147.itso.ral.ibm.com

Figure 407. Configure mail client: Mail and News server

6. Select **Applications->Netscape Communicator**. Scroll down to the Mail server type, and select one of the protocols. The IMAP Mail directory should be left blank in case you choose IMAP. The default is POP3.



Mail server type:

● Default

○ POP3

○ IMAP4

IMAP4 directory:

Figure 408. Configure mail client: Mail server type

15.1.4.6 Netscape Messenger advanced configuration

An administrator can only manage the main configuration parameters of the Internet Mail client using NSM. These parameters can be set at the system, group, or user level. Parameters that are not available through NSM can be changed by creating a Netscape override file, called overrides.js. This file is invoked when all users start Netscape. For more information about how to modify Netscape Communicator preferences, see 12.8, “Advanced customization using JavaScript” on page 360.

The first column in Table 74 on page 506 lists the Netscape Messenger preferences that an administrator may want to manage centrally. The second column indicates the corresponding parameters in overrides.js, and the third column describes of the parameters.

Table 74. Some Netscape Messenger preferences and configuration parameters

Settings	Parameters	Description
General Mail		
Check for mail every...minutes	mail.check_new_mail	Enables or disables automatic mail server checking for new messages. When enabled, checking occurs at the interval specified in mail.check_time.
	mail.check_time	Specifies the interval, in minutes, for checking the mail server when mail.check_new_mail is true. The default is 10. The range is upward from 1.
POP3 Mail		
Leave messages on server after retrieval	mail.leave_on_server	Controls whether messages are left on a POP3 mail server after downloading. This preference applies only if mail.server_type is set to 0 (POP3). The default is false, which moves mail to the local machine. Set to true to leave messages on the server after downloading.
When deleting a message locally, remove it from the server	mail.delete_mail_left_on_server	Not documented Default = false
Automatically download any new messages	mail.pop3_gets_new_mail	Not documented Default = true
IMAP Mail		
When I delete a message - Move it to the trash folder (1) - Mark it as deleted (0) - Remove it immediately (2)	mail.imap.server.<ImapServerHostname.domain>.delete_model	Not documented Default = 0
Clean up (Expunge) Inbox on Exit	mail.imap.server.<ImapServerHostname.domain>.cleanup_inbox_on_exit	not documented Default = True
Local Mail Disk Space		
Do not store messages locally that are larger than ...KB	mail.limit_message_size	Enables or disables a limit on the size of mail messages downloaded from POP3 mail servers. Messages larger than the specified size aren't downloaded. The default is false, which disables a limit. Set to true to impose a message size limit specified by mail.max_size.
	mail.max_size	Specifies the limit on the size of mail messages downloaded from POP3 mail servers, if mail.limit_message_size is true. The units are kilobytes. The default is 50. The range is from 1, upward.
Automatically compact folders when it will save over ... KB	mail.prompt_purge_threshhold	Enables or disables automatic message folder compacting, using the value specified in mail.purge_threshhold as the limit to allow for unused space. The default is false, which disables automatic compacting. Set to true to enable automatic compacting.

Settings	Parameters	Description
	mail.purge_threshhold	Specifies a limit on the unused space to allow in message folders before automatically compacting those folders, if mail.prompt_purge_threshhold is true. The units are in kilobytes. The default is 100. The range is from 1, upward.

The code gives an example of the Netscape Messenger preferences configuration in the Netscape overrides.js override file. See 12.8, “Advanced customization using JavaScript” on page 360, for the syntax. The parameters in the file will:

- Enable and lock “Check for mail every 20 minutes”
- Disable and lock “Leave messages on the server after retrieval”
- Disable and lock “When deleting a message locally, remove it from the server”
- Enable and lock “Automatic download any new messages”
- Enable and lock “When I delete a message, Mark it as deleted”
- Enable and lock “Clean up (Expunge) Inbox on Exit”
- Enable and lock “Do not store messages locally that are larger than 100 KB”
- Enable and lock “Automatically compact folders when it will save over 200 KB”

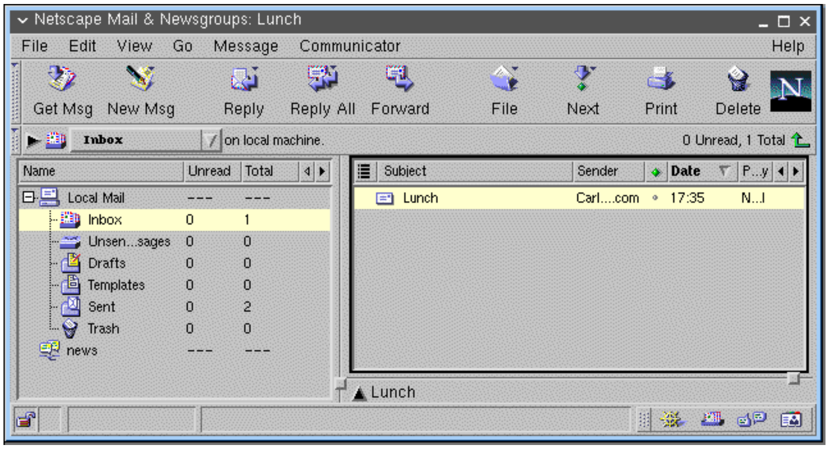
```
//General Mail preferences
lockPref("mail.check_new_mail",true);
lockPref("mail.check_time",20);

//POP3 Mail
lockPref("mail.leave_on_server",false);
lockPref("mail.delete_mail_left_on_server",false);
lockPref("mail.pop3_gets_new_mail.false",true);

//IMAP Mail
lockPref("mail.imap.server.MailServer.ibm.com.delete_model",0);
lockPref("mail.imap.server.MailServer.ibm.com.cleanup_inbox_on_exit",true);

//Local Mail Disk Space
lockPref("mail.limit_message_size",true);
lockPref("mail.max_size",100);
lockPref("mail.prompt_purge_threshhold",true);
lockPref("mail.purge_threshhold",200);
```

15.1.4.7 Notes POP3 or IMAP mail access from the Network Station

To access Netscape Messenger, follow these steps:

1. Click the **Netscape Communicator** icon to launch the program.
2. Select **Communicator** from the menu, and click **Messenger**.

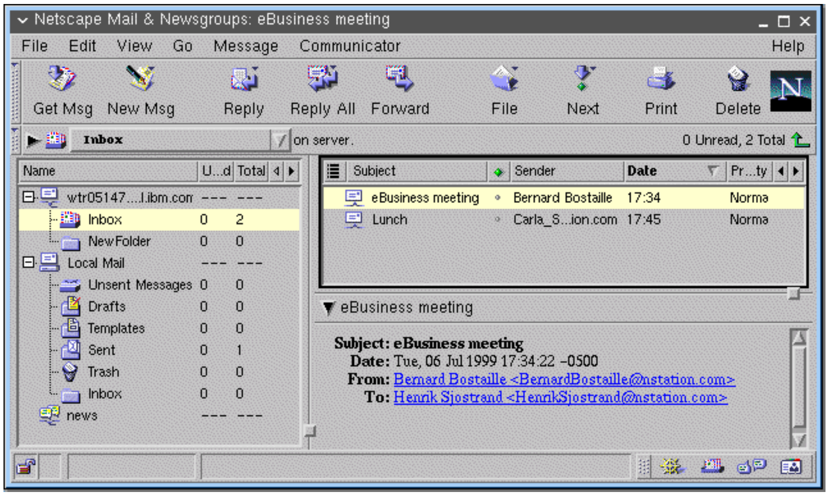
The POP3 and IMAP mail clients are shown in Figure 409 and Figure 410 on page 508.



Name	Unread	Total
Local Mail	---	---
Inbox	0	1
Unsen...sages	0	0
Drafts	0	0
Templates	0	0
Sent	0	2
Trash	0	0
news	---	---

Subject	Sender	Date	P...y
Lunch	Carl....com	17:35	N...l

Figure 409. Network Station POP3 mail client



Name	U...d	Total
wtr05147....l.ibm.com	---	---
Inbox	0	2
NewFolder	0	0
Local Mail	---	---
Unsent Messages	0	0
Drafts	0	0
Templates	0	0
Sent	0	1
Trash	0	0
Inbox	0	0
news	---	---

Subject	Sender	Date	Pr...ty
eBusiness meeting	Bernard Bostaille	17:34	Norma
Lunch	Carla_S...ion.com	17:45	Norma

Subject: eBusiness meeting
Date: Tue, 06 Jul 1999 17:34:22 -0500
From: Bernard Bostaille <BernardBostaille@nstation.com>
To: Henrik Sjostrand <HenrikSjostrand@nstation.com>

Figure 410. Network Station IMAP mail client

You can see that the IMAP client offers both a local copy of the mail and a server copy.

15.1.4.8 User Netscape mail configuration

The individual user can update several mail configuration parameters through the use of Network Station Manager by selecting the Network (under Environment) setup task. The settings that a non-administrator level user can change include their own user name, e-mail address, reply-to address, and home page. However, the user can view their mail configuration parameters from within Netscape as follows:

1. Open Netscape Communicator from the launch bar.
2. Click **Edit->Preferences->Mail & Newsgroups**.

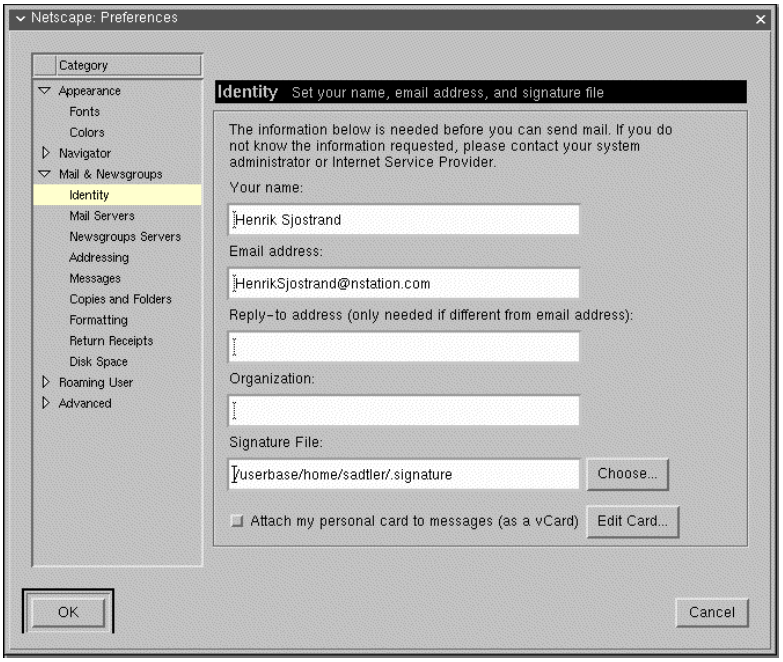
Note

Netscape e-mail and other preferences that are non-selectable or grayed-out are settings which are changed through Network Station Manager.

The following panels show the mail configuration from the Netscape user's point of view.

Edit->Preferences->Mail & Newsgroups->Identity

Figure 411 shows the existing settings for the user name and e-mail address. These settings were derived from changes made through the Network Station Manager. In this example, Henrik entered his own name and e-mail address since he didn't want his e-mail address to be based on his user ID. This was due to the fact that an administrator had used a system-wide $USER variable to set user e-mail addresses. This is explained in 12.3.2.1, "Configuring mail and proxy settings" on page 342.



Identity Set your name, email address, and signature file

The information below is needed before you can send mail. If you do not know the information requested, please contact your system administrator or Internet Service Provider.

Your name: Henrik Sjostrand

Email address: HenrikSjostrand@nstation.com

Reply-to address (only needed if different from email address):

Organization:

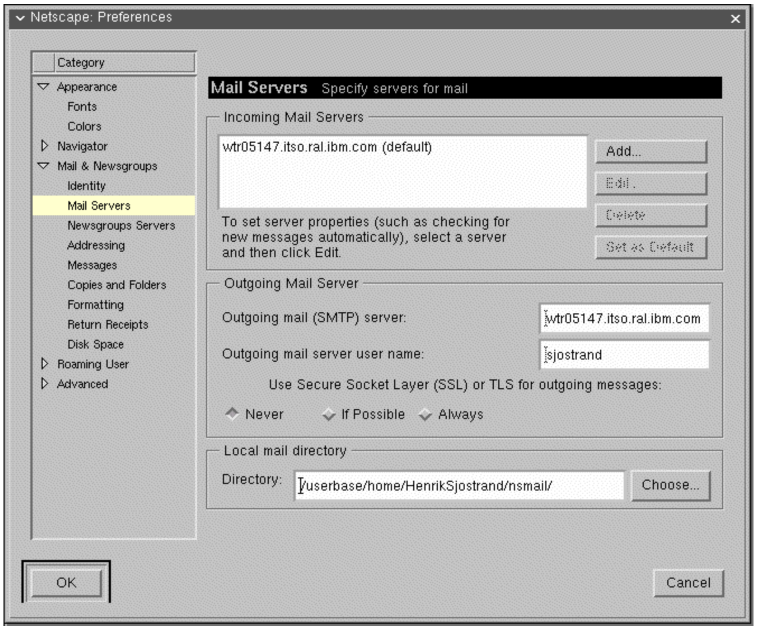
Signature File: /userbase/home/sadtler/.signature

□ Attach my personal card to messages (as a vCard)

Figure 411. Identity for IMAP example

Edit->Preferences->Mail & Newsgroups->Mail Servers

The user can change certain settings (Figure 412 on page 510) but several must be changed through Network Station Manager. For example, the outgoing and incoming mail server names must be set by an administrator using Network Station Manager. The following screen captures show the settings for incoming and outgoing mail server, and local directory information.



Mail Servers Specify servers for mail

Incoming Mail Servers

wtr05147.itso.ral.ibm.com (default)

To set server properties (such as checking for new messages automatically), select a server and then click Edit.

Outgoing Mail Server

Outgoing mail (SMTP) server: wtr05147.itso.ral.ibm.com

Outgoing mail server user name: sjostrand

Use Secure Socket Layer (SSL) or TLS for outgoing messages:

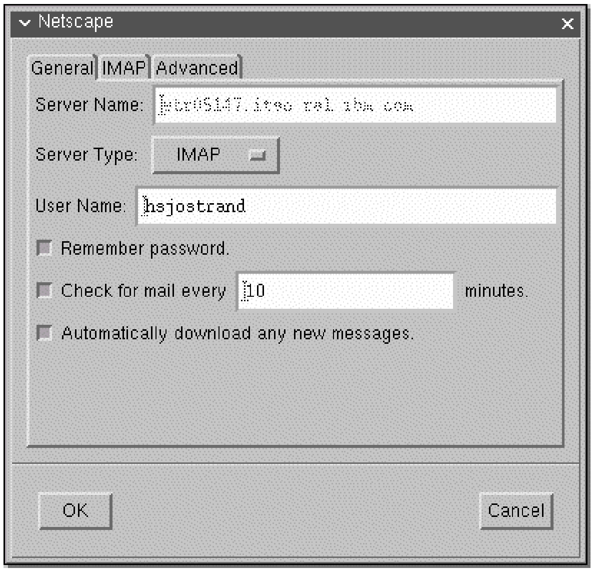
● Never ○ If Possible ○ Always

Local mail directory

Directory: /userbase/home/HenrikSjostrand/nsmail/

Figure 412. Mail Server definitions for IMAP example

Click the incoming mail server name (wtr05147.itso.ral.ibm.com) in the Incoming Mail Servers field. Then click **Edit**.



Server Name: wtr05147.itso.ral.ibm.com

Server Type: IMAP

User Name: hsjostrand

□ Remember password.

□ Check for mail every 10 minutes.

□ Automatically download any new messages.

Figure 413. Incoming mail server configuration

Now, you can change the type of mail (Server Type field), change the frequency to check for new mail, and so on.

15.1.4.9 Local mail files location on the file server

The local mail files of Network Station Internet mail clients are located by default on the user home directories of the boot server drive:\NetworkStationV2\userbase\home\UserID\.

A directory called (by default) *nsmail* is created on the POP3 and IMAP user home directories. This directory contains the different folders of the local mail.

An additional directory called (by default) ns_imap is created for the IMAP users. This directory contains the folder settings of the IMAP server mail file. Since multiple IMAP servers can be configured, the ns_imap directory contains one sub-directory per IMAP server.

The directory structure for a POP3 and a IMAP mail user are respectively shown in Figure 414 and Figure 415.

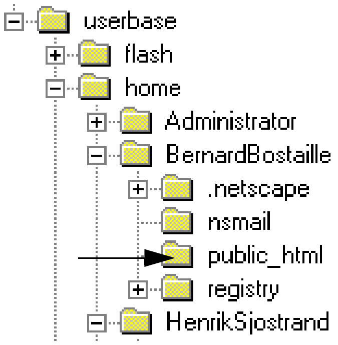


Figure 414. Default POP3 mail directory in the user home directory on the NSM server

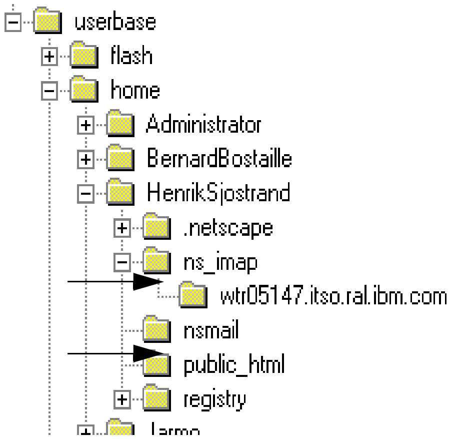
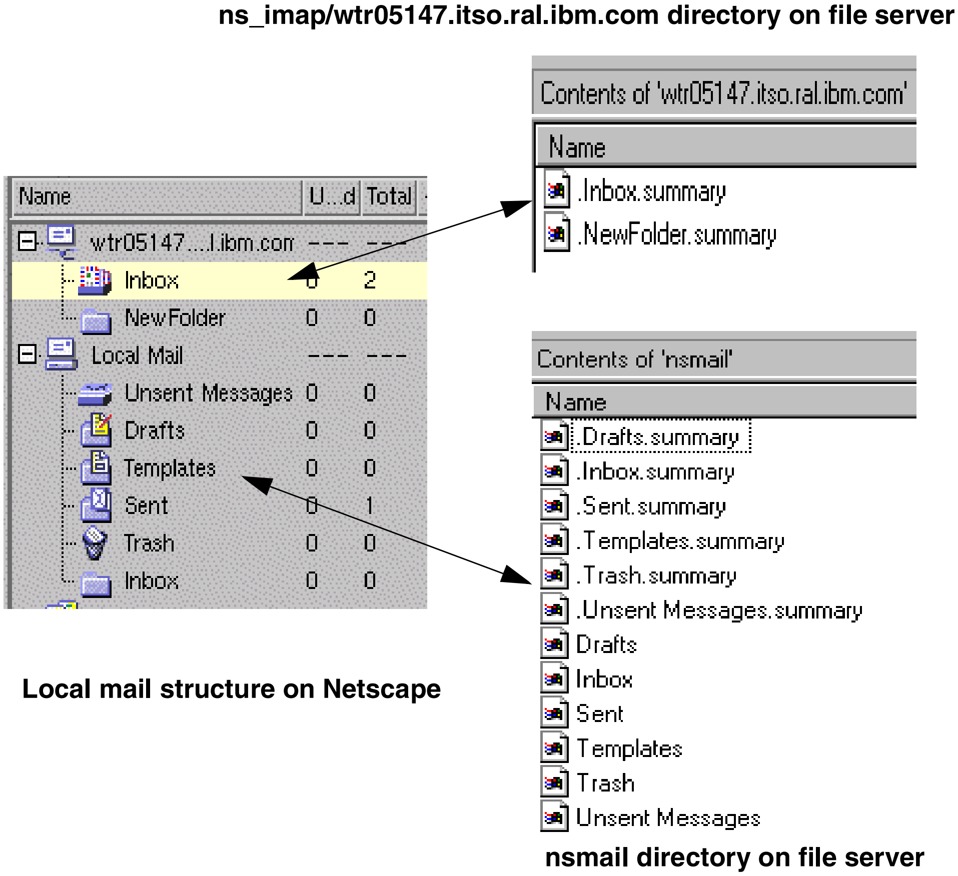


Figure 415. Default IMAP mail directories in the user home directory on the NSM server

Figure 416 on page 512 compares the IMAP mail structure as it appears on Netscape Messenger and the corresponding directory structures on a user home directory.


ns_imap/wtr05147.itso.ral.ibm.com directory on file server
Local mail structure on Netscape
nsmail directory on file server

Name	U...d	Total
wtr05147....l.ibm.com	---	---
Inbox	0	2
NewFolder	0	0
Local Mail	---	---
Unsent Messages	0	0
Drafts	0	0
Templates	0	0
Sent	0	1
Trash	0	0
Inbox	0	0

Contents of 'wtr05147.itso.ral.ibm.com'

Name
.Inbox.summary
.NewFolder.summary

Contents of 'nsmail'

Name
.Drafts.summary
.Inbox.summary
.Sent.summary
.Templates.summary
.Trash.summary
.Unsent Messages.summary
Drafts
Inbox
Sent
Templates
Trash
Unsent Messages

Figure 416. Local mail directory structure

15.1.5 Using the LDAP client

Internet mail clients can use the *Netscape Address Book* from a Network Station to search for recipients addresses in the Domino Address Book.

Figure 417 and the following list show the elements of such a configuration:

- A Domino server running the LDAP service
- A Network Station with Netscape Address Book
- A file server

The file server is, by default, the Network Station boot server where the user home directories reside.

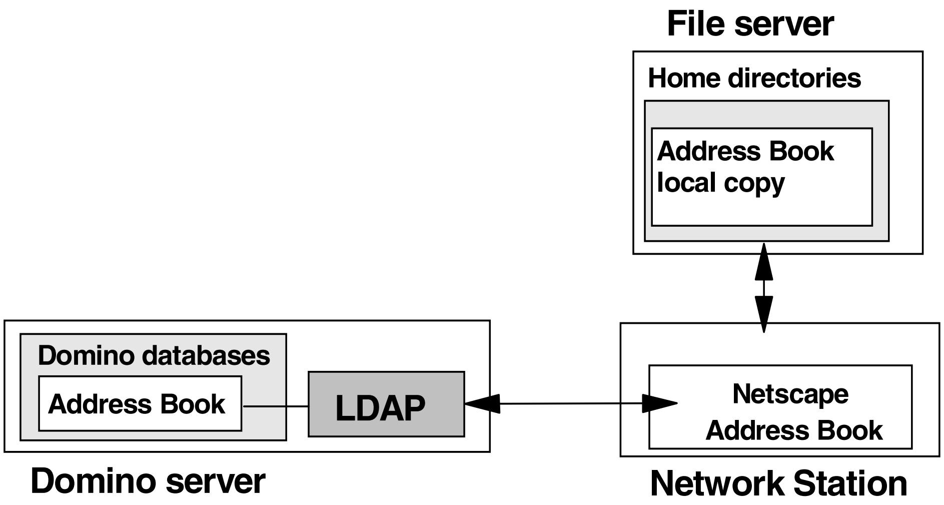


Figure 417. Domino LDAP service

15.1.5.1 LDAP protocol

Lightweight Directory Access Protocol (LDAP) uses TCP/IP to allow clients to access directory information. LDAP defines a standard way to search for and manage entries in a directory (for example, a Domino Address book), where an entry is one or more groups of attributes (for example, mail addresses, phone numbers) that are associated with a distinguished name (for example, the user name). A distinguished name is a name that uniquely identifies an entry within the directory tree. A directory can contain many types of entries, such as entries for users, groups, devices, and application data.

15.1.5.2 Domino LDAP service configuration

Let’s look at what is involved in setting up LDAP for users in order to add the Domino address book for their use.

LDAP service startup

To start the Domino LDAP task while the Domino server is running, type the following server command on the Domino console:

```
load LDAP
```

Internet address formation

First, we need to understand how the Domino server implements the LDAP service. To return an Internet e-mail address for a user registered in the Domino Directory to an LDAP client, the LDAP service searches for:

- A fully-formed Internet address, listed in one of the fields of the Person document (for example, Internet Address BernardBostaille@nstation.com)
- Rules specified in the “Internet address lookup” field in the SMTP Address Conversion section of a Global Domain document.

  If your organization uses more than one Global Domain document, you must select “Yes” in the Use as default Global Domain field of the Global Domain document you want to use. To create or edit a global domain document, follow these steps:

  a. From the Lotus Domino Administrator client, select **File->Open server**.

b. Select a server to administer.

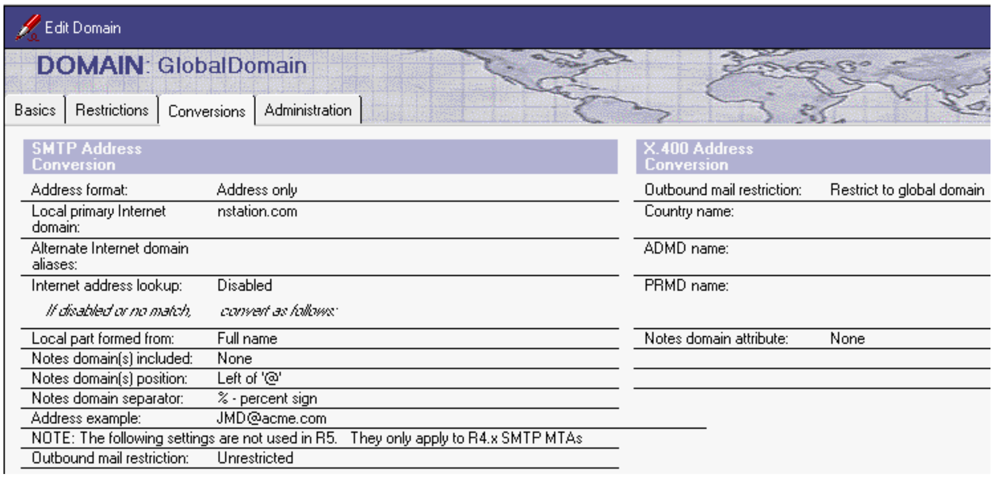
c. Click the **Configuration** tab. Then, expand the **Messaging** section.

d. Select **Domains**. Then, select one of the domains, or click **Add Domain**.

e. On the **Basics** tab, select “Yes” in the Use as default Global Domain field

f. On the **Conversions** tab (Figure 418), disable the Internet address lookup and specify the Internet address lookup rules. The Internet address lookup tells Domino to look in the Person documents for an Internet address. By disabling it, you are saying you have chosen not to enter Internet addresses for each user. Our addresses follow a general standard that we define here.

g. Save the document.



SMTP Address Conversion

Address format: Address only
Local primary Internet domain: nstation.com
Alternate Internet domain aliases:
Internet address lookup: Disabled
If disabled or no match, convert as follows:
Local part formed from: Full name
Notes domain(s) included: None
Notes domain(s) position: Left of '@'
Notes domain separator: % - percent sign
Address example: JMD@acme.com
NOTE: The following settings are not used in R5. They only apply to R4.x SMTP MTAs
Outbound mail restriction: Unrestricted

X.400 Address Conversion

Outbound mail restriction: Restrict to global domain
Country name:
ADMD name:
PRMD name:
Notes domain attribute: None

Figure 418. Global Domain Conversions tab

- A DNS domain name retrieved from the operating system of the Domino server machine

Configuring the fields that anonymous LDAP users can access

To specify the fields that anonymous LDAP users can access, perform the following steps:

1. From the Lotus Domino Administrator client, select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab, and expand the **Server** section. Click **Configurations** under Server.
4. If there is a Configuration Settings document for all servers in the domain, complete the following tasks:

   a. Expand **Directory**, and select **Directory Settings**.
   b. Click **Edit Directory Settings**.

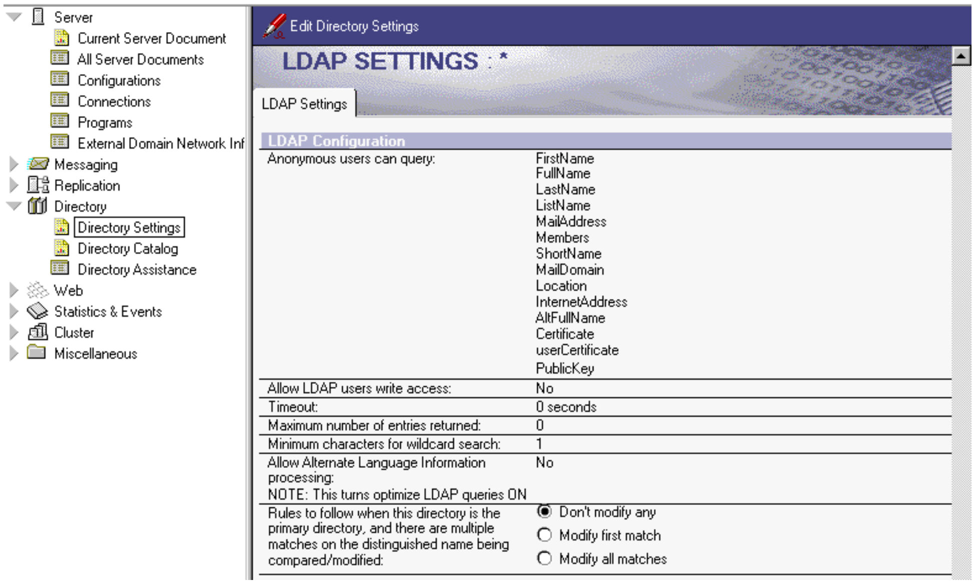
5. If there is not a Configuration Settings document for all servers in the domain, complete the following steps:

   a. Expand **Server**, and select **Configurations**.

   b. Click **Add Configuration** or **Edit a Configuration document**. Select **Yes** next to “Use these settings as the default settings for all servers”.

c. Click the **LDAP** tab.

6. Click the box after “Choose fields that anonymous users can query via LDAP”. Specify the fields that anonymous users can query, and click **OK**.
7. Click **Save->Close**.
8. Stop and restart each Domino server that runs the LDAP service.



LDAP Configuration

Anonymous users can query:	FirstName FullName LastName ListName MailAddress Members ShortName MailDomain Location InternetAddress AltFullName Certificate userCertificate PublicKey
Allow LDAP users write access:	No
Timeout:	0 seconds
Maximum number of entries returned:	0
Minimum characters for wildcard search:	1
Allow Alternate Language Information processing: NOTE: This turns optimize LDAP queries ON	No
Rules to follow when this directory is the primary directory, and there are multiple matches on the distinguished name being compared/modified:	● Don't modify any ○ Modify first match ○ Modify all matches

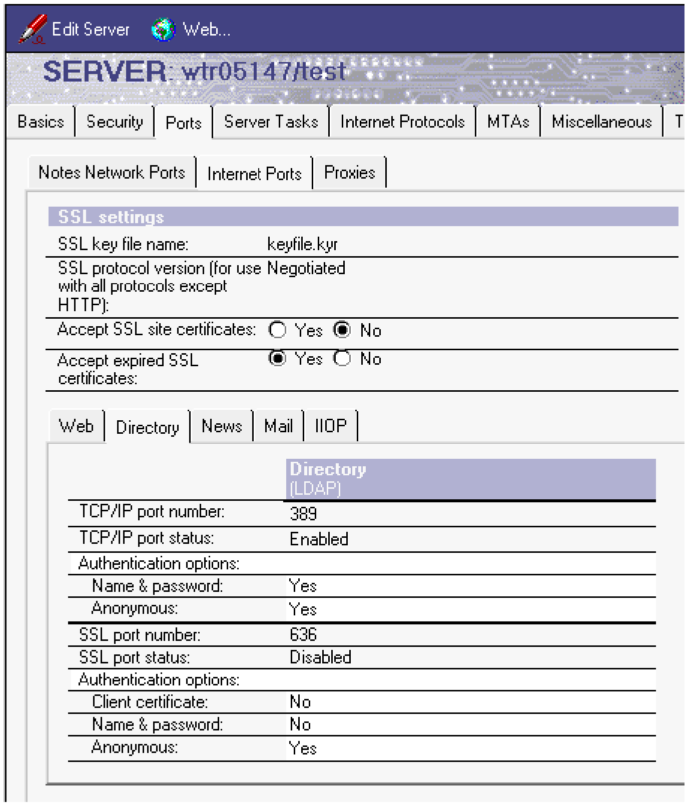
Figure 419. LDAP Settings

Security setup

By default, LDAP clients can connect to the LDAP service on a Domino server anonymously or by using name and password authentication over TCP/IP port 389. Domino supports also Secure Sockets Layer (SSL) authentication as well as SSL encryption.

To modify the default LDAP configuration (TCPIP port and security), from the Lotus Domino Administrator client, complete these steps:

1. Select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab. Then, open the server document for the server that runs the LDAP service.
4. Click the following tabs in order: **Ports->Internet Ports->Directory**.


Edit Server
Web...
SERVER: wtr05147/test
Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | T
Notes Network Ports | Internet Ports | Proxies
Web | Directory | News | Mail | IIOP

SSL settings

SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL certificates:	● Yes ○ No

	Directory (LDAP)
TCP/IP port number:	389
TCP/IP port status:	Enabled
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	636
SSL port status:	Disabled
Authentication options:	
Client certificate:	No
Name & password:	No
Anonymous:	Yes

Figure 420. Server LDAP settings

15.1.5.3 Netscape Address Book configuration through NSM

To enable access to Netscape Address Book from any Network Station, the NSM administrator must ensure that Netscape Communicator is included in the launch bar of the Network Station desktop (this is the default). Network Station Manager does not provide configuration parameters for the LDAP client.

15.1.5.4 Netscape Address Book Advanced configuration

The Domino address book can be defined as the main address book for all Network Station users by creating a Netscape override file, overrides.js. For more information about how to modify Netscape Communicator preferences, see 12.8, “Advanced customization using JavaScript” on page 360.

The first column of Table 75 lists Netscape Address Book preferences that an administrator may want to manage centrally. The second column indicates the corresponding parameters in overrides.js, and the third column gives a description of the parameters.

Table 75. Some Netscape Address Book preferences and configuration parameters

Settings	Parameters	Description
Directory description	ldap_2.servers.<name>.description	Contains the name of the directory service as users should see it in the Address Book. Replace <name> with the name of a particular directory service. The general default is an empty string.
Directory position in the directories list	ldap_2.servers.<name>.position	Not documented Position in the Directory List (Personal Address Book = 1)
LDAP server	ldap_2.servers.<name>.serverName	Contains the DN name of an LDAP directory service, for example, directory.netscape.com. This preference isn't defined for non-LDAP resources. The default value is an empty string.
PinPoint Addressing -> Look for addresses in the following -> Directory server	ldap_2.autoComplete.useDirectory	Uses the entries in the LDAP directory when using the autocomplete addressing feature. The default is true.
PinPoint Addressing -> Directory server used for autocomplete addressing	ldap_2.servers.<name>.autoComplete.enabled	Specifies the LDAP directory used for autocomplete addressing. The default is false, which is disabled. To enable this feature, specify the directory server and set this preference to true.

The following file gives an example of the Netscape Address Book and PinPoint Addressing preferences configuration in the overrides.js file. The parameters in the file will:

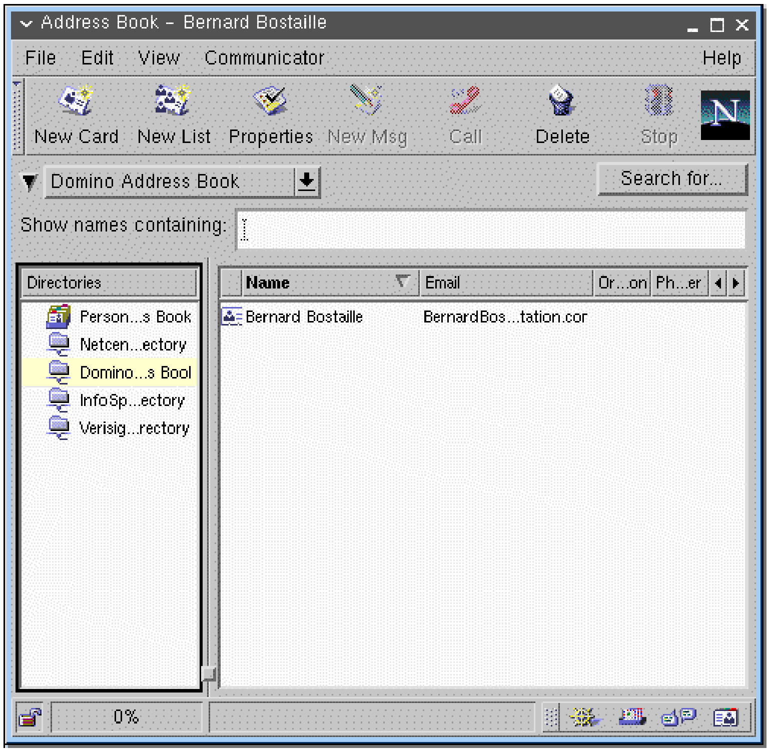
- Add Domino Address Book to the address book list in position 3 and point it to the Domino server wtr05147.itso.ral.ibm.com.
- Enable the PinPoint Addressing using “Domino Address Book” to look for addresses.

```
lockPref("ldap_2.servers.DominoAddressBook.description", "Domino Address
Book");
lockPref("ldap_2.servers.DominoAddressBook.position", 3);
lockPref("ldap_2.servers.DominoAddressBook.serverName",
"wtr05147.itso.ral.ibm.com");
lockPref("ldap_2.servers.DominoAddressBook.useDirectory", true);
lockPref("ldap_2.servers.DominoAddressBook.description", "Domino Address
Book");
```

15.1.5.5 Domino Address Book access from the Network Station

To access Netscape Address Book (Figure 421 on page 518), complete these steps:

1. Click the **Netscape Communicator** icon to launch the program.
2. Choose **Communicator** from the menu, and click **Address Book**.



Name	Email	Or...on	Ph...er
Bernard Bostaille	BernardBos...tation.cor		

Figure 421. Netscape Address Book

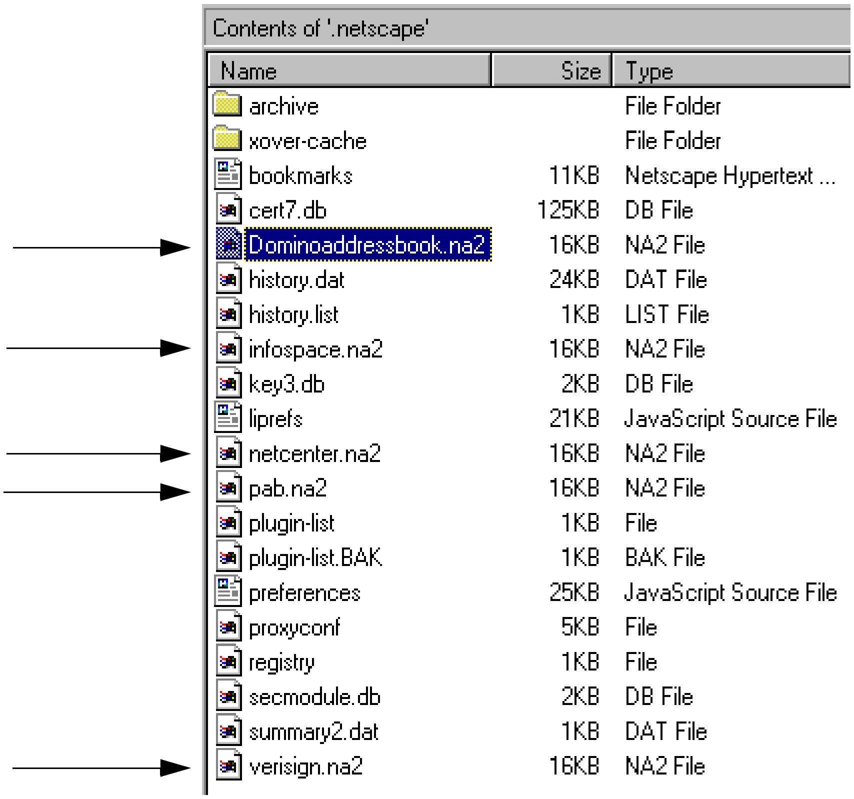
If you modify the overrides.js file as shown in the previous section, Domino Address Book will appear at the third position in the directory list after the Personal Address Book.

With the PinPoint Addressing configuration, Netscape Messenger will “autocomplete” addresses using names from the Domino Address Book.

15.1.5.6 Local Address Book copy location on the file server

A local copy of each defined address book is created, with the extension .na2, in the user home directory on the file server drive:\NetworkStationV2\userbase\home\username\.netscape.

The copies do not contain the entire address book, but only names you searched for in Netscape Address Book. The directory structure for an LDAP client is shown in Figure 422.



Contents of '.netscape'

Name	Size	Type
archive		File Folder
xover-cache		File Folder
bookmarks	11KB	Netscape Hypertext ...
cert7.db	125KB	DB File
Dominoaddressbook.na2	16KB	NA2 File
history.dat	24KB	DAT File
history.list	1KB	LIST File
infospace.na2	16KB	NA2 File
key3.db	2KB	DB File
liprefs	21KB	JavaScript Source File
netcenter.na2	16KB	NA2 File
pab.na2	16KB	NA2 File
plugin-list	1KB	File
plugin-list.BAK	1KB	BAK File
preferences	25KB	JavaScript Source File
proxyconf	5KB	File
registry	1KB	File
secmodule.db	2KB	DB File
summary2.dat	1KB	DAT File
verisign.na2	16KB	NA2 File

Figure 422. Local Address Books copy on the file server

15.1.6 NNTP News client

News clients can use *Netscape Messenger* from a Network Station to access USENET newsgroup or private newsgroups on a Domino server.

Figure 423 on page 520 and the following list show the elements of such a configuration:

- A Domino server running the Network News Transfer Protocol (NNTP) service
- A Network Station with Netscape Messenger
- A file server

The file server is, by default, the Network Station boot server where the user home directories reside.

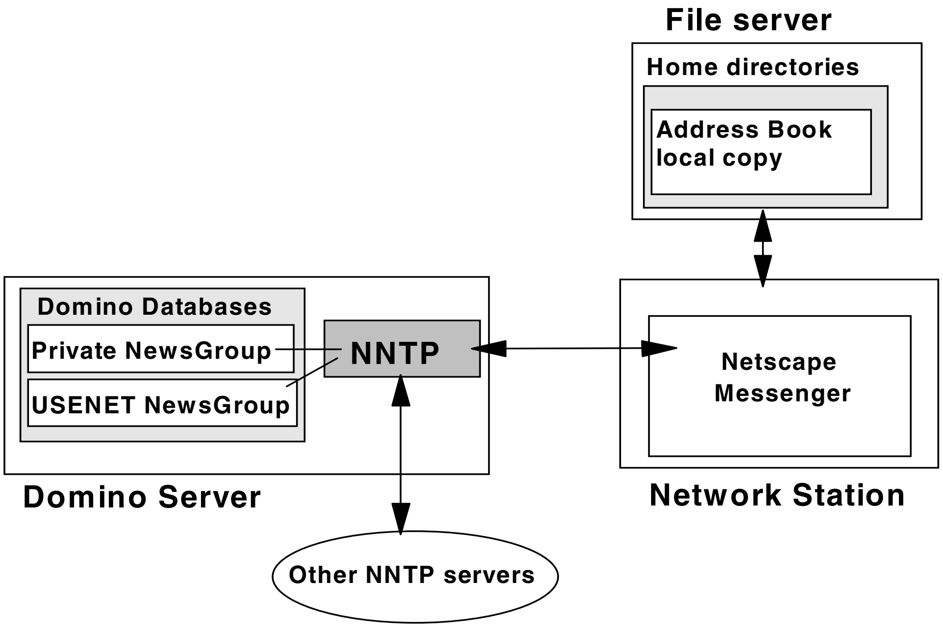


Figure 423. Domino NNTP service

15.1.6.1 NNTP protocol

Network News Transfer Protocol (NNTP) is a protocol that uses TCP/IP to connect to USENET newsgroups. USENET is a distributed bulletin board system that specializes in online group discussions on a variety of topics. The set of topics and responses related to a particular subject is called a *newsgroup*. A newsgroup contains postings or articles. A posting that you send to a newsgroup or that you receive from one is called an *article*. Any article that is posted to a newsgroup is carried to all subscribers of that newsgroup.

Newsfeeds are the periodic transfer of newly posted newsgroup articles from one server to another.

15.1.6.2 Domino NNTP service configuration

You can install the Network News Transfer Protocol (NNTP) service on a Domino server. This enables you to send and receive news articles from USENET newsgroups as well as create, moderate, and manage private newsgroups.

Using a Domino server with the NNTP service enables users to obtain newsfeeds from the Domino server and to read news articles in a Notes database. Administrators can use Domino security such as access control lists (ACLs) to control access to newsgroups.

The following sections only explain how to create and configure a private newsgroup on the Domino server.

NNTP service startup

To start the NNTP server task while the Domino server is running, type the following server command on the Domino console:

```
load NNTP
```

Private NewsGroup creation

Before you create a newsgroup, you set up the Database Profile document. In this document, you specify whether a newsgroup is public, private, or private/moderated. You also specify access rights for private newsgroups.

You must save the Database Profile document before you perform the steps to create the newsgroup. Saving the Database Profile document allows the newsgroup to appear to NNTP clients, Notes clients (Release 4.6 and later), and Web browsers.

The following steps takes you through this process, including creating the database profile. We create a private newsgroup called *PrivateNews* as follows:

1. From the Domino Administrator, choose **File->Database->New**.
2. Complete the fields shown in Table 76.

Table 76. Fields for creating new private newsgroup

Field	Enter
Server	The name of the server that will store the newsgroup, for example wtr05147/test.
Title	The newsgroup name. For a private newsgroup, do not begin the name with a USENET hierarchy name (comp, misc, news, rec, sci, soc, talk, humanities, and alt), for example, PrivateNews.
File Name	The name of the database file that will store the newsgroup. The extension .NSF is appended by default, for example, PrivNews.nsf.
Folder	The directory of the newsgroup database. The default is the data directory.
Template	NNTP Discussion 5.0 from the server template list.

3. Click **OK**. The Database Discussion document appears.
4. Click **Click here to open database**.
5. Click **Edit Database Profile**.
6. In the Database Profile document, complete the fields shown in Table 77. Then, save the document.

Table 77. Fields for Database Profile document

Field	Enter
Database Profile editors	Names of users who are allowed to modify the Database Profile. The default is the name of the newsgroup creator. Users whose names you enter are assigned Manager access in the database, for example, Administrator.
Private	Choose **Private** to create a private newsgroup.
List of users who can access the database	Enter the names of users who can access your database. These users will be given Author access, for example, Bernard Bostaille.

Field	Enter
Moderated	Choose **Moderated** to if you want a moderated, private newsgroup. Then, complete these fields: - Name of moderator: Name of the user who posts and removes news articles. This user is assigned Editor access in the database ACL. - E-mail address of Moderator: E-mail address to use to send articles and requests to the newsgroup moderator. If you leave the field blank, Domino creates a private, unmoderated newsgroup.

7. (Optional) To list the database in the database catalog, complete the following tasks:
   a. Open the **Database Properties** box.
   b. Click the **Design** tab, and then choose **List in Database Catalog**.

Note: When you add a new newsgroup database, you need to stop and start the NNTP service on the Domino server to make it available.

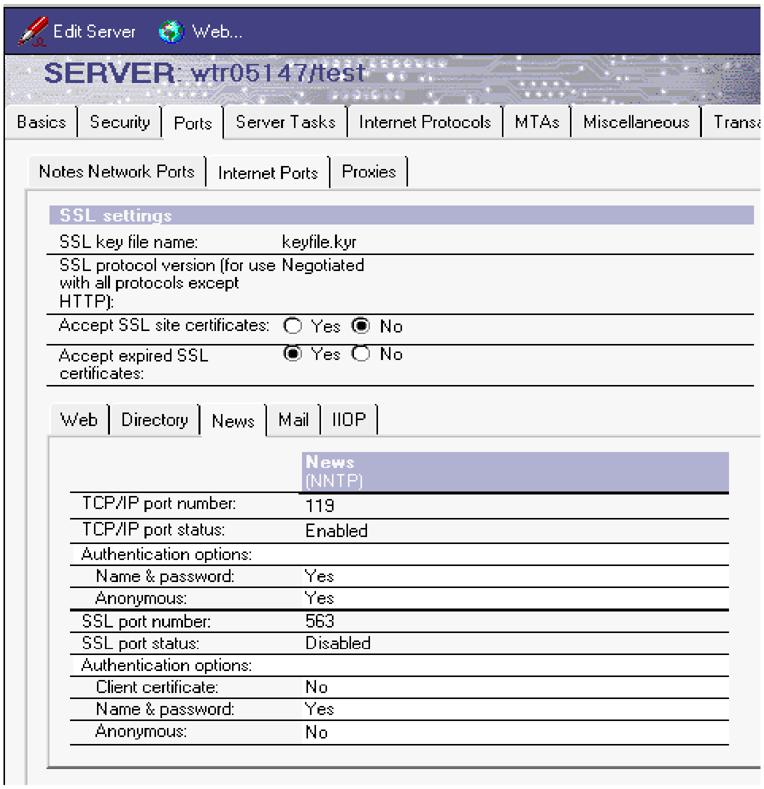
Security setup

By default, NNTP clients can connect to the NNTP service on a Domino server anonymously or by using name and password authentication over TCP/IP port 119. Domino also supports Secure Sockets Layer (SSL) authentication as well as SSL encryption.

The security settings apply to newsreader clients and remote servers with NNTP that connect to the Domino server with the NNTP service, to pull newsgroup articles from or push articles to it.

To modify the default NNTP configuration (TCPIP port, Security), from the Lotus Domino Administrator client, follow these steps:

1. Select **File->Open server**.
2. Select a server to administer.
3. Click the **Configuration** tab. Then, open the server document for the server that runs NNTP service.
4. Click the following tabs in order: **Ports->Internet Ports->News** (Figure 424).



SSL settings

SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	○ Yes ● No
Accept expired SSL certificates:	● Yes ○ No

	News (NNTP)
TCP/IP port number:	119
TCP/IP port status:	Enabled
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	563
SSL port status:	Disabled
Authentication options:	
Client certificate:	No
Name & password:	Yes
Anonymous:	No

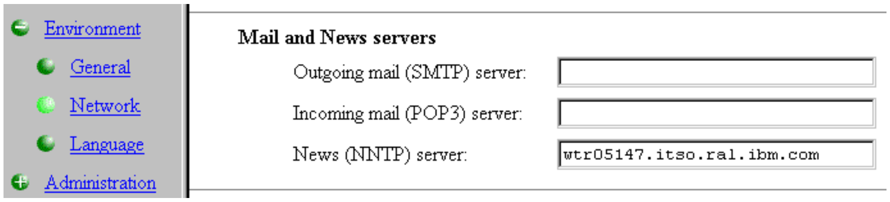
Figure 424. NNTP configuration

15.1.6.3 Network Station NNTP configuration through NSM

To enable access to Netscape Messenger from any Network Station, the NSM administrator must ensure that Netscape Communicator is included in the launch bar of the Network Station desktop (this is the default).

To define a NNTP user for Network Station users, complete these steps:

1. Log on to the NSM using a user name that is part of the NSMAdmin group.
2. Select the **System** preferences level.
3. Select **Environment->Network**.
4. Scroll down to the Mail and News server section. Complete the News server field as illustrated in Figure 425.



Mail and News servers

Outgoing mail (SMTP) server:	
Incoming mail (POP3) server:	
News (NNTP) server:	wtr05147.itso.ral.ibm.com

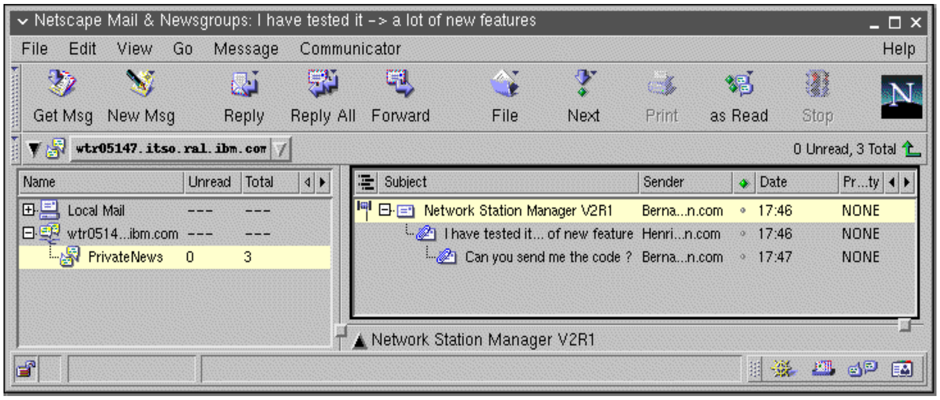
Figure 425. Identify the name of the News server

15.1.6.4 Domino Newsgroup access from the Network Station

To access the private newsgroup we created on the Domino server, complete these steps:

1. Click the **Netscape Communicator** icon to launch the program.
2. Choose **Communicator** from the menu, and click **Messenger**.
3. Select the News server **wtr05147.itso.ral.ibm.com.ibm.com** that we defined in NSM.
4. Select **File->Subscribe**.
5. Enter a user name and password.
6. Select **PrivateNews**, and click **Subscribe**.

The PrivateNews newsgroup now appears in the wtr05147.itso.ral.ibm.com News server section. Figure 426 shows the Network Station News client.


Netscape Mail & Newsgroups: I have tested it -> a lot of new features
File
Edit
View
Go
Message
Communicator
Help
Get Msg
New Msg
Reply
Reply All
Forward
File
Next
Print
as Read
Stop
wtr05147.itso.ral.ibm.com
0 Unread, 3 Total

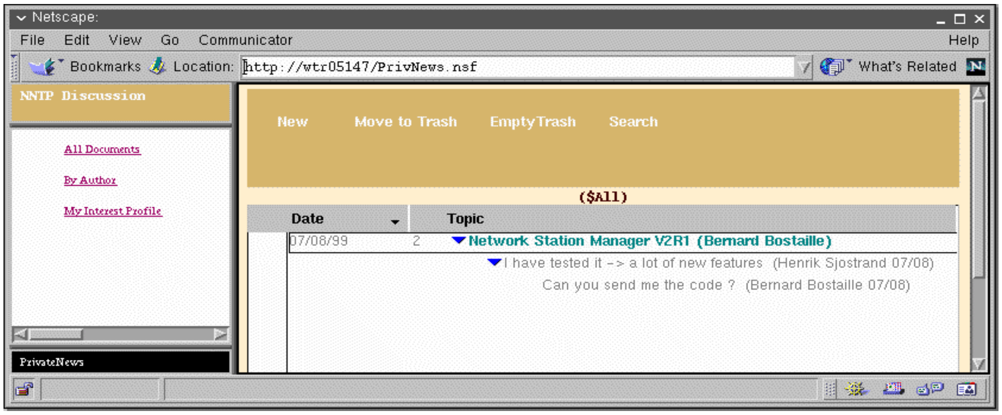
Name	Unread	Total
Local Mail	---	---
wtr0514...ibm.com	---	---
PrivateNews	0	3

Subject	Sender	Date	Pr...ty
Network Station Manager V2R1	Berna...n.com	17:46	NONE
I have tested it... of new feature	Henri...n.com	17:46	NONE
Can you send me the code ?	Berna...n.com	17:47	NONE

Network Station Manager V2R1

Figure 426. Network Station news client

The newsgroup that we created on the Domino server is a Notes database. Therefore, the PrivateNews database can also be accessed from the Netscape Navigator. More functions are available to news users when a Domino newsgroup is accessed as a Notes database from the browser. Figure 427 shows the News database accessed from Netscape Navigator.



Location: http://wtr05147/PrivNews.nsf

Date		Topic
07/08/99	2	Network Station Manager V2R1 (Bernard Bostaille)
		I have tested it -> a lot of new features (Henrik Sjostrand 07/08)
		Can you send me the code ? (Bernard Bostaille 07/08)

Figure 427. Newsgroup access from Netscape Navigator

15.1.7 Domino services automatic startup

To start the HTTP, POP3, IMAP, SMTP, LDAP, and NNTP services automatically when you start the Domino server, edit the ServerTasks setting in the NOTES.INI file to include the corresponding commands.

If the Domino administrator selects these services during the setup of the Domino server, Domino adds them, by default, to the NOTES.INI.

15.1.8 Additional information

If you need additional information about the installation and configuration of a Domino server, refer to:

- The online help Notes database entitled “Domino administration help”.

  This database is automatically installed on the Domino server and the Domino Administration client.
- *Lotus Domino for AS/400 R5: Implementation*, SG24-5592
- *Lotus Domino R5 for IBM RS/6000*, SG24-5138

Chapter 16. Kiosk mode

In most Network Station installations, customers want to take advantage of the Network Station's ability to run multiple applications at the same time. They also want to be able to allow different users to access different applications based on their work responsibilities. In other environments, however, it is sometimes desired to configure the Network Stations to run only one application or to let all Network Stations run the same set of applications. To allow easy configuration of this, NSM V2R1 offers two modes of operation: *kiosk mode* and *suppressed login mode*.

Neither of these modes require that an end user manually log on to a Network Station when it's powered on. The login is either done automatically without the end-user knowing about it, or it is not done at all.

The suppressed login mode was actually introduced in NSM V1R3, but was then often referred to as kiosk mode. Now that NSM V2R1 treats these two modes differently, it is important to distinguish them.

Information on both kiosk mode and suppressed login mode can also be found in the *IBM Network Station Manager Advanced Information* publication that can be downloaded from the Network Station site at:
`http://www.pc.ibm.com/us/networkstation/tech_library.html`

16.1 Kiosk mode versus suppressed login

These two modes work somewhat differently. It's important to understand what the differences are to select the mode that best suits a particular environment. Remember, neither mode requires an end user to manually log on.

16.1.1 User login

In kiosk mode, the Network Station runs without any user logged on.

In suppressed login mode, a pre-defined user account is used by the Network Station to perform an automatic logon, without user intervention. Many Network Stations can share the same user ID, or each Network Station can be assigned an individual user ID to perform its logon. Both methods have their advantages and disadvantages.

16.1.2 User updates

Most applications running locally in the Network Station use the user's home directory to store user-specific data such as Netscape browser bookmarks and cookie files, emulator preferences, and so on. In kiosk mode, there is no user logged on. Because of this, a Network Station running in kiosk mode creates a temporary user home directory in a so called *In-memory File System* (IFS).

Note: This *In-memory File System* (IFS) for a Network Station running in kiosk mode should not be confused with the AS/400 System's Integrated File System (IFS).

The IFS is similar to a RAM disk or virtual disk with which some PC users may be familiar with. It creates a virtual hard disk in RAM. Access to it is done just as if it was a real hard disk. However, since the accesses go directly to RAM as opposed to a hard disk, the performance is several magnitudes higher. The IFS is automatically created and mounted whenever the Network Station is configured to run in kiosk mode. Any information that is written to the IFS is lost when the Network Station is rebooted.

Since IFS is mounted in RAM, a Network Station configured for running in kiosk mode may require more RAM than if configured for running in suppressed login mode (or normal login mode).

In suppressed login mode, the predefined user ID used for automatically logging on is used for storing the home directory (just as with any Network Station user logging on). This means that if a user makes any changes (for example, updates to the bookmarks file) those changes will remain persistent and can be retrieved the next time the Network Station is powered on. If this is the case, each Network Station should be assigned its own individual user ID so the changes one user makes do not affect all other Network Station users.

Note

In both modes of operation, it is actually best to deny the user the ability to save preferences. It may fool them into believing that they will be retrieved the next time the user powers on their Network Station (kiosk mode) or it may cause other users to be given these settings.

Consider, for example, the suppressed login mode where several Network Stations share the same user ID. One user changes the color mapping in the 3270 emulator and saves those preferences. Another user powers on their Network Station, which automatically logs on with the same user ID as the first user's Network Station. In this situation, the user receives the color mapping just created by the first user.

16.1.3 Window appearance

The way the applications look on the screen is also slightly different between the two modes.

In kiosk mode the first application launched runs in so called *chrome less mode*. This simply means it does not have any window borders surrounding it, so it covers the whole screen (full-screen). If the first application is able to launch new applications running locally in the Network Station (for example, the browser has this capability), then these applications will run with surrounding borders. If an application does not have a border, the user is not able to move the window on the screen or to minimize it, so the first application launched in kiosk mode always stays fixed, in full-screen. Also, in kiosk mode, the user does not have access to the Network Station's Launch Bar for starting new applications.

In suppressed login mode, however, the look of the Network Station's desktop is the same as when a user performs a manual login (suppressed login just automates this task using predefined user IDs). All applications run in their own window. The windows have borders surrounding them, and the user can move and minimize them. The users have access to the launch bar and can start new applications from it.

16.1.4 Auto restart

If an application running in kiosk mode is terminated, the application is automatically restarted. For example, if the ICA client is used and the user logs off from the Metaframe server, the ICA client is terminated but will be automatically restarted.

In suppressed login mode, it is not automatically restarted. Some applications have the ability to restart themselves if so configured using command line options when invoking them.

16.1.5 Auto start

In kiosk mode, the applications you defined to run are automatically started.

In suppressed login mode, you have the option of automatically starting one or more applications by putting them in the Startup folder in NSM or just allowing the user to start them manually from the launch bar.

16.1.6 NSM configuration

If using suppressed login mode, NSM can be used to configure settings at all levels (System, group, user, and workstation).

If using kiosk mode, no user logs onto NSM. NSM can, therefore, only be used to make settings at the System level and workstation-specific level. Also, those NSM settings that are stored in the allusers.nsm file (some System-level settings are) cannot be used from NSM, since the allusers.nsm file is read after a user logs on. This file is never read in kiosk mode. If you make changes like these, you should save them in the allkiosk.nsm file or <nc-id>.nsm files.

16.1.7 Summary

Table 78 gives a summary of the differences between the kiosk mode and the suppressed login mode in NSM V2R1.

Table 78. Comparison of modes

	Kiosk mode	Suppressed login
User is authenticated	No	Yes, predefined user IDs
Access to server file system	read-only	read-write
NSM configuration levels	System, NC-specific	System, group, user, NC-specific
Window borders	No for the initial application, but subsequent applications will have borders.	Yes
NC desktop, Launch Bar presence	No, the initial application is the base desktop, and it runs in full-screen.	Yes
Number of applications	One only, but if that application has the capability, it may launch other applications or open multiple other windows.	One or more

	Kiosk mode	Suppressed login
Application launching	Auto-started Auto-restarted (automatic)	Configurable

The choice between when to use kiosk mode and suppressed login mode depends on what you want to accomplish, which applications you need to access, what the environment looks like, and what types of users there are (employees or just visitors) for example.

Consider the following points to help you decide which mode you want.

The *kiosk mode* is well suited for:

- Setting up the Network Station as a Windows-based terminal, when all users should only have access to one or more Metaframe servers.
- Using the Network Station as a public browser kiosk, for example in banks for providing Internet banking services.
- When replacing 3270/5250/VT emulators with Network Stations and you only want to provide the users with roughly the same features as they had before.
- When you want to use the Netscape browser as the desktop, so it is used for access to all resources on your network. From the Netscape browser, you can create a home page for each individual user or department that contains icons for the applications they need to access.
- When you have any particular application, for example, a Java application used in a retail environment or airline ticket sales, and the users only work with this single application.

The *suppressed login mode* is well suited for:

- When you have several users that all should have exactly the same set of (multiple) applications, the same application preferences (that is, colors, keyboard remaps and so on), and you want to simplify the environment for the user by removing the additional Network Station login step. The users can then just power on their Network Stations and get the desktop and any applications with which they have been provided.
- When you want some Network Stations to require an end user to logon and some to not require them to log on, and when those that should not require it are given a wide range of IP addresses (like 9.24.104.100 to 9.24.104.199), for example, using DHCP.
- When you need to retain certain preferences or settings between different sessions. In suppressed login mode, the applications can read these from the user’s home directory (that is, the user ID used for automatically logging on). If an application only allows setting these preferences from itself and not from NSM or using an external configuration file (RealPlayer, for example), the application can be started once for the user ID and configured. Then, these settings will be read on the next startup. This is usually most suitable when using a shared user ID.

16.2 Kiosk mode

V2R1 of the Network Station Manager provides for the single application kiosk setup. There are a variety of sample files provided in the $ServBase/defaults directory. These files, with the suffix .ksk, are copied to the appropriate configuration directory and modified to reflect the proper parameters for the environment. While this is not automated, it is straightforward as demonstrated in 16.2.1, "Step-by-step instructions for a single application kiosk setup" on page 531.

Alternatively, many customers want to be able to launch several applications, possibly including the desktop, without requiring any login. While this could be done with suppressed login mode (see 16.3, "Suppressed login mode" on page 539), there is typically no configuration server in these environments or no need to authenticate since there are no user preferences or home directory requirements. The boot itself may be from Compact Flash with no separate configuration/authentication server. Section 16.2.2, "Step-by-step instructions for multiple application kiosk setup" on page 535, leads you through the steps.

16.2.1 Step-by-step instructions for a single application kiosk setup

When setting up kiosk mode, you use a number of pre-defined application templates shipped with NSM V2R1. These are configured for establishing each individual Network Station application in kiosk mode. You copy the template most suitable for your needs and then customize it for your specific environment. This may require you to specify an IP address for a host system to access or the name of a Java application you want to use and so forth.

The templates (shown in Table 79) are located in the $ServBase/defaults directory on the NSM server.

Table 79. NSM V2R1 kiosk templates

Application	Template file name
ICA client	ica.ksk
ICA Remote Application Manager	icaram.ksk
Netscape Communicator	netscape.ksk
3270 emulator	ns3270.ksk
5250 emulator	ns5250.ksk
VT emulator	nsterm.ksk
Java application	java.ksk
Java appletviewer	appletviewer.ksk
xterm (command) window	unix.ksk

All kiosk templates are, just as the other download profiles, written in XML.

We now guide you through the steps necessary to setup an application for kiosk mode. We use the 5250 emulator as an example. Most of these tasks must be done manually, since the management of the kiosk files are not yet integrated into

NSM. The configuration of the application itself (such as keyboard remapping enabled or disabled) is the same as for non-kiosk usage, and you do it from NSM.

The following section describes how to set up kiosk mode for a few specific Network Stations and also how to do it for *all* your Network Stations booting from this NSM server.

16.2.1.1 Selecting which Network Stations should use the kiosk mode

The first step is to decide which Network Stations should use the kiosk mode and whether you should address them using their IP address, TCP/IP host name, or MAC address. If you set up kiosk mode for all Network Stations, it's not necessary to address each of them specifically. You don't need to find out their IP address, host name, or MAC address.

To determine the IP address for a Network Station, you can press the ESC key during its boot process and then select **Configure network settings** from the NS Boot Main Menu that is displayed. If you are using DHCP, you will not be able to see an IP address because the Network Station has not been assigned one at this time. If you use DHCP, you should consider using either the host name or, perhaps even better, the MAC address to address the Network Stations.

To determine the Network Station's MAC address, select **Display hardware information** from the NS Boot Main Menu.

If you use the host name as the identifier, you need to retrieve the host name from your DNS server.

Tip

If your Network Station is powered on (or you can power it on) and displays the desktop, you can press Ctrl+Alt+I simultaneously to display information about this Network Station. In the dialog that pops up, you see the Network Station's IP address, its host name (if one is found), and its MAC address.

The IP address, host name, or MAC address you retrieved will be used in the <nc-id> field as mentioned in the following description.

A note on the <nc-id> format

- If the IP address is used, the format should be a dotted decimal TCP/IP address, for example 9.24.104.192.
- If the host name is used, it should be the host name that the Network Station receives when it performs a reverse name lookup to get its host name from its IP address. If the DNS (or hosts file) returns a fully qualified host name (like hondo1.itso.ral.ibm.com), this should be used. If the DNS (or hosts file) returns only the host name part and not the domain name part (like hondo1), this should be used. Use nslookup *ipaddress* to see what your DNS returns.
- If the MAC address is used, it should be a full 12-character MAC address without colons and with single-digit fields padded with a leading zero. For example, if a Network Station has a MAC address of 0:6:29:F5:D7:3, the valid MAC address would be 000629F5D703.

Our experience tells us it is usually most convenient to address the Network Stations using their IP addresses. Then we don't need to keep track of their MAC addresses, which is inconvenient in large environments. Also, even though the host name may seem like the most convenient way to address the Network Station, this may require adding a Dynamic Domain Name Server (DDNS) if you are using DHCP. Then you need to map each MAC address to a host name, meaning you will have to keep track of the MAC addresses anyway. In the following examples, we use the IP addresses.

16.2.1.2 Editing the kiosk template file

The next task is to copy and edit the kiosk template to suit your needs.

Step 1

Locate the kiosk template file for the application you want. In our example, we used the ns5250.ksk file. Copy this template to the $UserBase/profiles/ncs directory. This is the directory where the Network Stations look for their NC-specific download profiles.

The 5250 emulation template (ns5250.ksk) is shown in Figure 428 on page 534.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCREGISTRY SYSTEM "ncregistry.dtd" >
<!-- 5250 Emulator Sample Profile for Single Application (kiosk) Mode -->
<NCREGISTRY>
<OBJECT NAME="/config">
<CATEGORY NAME="WORKSTATION">
<PROPERTY NAME="pref-screen-background-color">black</PROPERTY>
</CATEGORY>
</OBJECT>
<OBJECT NAME="/desktop/preferences">
<CATEGORY NAME="DESKTOP">
<PROPERTY NAME="desktop_command">nsm_wrapper ns5250 -geometry 9999x9999+0+0</PROPERTY> B
</CATEGORY>
</OBJECT>
<OBJECT NAME="/login/session">
<CATEGORY NAME="KIOSK">
<PROPERTY NAME="commands" TYPE="LIST" ACTION="APPEND">
<ELEMENT>
<FIELD NAME="op">SET</FIELD> A
<FIELD NAME="arg1">NSM_KIOSK_MODE</FIELD>
<FIELD NAME="arg2">ON</FIELD>
</ELEMENT>
</PROPERTY>
</CATEGORY>
</OBJECT>
</NCREGISTRY>
```

Figure 428. Kiosk template file for 5250 emulator

Look at the three lines in Figure 428 marked with A.

```
<FIELD NAME="op">SET</FIELD>
<FIELD NAME="arg1">NSM_KIOSK_MODE</FIELD>
<FIELD NAME="arg2">ON</FIELD>
```

These three lines are present in all kiosk templates. They tell the application that it should run in kiosk mode. When this download profile is read during the Network Station's boot process, the value NSM_KIOSK_MODE is set to ON in the NC Registry.

Step 2

Modify the file to suit your environment. The most likely modification for the emulator templates is the addition of the host name or IP address so the emulator connects automatically. The line with the B marker in Figure 428 is the line to modify. Modifying this line to connect the 5250 session to host 9.9.99.999 would look like this:

```
<PROPERTY NAME="desktop_command">nsm_wrapper ns5250 9.9.99.999 -geometry
9999x9999+0+0</PROPERTY>
```

The second parameter sent to the 5250 emulator is `-geometry 9999x9999+0+0`.

Geometry specifies that the emulator is to start with a window size of 9999x9999 pixels starting at position (0,0) which is the upper-left corner of the screen. Since the emulator cannot fit a window as large as 9999x9999 pixels onto the screen, it takes the closest possible value it can fit, which is the resolution of your display. Therefore, the emulator will run in full-screen mode.

Different applications have different configurable options. You may add any options that are supported by the specific application you are configuring.

Step 3

Rename the file to <nc-id>.nsm, where *<nc-id>* is the MAC address, IP address, or TCP/IP host name of the Network Station, for example:

```
9.24.104.192.nsm
9.24.104.193.nsm
9.24.104.194.nsm
000629F5D703.nsm
00063244730B.nsm
hondo4.itso.ral.ibm.com.nsm
hondo5.itso.ral.ibm.com.nsm
```

If you are using DHCP and using IP addresses for the names, this would require you to create one kiosk file for each possible IP address the Network Stations can pick up. In this case, you may want to consider using the MAC addresses to address the Network Stations, give them a static IP addresses, or even consider running all Network Stations in kiosk mode.

If you want to configure *all* your Network Stations booting from this NSM server for kiosk mode you can take a shortcut. Instead of copying the modified template file to one file for each of your Network Stations, you can copy this file to the $UserBase/profiles directory and call it `allncs.nsm`.

The allncs.nsm download profile contains settings for all Network Stations so all Network Stations read it during their boot process. This means that if it contains the lines that configure a Network Station for kiosk mode, all Network Stations will switch into kiosk mode.

If you should already have an allncs.nsm file (for example, if you have made changes in NSM that is stored in the allncs.nsm file), you must manually merge the commands from the kiosk file with the information in your existing allncs.nsm file. Since this may be tricky, you could delete your allncs.nsm file, copy the template to allncs.nsm, and then make your changes again. Then, NSM will take care of the merging part for you.

An alternative would be to save the information in the allkiosk.nsm file similar to the method suggested in the following section.

16.2.2 Step-by-step instructions for multiple application kiosk setup

The techniques and supporting file structures described in this section were first released with NSM V2R1M0 PTF 4 in February 2000. Prior releases and PTF levels do not contain all of the support referenced here.

During the boot process, the Network Station reads a number of configuration files. These files control the capabilities of the workstation itself (for example, printing, display, mouse, and so on) as well as the environment for the end user. The files are generated by NSM and contain eXtensible Markup Language (XML) directives to populate the registry. The registry is read by the operating system, desktop, and applications to determine the customizations to be applied. It is similar in concept to the Microsoft Windows 95/98/NT registry.

To build the registry in kiosk mode, the following files are read in order:

- $UserBase/profiles/shipped.nsm (shipped defaults; should not be edited).
- $UserBase/profiles/allncs.nsm (NSM-configured system-wide workstation preferences; should not be edited).
- $UserBase/profiles/allkiosk.nsm file if it exists.
- If no allkiosk.nsm file is present, the $UserBase/profiles/ncs directory is then searched for an nc-id.nsm file, where *nc-id* is the host name, MAC address, or IP address of the booting Network Station. The files are searched in that order. If more than one file matches (for example, a hostname.nsm and IP_address.nsm), the results are unpredictable.

After the registry is populated with the workstation environment, the windowing system (Xwindows) initializes and the login process starts. Login then starts the window manager. If any of the .nsm files contained a setting indicating that the terminal is to boot in kiosk mode, then the login dialog is bypassed and the application specified in the registry as the kiosk application is started.

Since there is no user login in kiosk mode, there is no concept of a user or group. Therefore, the $UserBase/profiles/allusers.nsm is not read, nor are any of the group/user preference files in $UserBase/profiles/groups and $UserBase/profiles/users used.

16.2.2.1 Creating the kiosk file

The remainder of this section discusses setting up kiosk files that allow multiple applications to be run. The focus is on bringing up the Network Station desktop and then launching the applications either via icons or through the Startup folder.

The methodology for building these environments will be to use NSM to create and customize the workstation and desktop and application environment. These preferences will then be placed in a single workstation configuration file or allkiosk.nsm file. The following steps take you through the process.

In kiosk mode, only the first application that launches is chromeless. Since the desktop is the first application, it is effectively the chromeless application even though it isn't “chromed” from the beginning. Applications launched via desktop icons or the Startup folder appear with window decorations unless other resources are set up to remove the chrome. Several of the applications have special controls in their .ksk file, such as invoking the nsmrun program.

The steps for creating the files needed to run multiple applications in kiosk mode are shown here. This setup assumes that these applications will be launched from the desktop. Section 16.2.3, “Multiple applications without a desktop” on page 538, discusses running without the desktop.

1. Save files.

   The procedures described in subsequent steps cause the $UserBase/profiles/allncs.nsm and $UserBase/profiles/allusers.nsm files to be changed. You should make backup copies of these files prior to starting. If you restore these files at a later time, you will return to the NSM configuration in place before the kiosk setup started. If you forget to make backups or they are unavailable or unusable for some reason, default versions can be retrieved from $ServBase/defaults.

2. Configure preferences.

   a. Start NSM. After logging in (you need to be the administrative user), choose **System** in the **Set Preference Level:** box.

   b. From the **Setup Tasks** menu, click on each task that you want to perform. Be sure to click the **Save** button when you complete each panel.

   c. It is possible to auto start one or more of the applications when in kiosk mode. To enable this, simply add the applications to the Startup folder on the Launch Bar Settings panel. It is also possible to hide the Start menu, constrain the windows to the desktop, and remove the memory meter all through NSM. The only desktop information that cannot be changed is the Startup icon. It is present on every desktop. Although it can be manually deleted, this is not recommended.

3. Test the configuration.

   At this point, you should test the configuration to make sure it behaves properly. You will edit several files, so it is easier to ensure that the behavior will be as expected if you test without the kiosk mode first. Boot the Network Station normally and login as the administrative user. Unless you have configured something specific for the administrative user, you should see your desktop, icons, and applications. Test to ensure that the applications launch, that defined printers are working, and so on. Make any changes now via NSM.

   The Startup folder cannot be removed using NSM. If you do not want a Startup folder, you can remove it from the final kiosk file as explained below.

4. Create the allkiosk.nsm file.

   The result of the configuration work with NSM updates two files:

   - $UserBase/profiles/allncs.nsm
   - $UserBase/profiles/allusers.nsm

   The allncs.nsm file containing the workstation preferences is read during both normal boot and kiosk mode boot. However, since there is no notion of a user when in kiosk mode, the user preferences that were configured and stored in allusers.nsm are not read. Therefore, the allusers.nsm file must be copied to a new file called allkiosk.nsm in the same directory.

5. Add the kiosk flag.

   Everything is now complete except to set the flag, which tells the login manager to start up the system in kiosk mode rather than continuing on to a full or suppressed login. In the allkiosk.nsm file, find the line:

   ```
   <OBJECT NAME="/login/session">
   ```

   Then find the first occurrence of `</OBJECT>`, which follows that line.

   Insert the following lines prior to the </OBJECT> line:

   ```
   <CATEGORY NAME="KIOSK">
   <PROPERTY NAME="commands" TYPE="LIST" ACTION="APPEND">
   <ELEMENT>
   <FIELD NAME="op">SET</FIELD>
   <FIELD NAME="arg1">NSM_KIOSK_MODE</FIELD>
   <FIELD NAME="arg2">ON</FIELD>
   </ELEMENT>
   </PROPERTY>
   </CATEGORY>
   ```

For VT emulation, as in our example, you also need to add the following lines from the nsterm.ksk file prior to the </PROPERTY> line:

```
<ELEMENT>
<FIELD NAME="op">RUN</FIELD>
<FIELD NAME="arg1">/usr/bin/nsmrun nsterm</FIELD>
<FIELD NAME="arg2">FALSE</FIELD>
</ELEMENT>
```

Save the result back into the allkiosk.nsm file.

The $ServBase/defaults/app.ksk file for each application should be checked to see if there are any additional setup parameters for kiosk mode. Several of the applications use the `nsmrun` command and some resource settings to turn off the window decorations. If this is the desired behavior, these lines can be copied into the appropriate object definitions in the allkiosk.nsm file.

If you do not need a Startup folder and do not want the Startup icon on the desktop, remove the lines beginning with:

```
<MENU NAME="Startup-FOLDER-system-1">
```

and ending with the matching </MENU> from the allkiosk.nsm file.

6. Test the configuration again.

   Test again the Network Station to boot from the server. It should recognize and process the allkiosk.nsm file and come up in kiosk mode. You can then test the applications to ensure that everything works correctly.

   If you have any behavior problems with an application, check first to see that you set up the correct information in NSM. Then check the appropriate single-application template kiosk files in the $ServBase/defaults directory to ensure that any kiosk-specific options are in the allkiosk.nsm file.

7. Deploy the configuration.

   If every Network Station is to boot to the same kiosk, you are finished. You can also create individual workstation configuration files for Network Stations that need to be booted using kiosk mode or with some other desktop preferences by moving the allkiosk.nsm file to $UserBase/profiles/ncs/nc-id.nsm. Note that if you have an allkiosk.nsm file, any workstation configuration files are ignored.

   The naming and placement of the multiple application kiosk file is the same as that for a single application file. Refer to the *IBM Network Station Manager Advanced Information* publication for more information on kiosk file naming.

16.2.3 Multiple applications without a desktop

The previous sections discussed the setup for kiosk mode using the desktop to contain icons for launching the applications and using the Startup folder to autostart some or all of the applications. There may be cases where the desktop is not required and the customer wants to start up multiple applications with no desktop. The windowing system is active, so windows can be moved, resized, and iconified using the mouse. The Alt+Tab key sequence can also be used to move among the windows. However, since there are no desktop icons, if an application is closed, it cannot be restarted. If the application on the exec line (see below) is closed, the entire script is re-executed and all the applications restart. This may require some user training.

The procedure for doing this is a combination of the multiple application setup discussed in the prior sections and the single application kiosk setup. Since only a single application can be started in kiosk mode, a script is created to be that application (rather than the desktop as in the previous section). This script then launches the desired applications. Each application, except the last, is placed in the background (in UNIX parlance). The final application is started using the `exec` command to replace the script's execution with its own.

Note: Do not worry if you don't know UNIX. Like the XML examples, this is pretty much a cut and paste function.

Rather than provide a lengthy explanation, an example is used to illustrate how to create the appropriate files. The example scenario is the same as we used for the desktop kiosk setup (VT220, 5250, and Netscape).

Begin by using the multiple application kiosk setup procedure to create the allkiosk.nsm file. Remove the lines enclosed with:

```
<PACKAGE NAME="/desktops/default">
</PACKAGE>
```

Then, add the following lines:

```
<OBJECT NAME="/desktop/preferences">
<CATEGORY NAME="DESKTOP">
<PROPERTY NAME="desktop_command">/usr/local/bin/kiosk_script</PROPERTY>
</CATEGORY>
</OBJECT>
```

If all Network Stations are to boot in this kiosk mode, you are finished. To make it a workstation configuration file, rename it to $UserBase/profiles/ncs/nc-id.nsm. Note that if you have an allkiosk.nsm file, any workstation configuration files are ignored.

Next, create the shell script in $ProdBase/usr/local/bin/kiosk_script. This script will contain the command lines from the allkiosk.nsm file as shown here:

```
#/bin/sh
#
# These applications must be placed in the background by using the
# '&' at the end of the command. Otherwise, these commands are
# identical to the commands defined in the *.ksk templates
nsm_wrapper nsterm -host bissell.austin.ibm.com -title "VT\ 220\ Emulator" -ti vt220
-geometry
nsm_wrapper ns5250 rocket.austin.ibm.com -geometry 9999x9999+0+0 &
#
# The last application must be executed on this process and not put in
# the background. Otherwise, this script process will terminate
# and will trigger a logout event.
exec run_netscape http://bissell.austin.ibm.com/nc
```

16.3 Suppressed login mode

In the suppressed login mode, as opposed to kiosk mode, a user is actually logging on when the Network Station is powered on. The logon dialog, however, is not displayed to the end-user. Instead, a pre-defined user ID and password are used to automatically logon the Network Station, without any user intervention. For an end user, the suppressed login mode looks the same as the kiosk mode. The user does not have to log on in either mode.

The main advantage of having a user logged on is that preferences and other settings *can* be stored in the home directory and retrieved the next time the Network Station is powered on. However, as you will see, it may not always be appropriate to enable users to store preferences. With the suppressed login mode, you also have somewhat higher flexibility when using NSM to configure the settings because you can use both the group and user level in NSM to make settings.

To set up a suppressed login, you identify which of your Network Stations should use suppressed login, just as you did with the kiosk mode. In suppressed login mode, you can only use the Network Stations' IP addresses or host names to address each of them. The MAC address is *not* an option.

Once you decide which IP addresses or host names should use suppressed login, you create a file with their IP addresses or host names and the user ID and password each of them should use. You can define one user ID for each individual Network Station. Or, by using wild cards, you can allow multiple Network Stations to logon using the same user ID, thus sharing it. Most of the Network Station applications work very well when using a shared user ID. The Netscape Communicator browser, however, prefers individual user IDs, one for each Network Station. Please refer to 16.5, "Application-specific considerations and other considerations" on page 549, for more information on special considerations for each of the Network Station applications.

After the list with IP address/host name and user ID/password combinations is created, it should be encrypted using a utility shipped with NSM, and then stored in the correct path for the Network Station to pick it up. The encrypted file is always called kiosks.nsl. Note that this is not really kiosk mode. Therefore, the filename is not very logical, but it is inherited from NSM V1R3, where suppressed login was the only kiosk-like mode available.

Then, when a Network Station is powered on and the ACTlogin (the one that manages the login dialog and user authentication) command is executed, it searches for the kiosks.nsl file. If found, it checks to see if it can find a match for the Network Station's IP address or host name in it. If found, it picks the corresponding user ID and password and automatically logs on with this. If a match is not found in the file (or if the kiosks.nsl file is not found at all), the login dialog is displayed and the end user has to logon manually. You can easily mix suppressed login mode with manual login mode in your network (as you can with kiosk mode or manual login mode also) by including or omitting certain Network Station's IP addresses in the kiosk file.

Now we go through these steps more in detail:

1. Decide which Network Stations should use suppressed login and find out their IP addresses or host names.
2. Create a user ID (or multiple if you don't want to share it among many Network Stations) on the NSM server. As for any Network Station user ID, you must make sure it has sufficient authority to be allowed to logon.

> **Windows NT servers**
>
> For Windows NT, this means the user must be a member of the local NSMUser group. The password (do not use a blank password) should be set so it does not have to be changed at the next logon, cannot be changed by the user, and never expires.

3. Once the user ID is created, it is time to create the source kiosk file. Use your favorite text editor to create this text file. It does not have to be in UNIX format so you can use Notepad if you're using Windows NT. We called it kiosk.txt:

```
# NStation Corp. Kiosk setup
^9\.24\.104\..*$ icauser secret
^9\.24\.105\.1[0-9][0-9]$ normalnc secret
^9\.24\.105\.8$ webkiosk1 hemligt
^9\.24\.105\.9$ webkiosk2 hemligt
^9\.24\.105\.10$ webkiosk3 hemligt
^9\.24\.105\.11$ webkiosk4 hemligt
^demo corplogo abc
```

The syntax for this file is called Regular Expression Notation. It's the same that was used to setup suppressed login in NSM V1R3. The syntax may not be the most trivial or intuitive you have seen. As usual when something is complicated, it's powerful. See 16.3.2, "Regular Expression Notation" on page 544.

Our file defines the following behavior:

- All Network Stations with an IP address of 9.24.104.xxx will log on with user ID `icauser` and password `secret`. This means that a whole C-class subnet is used. We can then configure the user `icauser` to only run the ICA client.
- All Network Stations with an IP address in the 9.24.105.100 to 9.24.105.199 range will logon with the user ID `normalnc` and password `secret`. We could then configure this user ID to autostart the 5250 emulator and to give it access to the ICA client and the VT emulator on the Launch Bar.
- The Network Stations with an IP address in the 9.24.105.8 to 9.24.105.11 range will logon with user ID `webkiosk1` to `webkiosk4` respectively. We can then configure these user IDs to run the Netscape browser. Then each Network Station will have their own user ID, which works best with Netscape.
- All Network Stations that have a host name beginning with `demo` (such as demoabc demo1, demo25, etc.) will logon with the user ID `corplogo` and password `abc`. We could then use NSM to configure the corplogo users to only run a Java applet with a spinning 3D logo for our company, for example to use in showrooms.
- All other Network Stations will display the manual login prompt.

Make sure you press Enter after each line, even if you have only entered one single line. Otherwise, the encoding program may not work.

The kiosk file is read from top to bottom and the first matching pattern found is used.

4. Encode the file so the passwords it contains do not show up in clear text. Each platform (AS/400, RS/6000, and Windows NT) does this differently. Please refer to Table 80 for more information.

Table 80. Platform-by-platform kiosk file encoding commands

Platform	Program Syntax

AS/400	`CALL PGM(QYTC/QYTCMTKS)`
	`PARM('/QSYS.LIB/MYLIB.LIB/MYFILE.FILE/KIOSKS.MBR' '37')`
	• `'/QSYS.LIB/MYLIB.LIB/MYFILE.FILE/KIOSKS.MBR'` is the full path and name of the unencoded file.
	• `'37'` is the CCSID value. This parameter is optional and defaults to CCSID 37 if omitted.

RS/6000	`/usr/netstation/bin/createKIOSKS kiosk.source` `kiosk.source` is the name of the unencoded file.
Windows NT	`d:\nstation\servbase\bin\nsmkiosk x:\myDir\kiosk.source` • `d:\` is the default installation drive and path. • `x:\myDir\kiosk.source` is the full path and name of the unencoded file.

If the encoding is successful, it does not display any output to the screen, but it creates the kiosks.nsl file in the $UserBase/profiles/ncs directory.

If nsmkiosk encounters an error, it displays an error message (numeric) on the screen. Use Table 81 to determine the action to take given an error code.

Table 81. nsmkiosk error codes, descriptions, and actions

Error code	Description	Action
1	The unencoded filename parameter is not specified.	Make sure that you specified a parameter with the name of the unencoded file.
2	The CCSID parameter is not valid.	Make sure that you specified a valid CCSID.
3, x	The unencoded file cannot be opened or read.	Make sure that you specified the correct full path and name of the unencoded file. Make sure that the user running the encoding program has the correct authority to read the unencoded file.
4, x	The encoded file cannot be created or written.	Make sure that the user running the encoding program has the correct authority to create or write the encoded file.
5	An internal code page conversion error has occurred.	Contact IBM Service.

Error code	Description	Action
6	There is invalid data in the unencoded file.	Make sure that the unencoded file is created following the instructions in step 3. If you specified a CCSID as an input parameter, make sure that it matches the CCSID with which the file was created.

After you perform these steps, you should go into NSM and configure settings for the user ID you will use for the suppressed login mode. This is done the same as you would do with any normal user ID.

Since the unencoded kiosk.txt file contains passwords in clear text, you should consider moving it to a secure location where end users do not have access to it. On the other hand, the user IDs and passwords you use for kiosk login are usually not given any extended permissions. Even if a user would manage to obtain one of these “secret” user IDs, they would probably not be able to do a lot harm.

16.3.1 Suppressing the launch bar

In suppressed login mode, the user has access to the launch bar so they can launch any applications provided to him there. If you want, you have the option of disabling the complete launch bar and, for example, only auto starting the applications the user should have access to. You auto-start applications by adding their icons to the Startup folder in NSM.

To do this, you must override the default setting for the NC Registry desktop_command with another value. The default value for this setting is ncdeskmgr, which launches the launch bar itself. In kiosk mode, the kiosk templates handles this for you and sets the desktop_command setting to the application used in each template file.

Attention

This technique is a work-around that we discovered. It is not supported by IBM so it should only be used by advanced users. Be sure to make backup copies of any files you manually alter. If you have trouble, restore your original configuration files.

To remove the launch bar, you can use the following XML coding:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCREGISTRY SYSTEM "ncregistry.dtd" >
<!-- No Launchbar example -->
<NCREGISTRY>
<OBJECT NAME="/desktop/preferences">
<CATEGORY NAME="DESKTOP">
<PROPERTY NAME="desktop_command"> </PROPERTY>
</CATEGORY>
</OBJECT>
</NCREGISTRY>
```

As you see, it replaces the ncdeskmgr with a space (between "desktop_command"> and </PROPERTY), which disables the ncdeskmgr and thus the Launch Bar.

If you want all your Network Stations to use this, you can create this file and copy it to $UserBase/profiles and call it allncs.nsm. This is the download profile read by all Network Stations (see 8.4, “Download profiles” on page 173).

If you only want specific Network Stations to suppress the Launch Bar, you can create this file for each individual Network Station that should suppress it. As usual, you can name these files for each Network Stations using the IP address, host name or MAC address. You should create one for each Network Station and copy it to the $UserBase/profiles/ncs directory.

For example, let’s say we created four files called 9.24.105.8.nsm to 9.24.105.11.nsm with the above syntax and used the kiosk file we created above. These four Network Stations that used suppressed login to run the Netscape browser would not display the Launch Bar.

16.3.2 Regular Expression Notation

The Regular Expression Notation is a powerful set of characters that can be used to perform character-based matching, for example, to match IP addresses, host names, and so forth. This is used both when setting up suppressed login mode, but also when using the NSM Command Line interface.

Table 82 lists the Regular Expression Notation special characters and their meaning.

Table 82. Regular Expression Notation special characters and their meaning

Pattern	Description
string	String (no special characters): A string with no special characters matches the first IP address or host name that contains the string.
[set]	Set: Matches a single character specified by the set of single characters within the square brackets.
^	Caret: Signifies the characters following the ^ are the beginning of the IP address or host name.
$	Dollar: Signifies the characters preceding the $ are the end of the IP address or host name.
.	Period: Signifies any one character. The period means match *any* character, not just the period in an IP address.
*	Asterisk: Signifies zero or more of preceding character.
\	Back slash: Signifies an escape character. When preceding any of the characters that have special meaning, the escape character removes any special meaning from the character. The back slash is useful to remove special meaning from a period in an IP address.

Using these characters, it's possible to perform matching between, for example, the Network Station's IP address or host name and those in the kiosk file. Table 83 shows some examples.

Table 83. Regular Expression Notation examples

Pattern	Examples of IP addresses or host names that match
10.2.1.9	10.2.1.9, 10.2.139.6, 10.231.98.6
^10\.2\.1\.9$	10.2.1.9
^10\.2\.1\.1[0-5]$	10.2.1.10, 10.2.1.11, 10.2.1.12, 10.2.1.13, 10.2.1.14, 10.2.1.15
kiosk	kiosk01, mykiosk, akioskbc
^kiosk$	kiosk
^kiosk0[0-4][0-9]$	kiosk000 through kiosk049
kiosk[3-8]	kiosk3, mykiosk4, akiosk5b
^kiosk	kiosk01, kiosk
kiosk$	mykiosk, kiosk, 3kiosk
kiosk...	kiosk123, mykioskabc, akiosk09bcd
kiosk*1	kiosk1, mykios1, akiosk1abc, kioskkkkkk12
^kiosk0..	kiosk001, kiosk099, kiosk0abcd
^kiosk0..$	kiosk001, kiosk099

Table 84 shows another more detailed example of using the wild cards to create a pattern. The pattern is in the left column. The next column shows the only possible matches for each position. The last two show possible IP address matches. The same method can be used using host names instead of IP addresses.

Table 84. Regular Expression Notation detailed example

Pattern 9\.24.1.4.24[0-9]	Matches	Matches 9.24.104.248	Matches 119.24.154.245
9	9, x9, xx9	9	119
\.	.	.	.
2	2	2	2
4	4	4	4
.	Any character including .	.	.
1	1	1	1
.	Any character including .	0	5
4	4	4	4
.	Any character including .	.	.
2	2	2	2
4	4	4	4

Pattern 9\.24.1.4.24[0-9]	Matches	Matches 9.24.104.248	Matches 119.24.154.245
[0-9]	0,1,2,3,4,5,6,7,8,9 (must be present)	8	5

Since there was no delimiting character at the beginning (^), the string could be preceded by more digits. Since the maximum characters between the periods is three in an IP address, this pattern leaves little room for flexibility. Having three characters the 24[0-9] string predetermines that the character before it must be a period (.). This is not a practical example but illustrates the use of the special characters.

A more practical example shown in Table 85 would be the following pattern that would apply to a range of IP addresses or host names assigned to the Network Stations that use the suppressed login mode:

```
^192\.168\..*\..*$ kiosk1 kpass
```

This lets all Network Stations with an IP address starting with 192.168 (a whole B-class subnet) automatically log in with user ID kiosk1 and password kpass.

Table 85. Regular Expression NOtation practical example

Pattern ^192\.168\..*\..*	Matches	Matches 192.168.2.1	Matches 192.168.244.53
^192	192	192	192
\.	.	.	.
168	168	168	168
\.	.	.	.
.*	0-999	2	244
\.	.	.	.
.*	0-999	1	53

The ^ specifies that this is the beginning, and no characters can precede 192. The * says 0 or more of the preceding character (., meaning any character). In an IP address, this leaves room for one to three digits.

You could narrow this down to only a C-class network IP with:

```
^192\.168\.10\..*$ kiosk1 kpass
```

16.4 Boot scenarios for kiosk and suppressed login mode

This section looks at three scenarios for the kiosk and suppressed login modes.

16.4.1 Boot server in kiosk mode

The methodology described in 16.2.3, “Multiple applications without a desktop” on page 538, is ideal for creating a boot server-only system. First, create allncs.nsm/allkiosk.nsm files on a system that has NSM loaded. This system will be the management server. Then, install only the NSM boot server code on the machines to be used as boot servers (such as the in-store processor in a retail environment). Lastly, transfer the allncs.nsm and allkiosk.nsm files from the management server to each of the boot servers using the protocol or management package you normally use to maintain your servers. Some customization may be necessary for IP address, host names, and so on.

As user needs change, you need to run NSM on the management server to make the appropriate changes and to merge and deploy the new allncs.nsm and allkiosk.nsm files.

16.4.2 Flash boot using kiosk files

Creating a compact flash card to use with the multiple application kiosk mode as described in this section is straightforward. The Flash Manager tool in NSM has an option to create a card in kiosk mode. The workstation configuration files or the allncs.nsm file and the shipped.nsm file are automatically picked up by the Flash Manager when a kiosk mode card is built.

Start NSM and then start the Flash Manager. Choose **Kiosk Files** from the NSM Configuration drop-down list on the first panel. From the Applications panel, select the applications to put on the flash card. Naturally, these should match the applications that were selected when the Desktop Launch Bar was configured.

Return to the Setup/Create screen, and click the **Create Image** button. A new card image will be created that contains the kiosk files.

Note: As of PTF 4, the allkiosk.nsm file is not automatically copied to the flash image directory. The workaround is to manually copy $UserBase/profiles/allkiosk.nsm to $UserBase/flash/Images/image_name{x86|ppc}/termbase/profiles/allkiosk.nsm. You will also have to edit the flash BOM file in $UserBase/flash/Images/image_name{x86|ppc}BOM to add an entry for allkiosk.nsm.

See Chapter 6, “Flash card management” on page 143, for more information.

16.4.3 Using DHCP with kiosk mode and suppressed login mode

When setting up Network Stations for either the kiosk mode or suppressed login mode, using DHCP can be both an advantage and a disadvantage.

Let’s say you have 200 Network Stations that you want to run in kiosk mode displaying, for example, the ICA client, an emulator, or the Netscape browser. All Network Stations are located on the same physical LAN segment (and TCP/IP subnet). On this segment, you have one NSM server serving these machines. Also, you have no other Network Stations on that segment (but you may have a number of PCs). In this case, DHCP works fine and gives you a simple setup. You copy the kiosk template file (ica.ksk, for example) to the allncs.nsm file and modify it to suit your environment. All Network Stations that boot from this NSM server would then run in kiosk mode, regardless of their IP address.

On the other hand, if you want to add, say 20 Network Stations to this segment and these should *not* run in kiosk mode, you cannot simply copy the kiosk file to the allncs.nsm file. Otherwise, it will cause all Network Stations to run in kiosk mode. Also, you cannot simply create 200 kiosk files, based on IP addresses, since you don’t know which IP addresses the 200 machines will get and which IP addresses the 20 machines will get.

In this case, you may consider using the suppressed login mode instead of kiosk mode and assign the 20 extra Network Stations static IP addresses. This way, you can define that the range of IP addresses given to the 200 Network Stations should use suppressed login and all others should display the manual login prompt. You would do this configuration in the kiosk.txt file as documented 16.3, “Suppressed login mode” on page 539.

If you still want to use kiosk mode, you have to assign static IP addresses to the 20 Network Stations, so you know what range the 200 Network Stations would fall in. Then you could create 200 kiosk files, one for each possible IP address.

Another possibility is to address the 200 Network Stations using their MAC address. This would require you to keep track of these MAC addresses, which we usually try to avoid.

You can also address them using their host names. However, then you would need to set up a DDNS and track the MAC addresses anyway.

However, if the 200 Network Stations were of one model, say S300, and the 20 Network Station of another, say S2800, you could setup an extra NSM server. By using DHCP classes, you could redirect the 200 S300 machines to one NSM server and copy the kiosk template to the allncs.nsm filename. The other 20 Network Stations would be directed to the other NSM server. You would not have any special kiosk or suppressed login configuration, just a normal setup. This setup would require a DHCP server that can support DHCP classes, like the eNetwork On-Demand DHCP server shipped with NSM for Windows NT or the DHCP server on the AS/400 system.

If you have NSM on Windows NT and you do not want to setup an extra NSM server, you can perform this trick:

1. Create a new directory on your (single) NSM server, and call it, for example: `x:\{float}\NetworkStationV2\userbase\nsmkiosk`. Make sure the group NSMUser has read access to it.
2. Export this directory using the eNetwork On-Demand NFS server as read-write and with the alias /NetworkStationV2/userbase/nsmkiosk.
3. Make any configuration settings in NSM as you prefer. As always with kiosk mode, since no user will be logged on, you can only make changes to the system level.
4. Copy the download profiles (these now contain the modifications you just made) from the x:\{float}\NetworkStationV2\userbase\profiles directory to the x:\{float}\NetworkStationV2\userbase\nsmkiosk directory. You need the shipped.nsm and allncs.nsm files (if they exist).
5. Copy the kiosk template you want to the x:\{float}\NetworkStationV2\userbase\nsmkiosk\allncs.nsm file, and modify it to suit your environment. This way, all Network Stations that read their download profiles from the nsmkiosk directory will read this allncs.nsm file and switch into kiosk mode.
6. In your DHCP server, set up the class corresponding to the 20 Network Station S2800 (the class is called IBM 8364-EXX for Ethernet models and IBM

8364-TXX for Token-Ring models) to read their configuration information from the default directory /NetworkStationV2/userbase/profiles. Then, set up the class corresponding to the 200 Network Station S300 (the class is called IBMNSM 2.1.0 for Ethernet models and IBMNSM 1.1.0 for Token-Ring models) to read their configuration information from the /NetworkStationV2/userbase/nsmkiosk directory. Your DHCP option 213 (which defines the path to the download profiles) would look like the example in Table 86.

Table 86. DHCP option 213 example

Network Station S2800 class	Network Station S300 class
/NetworkStationV2/userbase/profiles	/NetworkStationV2/userbase/nsmkiosk

This causes the 20 Network Station S2800 to read the default /NetworkStationV2/userbase/profiles/allncs.nsm file, which does not contain any kiosk mode configuration. They work according to any settings you make in NSM. The 200 Network Station S300 will read the /NetworkStationV2/userbase/nsmkiosk/allncs.nsm file, which has a kiosk configuration in it, and they will switch into kiosk mode. Since no user logs on in kiosk mode, they will not look for the /userbase/home, the /userbase/profiles/groups, or the /userbase/profiles/users directories.

If you use this setup, make sure to backup your nsmkiosk directory before upgrading NSM to a newer version, as it may remove this unknown directory. Also, any changes you make in NSM will not affect the download profiles in the nsmkiosk directory (as NSM is unaware of this directory). If you want to modify any settings for your kiosk machines, you need to backup the allncs.nsm and allusers.nsm file in the \userbase\profiles directory, copy these files from the \userbase\nsmkiosk directory to \userbase\profiles. Then, make configuration settings in NSM (which updates the files in \userbase\profiles), and copy the updated files from the \userbase\profiles directory back to the \userbase\nsmkiosk directory. Finally, restore the backup of the original files in the \userbase\profiles directory. If changes were made to the allusers.nsm file, you must manually migrate them into the allncs.nsm file.

As you see, using DHCP can be both a blessing and a curse when it comes to kiosk mode and suppressed login mode setups. If you understand how the Network Station works, you can most likely turn DHCP to your advantage.

16.5 Application-specific considerations and other considerations

Each local Network Station application has its own behavior and, therefore, may run better or worse in kiosk or suppressed login mode. We briefly discuss some of the considerations you should take into account when deciding which mode to use.

16.5.1 Disabling screen capturing

When running Network Stations in kiosk mode (and usually also in suppressed login mode), it is often desired to deny the user the ability to capture screen shots, which are stored in the user's home directories. This is especially true for kiosk mode, where the home directory remains in the IFS in RAM. Capturing screens can quickly fill up this memory.

The easiest way to disable screen capturing is to use the NSM Command Line Interface. For information on how to use the NSM Command Line see 8.5, “NSM Command Line Interface” on page 180.

If you are using suppressed login mode, you can disable screen capturing for the user ID that you use to automatically log on a Network Station with the following NSMCL commands (assume the user ID is called webkiosk):

```
INSERT IBMNSM/USER/webkiosk/DESKTOP/key_print_screen/ nil
INSERT IBMNSM/USER/webkiosk/DESKTOP/key_print_window/ nil
COMMIT
```

If you have separate user IDs for each Network Station, you must run these commands for each user ID (can be done by adding the user IDs to a list and then use the NSMCL list capabilities). Or, you can add the user IDs to a group and use the following NSMCL commands (assume the group is called webkioskgroup):

```
INSERT IBMNSM/USERGROUP/webkioskgroup/DESKTOP/key_print_screen/ nil
INSERT IBMNSM/USERGROUP/webkioskgroup/DESKTOP/key_print_window/ nil
COMMIT
```

When using the kiosk mode, we did not find any way to use the NSMCL utility to make these settings and automatically incorporate them either into each individual Network Stations’ <nc-id>.nsm file in the $UserBase/profiles/ncs directory or to the allncs.nsm file. NSMCL does not allow you to set this parameter on a workstation-basis, but only the user, group, or system level. Therefore, it cannot write it into the <nc-id>.nsm files. When performing the `settint` command on the system level, the changes are made to the allusers.nsm file. Because this is a so-called Session profile, it is not read until a user logs on. In kiosk mode, no user logs on, so the allusers.nsm file is never read in kiosk mode. Therefore, we had to modify the download profiles manually.

To do this, we modified our <nc-id>.nsm kiosk file ($UserBase/profiles/ncs/9.24.104.192.nsm) and added two lines to it. We used the 5250 emulator as an example (5250.ksk) (Figure 429).

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCREGISTRY SYSTEM "ncregistry.dtd" >
<!-- 5250 Emulator Sample Profile for Single Application (kiosk) Mode -->
<NCREGISTRY>
<OBJECT NAME="/config">
<CATEGORY NAME="WORKSTATION">
<PROPERTY NAME="pref-screen-background-color">black</PROPERTY>
</CATEGORY>
</OBJECT>
<OBJECT NAME="/desktop/preferences">
<CATEGORY NAME="DESKTOP">
<PROPERTY NAME="desktop_command">nsm_wrapper ns5250 was40.got.se.ibm.com -geometry
9999x9999+0+0</PROPERTY>
<PROPERTY NAME="key_print_screen" TYPE="STRING">nil</PROPERTY>
<PROPERTY NAME="key_print_window" TYPE="STRING">nil</PROPERTY>
</CATEGORY>
</OBJECT>
<OBJECT NAME="/login/session">
<CATEGORY NAME="KIOSK">
<PROPERTY NAME="commands" TYPE="LIST" ACTION="APPEND">
<ELEMENT>
<FIELD NAME="op">SET</FIELD>
<FIELD NAME="arg1">NSM_KIOSK_MODE</FIELD>
<FIELD NAME="arg2">ON</FIELD>
</ELEMENT>
</PROPERTY>
</CATEGORY>
</OBJECT>
</NCREGISTRY>
```

Figure 429. Kiosk template file for 5250 emulator with screen capturing disabled

As you can see, we added the following two lines after the desktop_command that starts the 5250 emulator:

```
<PROPERTY NAME="key_print_screen" TYPE="STRING">nil</PROPERTY>
<PROPERTY NAME="key_print_window" TYPE="STRING">nil</PROPERTY>
```

If using the allncs.nsm file for configuring kiosk mode, the same line should be added to that file instead.

16.5.2 3270, 5250, and VT emulator

All the emulators work very well in both kiosk and suppressed login mode. One point to consider, however, is that it’s usually best to turn off keyboard and color mapping. That way, a user is not fooled into believing that the changes they make will remain until the next time they power on their Network Station.

It often also makes sense to turn off all menus (for example, File, Edit, Options) to get the emulators to run in “true” full-screen mode. This is done using NSM.

As long as the user does not have the ability to store any preferences (keyboard mapping for example), you can use one shared user ID for all your Network Stations if you use suppressed login.

16.5.3 ICA client

The ICA client is also another application that is suitable both for kiosk mode and suppressed login mode. To set up a network of Network Stations to act as

Windows-Based Terminals (WBTs) is simple. Since it's a common setup, we describe the steps in Chapter 19, "Network Station as a Windows-based terminal" on page 605.

16.5.3.1 Suppressed login

Since the ICA client doesn't store any user-made preferences in the user's home directory, you can use one shared user ID for all your Network Stations if you use suppressed login.

If you deny the user the ability to create new connections in the ICA Remote Application Manager, you can use one shared user ID for all your Network Stations if you use suppressed login.

16.5.3.2 Kiosk

If you want, you can also start the ICA Remote Application Manager in kiosk mode. It then displays the list of pre-configured published applications and Metaframe servers to which your users can connect. In this case, you want to deny the users the ability to create new connections.

16.5.4 Netscape browser

The browser can run in both kiosk mode and suppressed login mode.

16.5.4.1 Suppressed login mode

When the browser starts, it creates a lock file in the user's home directory. This lock file contains information on which Network Station the browser runs. If a lock file is already present when the browser starts and it's not from the same Network Station, the browser displays a warning message. This message says that someone else is using the browser with the same user ID, and therefore, the user is not allowed to update the bookmarks, cookies files, etc. Only the first user starting the browser has write access to these files. Therefore, the browser does not run very well in suppressed login mode where the Network Stations share a single user ID. Either run the browser in kiosk mode or assign one user ID to each individual Network Station.

16.5.4.2 Kiosk mode

If the browser runs in kiosk mode, the home directory is stored in the *In-memory File System* (IFS).

Note: This IFS is for a Network Station running in kiosk mode and should not be confused with the AS/400 System's Integrated File System (IFS).

This means it will be empty every time the Network Station is powered on and the browser starts. Therefore, the browser will have to populate the home directory with the necessary files. This may slightly extend the browser's start up time.

Also, if running in kiosk mode, you should consider giving your users a pre-defined set of bookmarks. This can be done as described in 12.9, "Deploying standard enterprise bookmarks" on page 365.

16.5.5 Java applications and applets

How suitable a Java application or Java applet is to run in either kiosk mode or suppressed login mode depends solely on the application or applet itself. As long as an application does not require write access to a home directory where it needs to store persistent data, it usually runs fine in kiosk mode.

Chapter 17. Printing

This chapter gives you a high-level overview of the printing capabilities of the IBM Network Station. This subject is covered in detail in the *IBM Network Station Printing Guide*, SG24-5212. This Printing Guide written for the Network Station Manager V1R3 and covers IBM Network Station printing thoroughly. This chapter points out any new features of printing with NSM at V2R1.

17.1 Printing capabilities of the Network Station

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

The Network Station also provides print APIs and the SERIALD module. The SERIALD module (sometimes referred to as PARALLELD) controls both the serial and parallel interfaces (not limited to printing). SERIALD has its own IP ports, which can be accessed directly by remote systems. This may be necessary for special applications such as WinCenter using WinStation printers.

Note: Some helpful hints about printing in the ICA environment can be found in 14.7.3, “Connecting to local printers” on page 476.

Figure 430 on page 556 shows the flow of the print data for the first three examples of printing explained here.

Printing from remote hosts to the IBM Network Station printer

The LPD server on the IBM Network Station can receive print requests from any remote system that implements the LPR functionality as described in RFC 1179. On receipt of these requests, the LPD server routes the print job through the local API and to the module controlling access to the local serial or parallel port where the printers are attached. The LPD server can reject requests based on an access control list.

Printing from the IBM Network Station to remote printers

The LPRD (LPR daemon) requester on the IBM Network Station can send print requests to any remote system that implements the LPR functionality as described in RFC 1179. The LPRD runs in the background, handling requests from local applications to route print jobs to remote hosts instead of the local printers. Note that print requests can only come from local applications. Print requests originating on remote hosts and received by the LPD on the IBM Network Station cannot be routed back to another remote host through the use of the LPRD. Print requests from the local application go to the print API first, which passes them to the LPRD.

Printing from the IBM Network Station to a local printer

Output sent from local applications on the IBM Network Station to a local printer is sent directly to the print API and on to the SERIALD module, which handles local printers.

LU printing from an SNA host to the IBM Network Station printer

Using the TN3270E emulator, SNA print traffic can be sent to the IBM Network Station local printer. An emulation session on the Network Station requests printer services and specifies the LU name to associate with the printer. Output sent from the host to the printer is sent to the SNA LU and forwarded by the TN3270 server to the IP address of the Network Station.

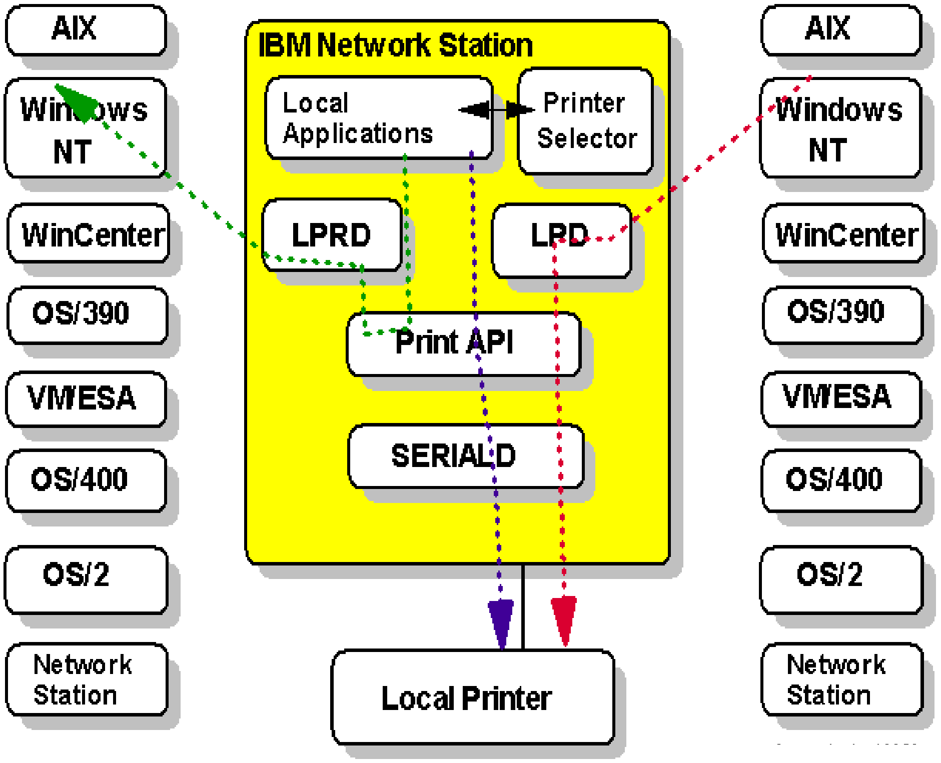


Figure 430. IBM Network Station printing

The LPR implementation on the IBM Network Station has to account for the fact that there is no local disk storage for spooling and for the restricted amount of memory. The implementation of LPR/LPD allows for two modes of printing.

Nonstreaming mode requires the entire data job to be generated completely before submitting the request to the remote printer.

Streaming mode allows the client to send a print request to a print server while the print data file is still being generated. This is useful for a print client or print server that has little or no storage, such as the IBM Network Station. Not all LPR/LPD capable products support streaming mode.

17.2 What's new in V2R1

The changes from V1R3 are minor changes for the most part. Among the changes, you will find:

- Up to 18 serial ports can now be defined on a Series 2800 because there are two native ports and possibly two PCI cards that can each support eight serial ports.

- On a Series 1000, there is one native port and a multiple serial port adapter card that allows four serial attachments for a total of five ports.
- Since the Series 2800 has two native serial ports, the IP ports 5962 (passthru mode) and 6462 (command interpret mode) have been added to the serial daemon for the second native serial port.
- The NSM configuration panels for printer settings now have a Serial Options setting that allows you to choose settings, which used to be done using override files in V1R3.
- The ASCII options for DBCS have been removed.
- The browser print dialog has changed slightly, and the print selector panel has also changed slightly, but the functionality is the same.
- The `lpr` (or `nclpr` which is equivalent) command can be used on the command line to initiate a print request.
- A print monitor window is available to display the current print jobs scheduled for local printers, which can also be canceled from that window.
- The VT emulator uses LPR/LPD.

17.3 Local application print interface

The Network Station applications produce printouts in certain formats as seen in Table 87. It is important to know what those formats are if your printer only supports one type of output.

Table 87. Supported printer formats for a given application

Application	PostScript	PCL	ASCII
5250 emulator	X	X	X
3270 emulator	X	X	X
ICA	X		
VTxxx emulation	X	X	X
Netscape	X		
Text Editor (NC Text)	X		
Calendar	X		
Paint (NC Draw)	X		

The print options and the print interface are different among the applications.

Reminder

Even though the browser on the Network Station only generates PostScript output, an alternative is available for cases where the customer wants to print to PCL printers.

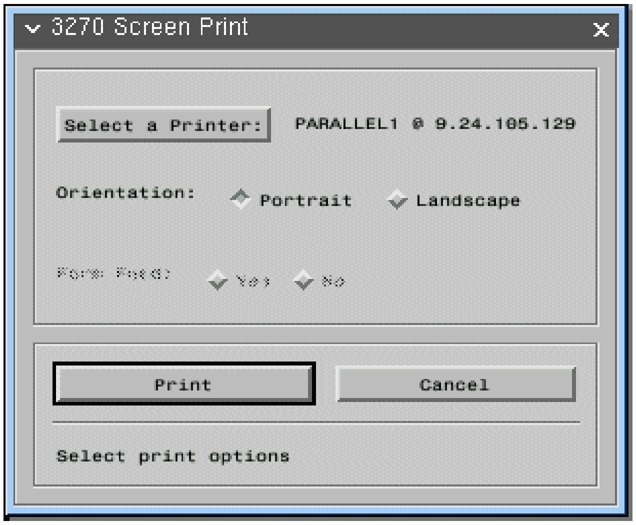
The solution is to use a Host Print Transform function, as described in *IBM Network Station Printing Guide*, SG24-5212, in Section 8.2, “Using the Transform Capabilities of Other Hosts”. An example using an AS/400 Host Print Transform is given (Figure 178 on page 174 describes this example graphically). There may be other solutions, such as GhostScript on AIX, that provide similar solutions but which were not tested prior to publication of the redbook. This redbook can be used as a reference for both NSM V1R3 and NSM V2R1 because using Host Print Transforms is the same regardless of which NSM is being used.

17.3.1 Emulator print interface

The emulators all offer local copy options:

- VT offers Print Screen and Print Scroll Buffer options from a menu.
- 5250 offers Screen Print and System options from a menu
- 3270 offers Screen Print.

The print interface, shown in Figure 431, looks the same for each of these options.



PARALLEL1 @ 9.24.105.129

Select print options

Figure 431. Emulator print selector

You can select a printer from a list of printers available to the user. You can also select the orientation and, if applicable, the form feed option.

Printer definition files are supported for 5250 and 3270 emulation. This is covered in 17.9, “Emulation PDT support” on page 569.

17.3.2 Netscape, Calendar, NC Draw, and NC Text

The Netscape, Calendar, NC Draw (Paint), and NC Text applications present a different print interface to the user. The print options for each application are found in the following menus:

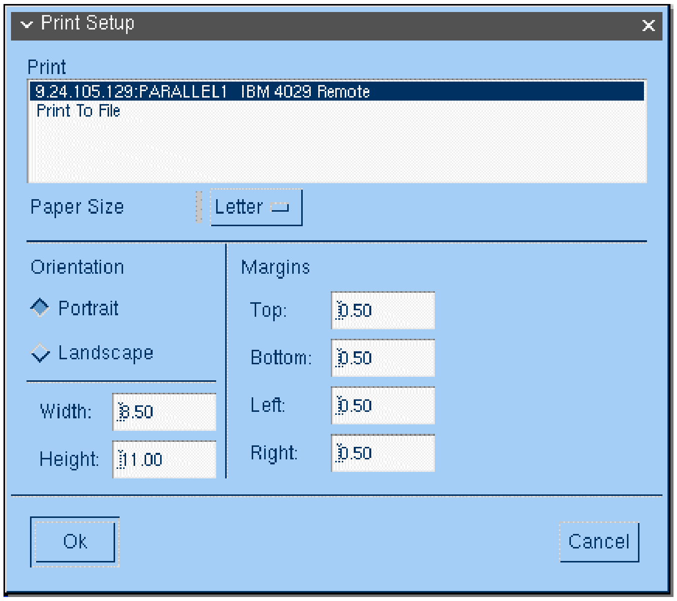
- Netscape, NC Draw, and NC Text: File->Print Setup and File->Print Frame options
- Calendar: Print Day, Print Week, Print Month, and so on buttons

Each of these applications allow you to set printer defaults with a printer setup frame, shown in Figure 432.

AS/400 printing from Netscape

AS/400 customers printing from Netscape (parallel printing) require the following system PTF (appropriate for the operating system level):

- V4R3 systems: 5769SS1-SF60984
- V4R4 systems: 5769SS1-SF60985



Print Setup

Print

9.24.105.129:PARALLEL1 IBM 4029 Remote
Print To File

Paper Size: Letter

Orientation

● Portrait
○ Landscape

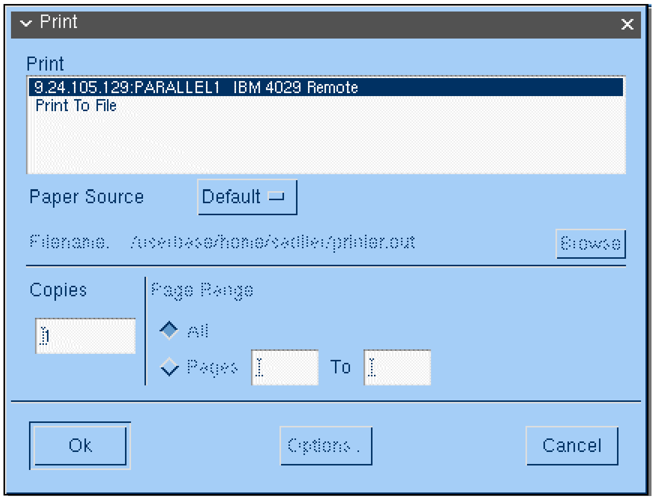
Width: 8.50
Height: 11.00

Margins

Top: 0.50
Bottom: 0.50
Left: 0.50
Right: 0.50

Figure 432. Netscape Print Setup display

Choosing the print option allows you to choose any printer and change some of the default options for this instance of printing, set in the printer setup frame (Figure 433 on page 560).



Print

Print

9.24.105.129:PARALLEL1 IBM 4029 Remote
Print To File

Paper Source: Default

Filename: /userbase/home/sadlier/printer.out

Copies: 1

Page Range
● All
○ Pages To

Figure 433. Print selection display

17.4 Printing to a local printer from Network Station applications

The Network Station supports local printers attached to the parallel or serial ports. To use the printer as a local printer for that Network Station, you must use NSM to define the local printer at the system or workstation level. Unless all workstations have local printers attached, you will most likely define them at the workstation level. A local printer defined at the workstation level will be available to all users that log on to that Network Station.

Bypass check for Carrier Detect

Some special printers do not assert Carrier Detect even when powered on. This causes the Network Station to think that the attached printer was powered off even though it was physically powered on and ready to print.

To circumvent this problem, IBM implemented a port-specific environment variable to bypass the check for Carrier Detect for special printers. During processing of a print job to a serial printer, the print code looks for an environment variable by the name “SERIALX_NOCD” where X stands for the port being used. For example, if a user is printing to the print queue SERIAL1, the print code will check to see if the environment variable SERIAL1_NOCD is exported and is set to a value of 1. Only then, it circumvents the check for Carrier Detect for the printer attached to the particular serial port. The environment variable can be set in NSM at the system level, user level, or group level.

This workaround applies to all S/2800, S/2200, S/1000, and S/300 models.

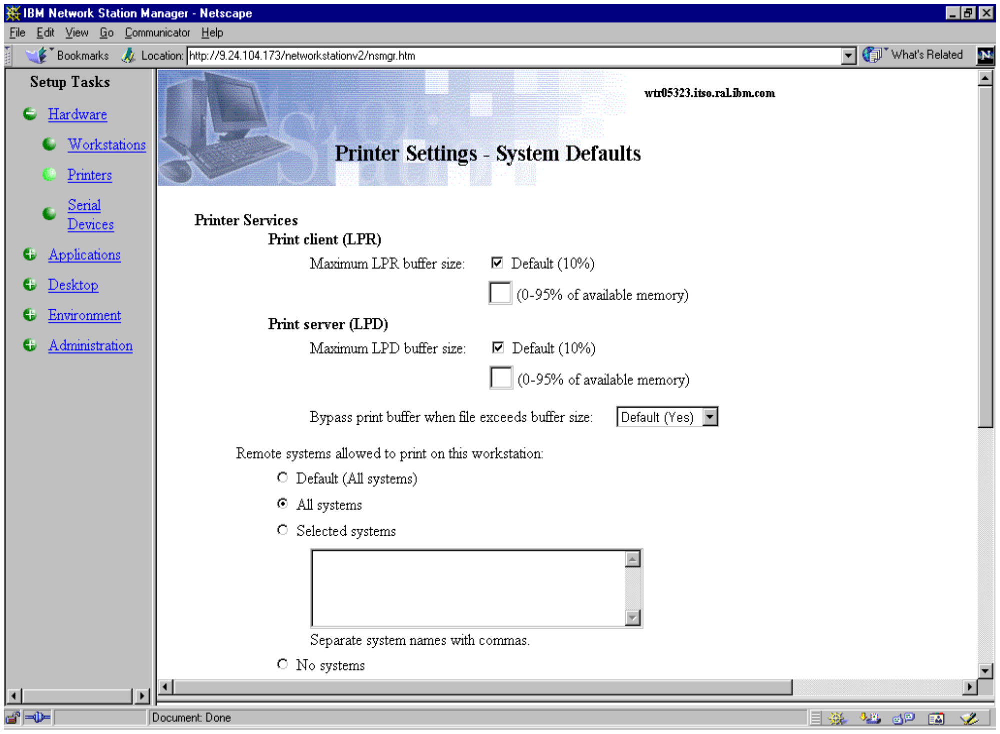
Defining printer settings

To define the local printer using NSM, follow these steps:

1. Set the preference level to system or workstation (MAC address, IP address).
2. Select the **Printers** option under **Hardware**.
3. Modify the Print Services Settings.
4. Define a local printer in the Printer List.

17.4.0.1 Print Services Settings

The first settings on the Printer settings panel deal with the LPR/LPD functions. The settings are shown in Figure 434.


IBM Network Station Manager - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://9.24.104.173/networkstationv2/nsmgr.htm
What's Related
Setup Tasks
Hardware
Workstations
Printers
Serial Devices
Applications
Desktop
Environment
Administration
Document: Done

wtr05323.itso.ral.ibm.com

Printer Settings - System Defaults

Printer Services

Print client (LPR)

Maximum LPR buffer size: ☑ Default (10%)

□ (0-95% of available memory)

Print server (LPD)

Maximum LPD buffer size: ☑ Default (10%)

□ (0-95% of available memory)

Bypass print buffer when file exceeds buffer size: Default (Yes)

Remote systems allowed to print on this workstation:

○ Default (All systems)

● All systems

○ Selected systems

Separate system names with commas.

○ No systems

Figure 434. Print Services settings

Note the following explanation for the fields on the Printer Settings page:

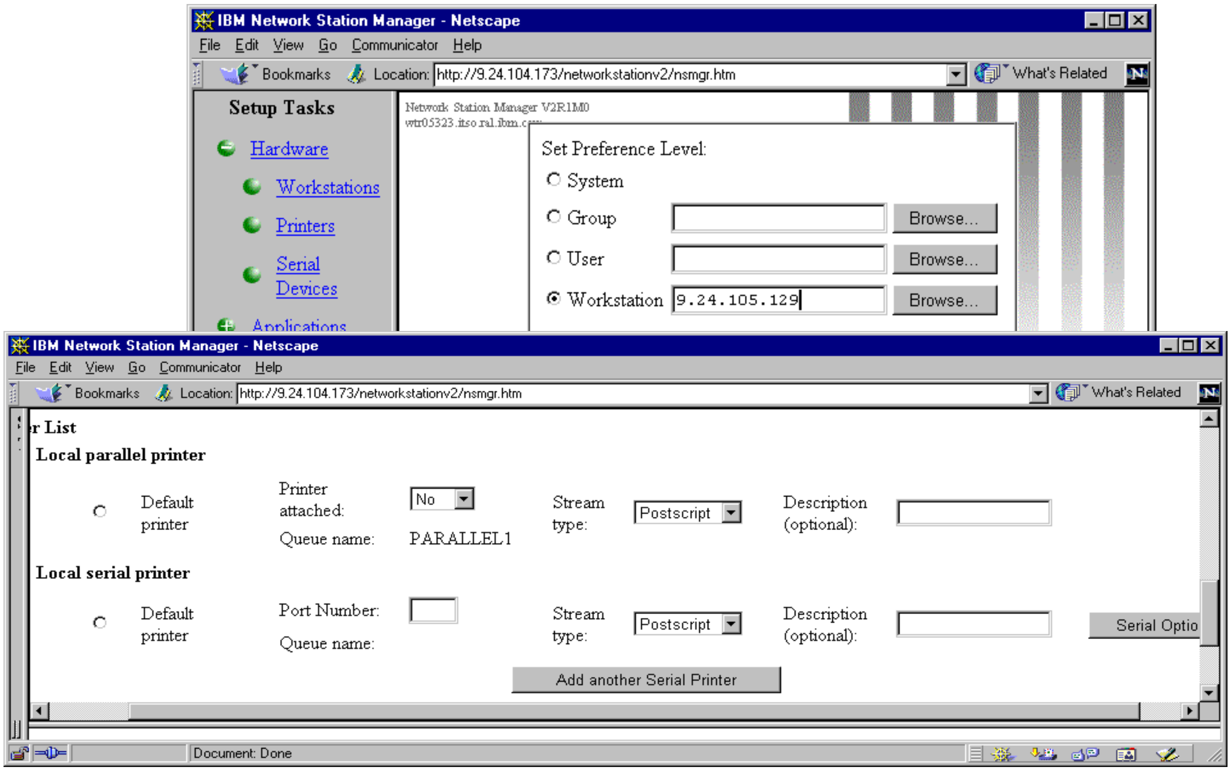
- **Maximum LPR buffer size:** Specifies the maximum size of the LPR buffer used when a print job generated by a local Network Station application needs to be routed to a remote printer. By default, this is set to 10% of the free memory at the time the print job is generated. The size can vary, depending on the size of free memory, but the minimum used will be 5 KB. This size is computed at the beginning of the print job, but is monitored during the processing to make sure the system does not fall too low on storage. If sending output to a nonstreaming host, the size of the buffer is important since the entire print file must be built in the buffer before sending it. If this field is set to 0%, the remote host must support streaming.
- **Maximum LPD buffer size:** Specifies the maximum size of the LPD buffer used when a print job is received from a remote host to be printed on a local printer. By default, this is set to 10% of the free memory at the time the print job is received.

  The LPD daemon has the ability to switch internally to streaming mode when the size of the job exceeds the print buffer. This is true whether the actual protocol used between the remote LPR and the local LPD is using streaming. Whether the LPD daemon does this depends on the Bypass print buffer when the file exceeds the buffer size setting. If set to no, the LPD daemon does not automatically switch to streaming and the job fails if it exceeds the size of the LPD buffer.

- **Remote systems allowed to print to this workstation:** Governs whether remote users can send output to the printer. You can enter a list of systems allowed to use the printer. This list will be used whether the print request comes through LPD or directly through the SERIALD daemon on a specific port.

17.4.0.2 Defining the local printer

Below the Printer Services settings is the Printer List. The first printers to be defined are the local printers, either parallel or serial (Figure 435).



IBM Network Station Manager - Netscape

Location: http://9.24.104.173/networkstationv2/nsmgr.htm

Network Station Manager V2R1M0
wtr05323.itso.ral.ibm.c...

Set Preference Level:
○ System
○ Group
○ User
● Workstation 9.24.105.129

IBM Network Station Manager - Netscape

Location: http://9.24.104.173/networkstationv2/nsmgr.htm

r List

Local parallel printer

○ Default printer — Printer attached: No — Queue name: PARALLEL1 — Stream type: Postscript — Description (optional):

Local serial printer

○ Default printer — Port Number: — Queue name: — Stream type: Postscript — Description (optional):

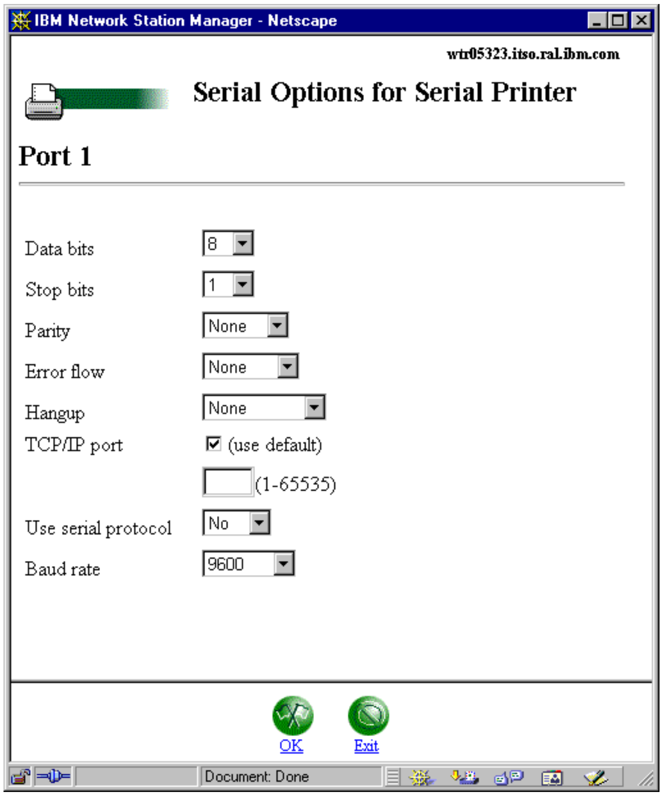
Document: Done

Figure 435. Defining a local printer

The options on this display are explained here:

- **Default printer:** If this printer is set to the default, it will be preselected in the printer selection panel presented to the user.
- **Printer attached:** Select yes to indicate that the printer is a local printer.
- **Queue name:** For a local printer, this will be either PARALLEL1 or SERIALx (where x is the port number) depending on the port to which the printer is connected. The printer queue name will be shown in the printer selection panel seen by the users.
- **Stream type:** Select PostScript, PCL, or ASCII.
- **Description:** This is an optional field that allows you to give a meaningful description for the printer that will show up on the printer selection panel for the users. The Description field has a special meaning if you define the printer definition files to be used with 3270 or 5250 emulation sessions. See 17.9, “Emulation PDT support” on page 569, for more information.

- **Port Number:** For serial printers, this is the number of the physical serial port to which the printer is attached.
- **Serial Options:** A button is available when defining printers on a serial port to specify more options. The panel where these options are defined is shown in Figure 436.


IBM Network Station Manager - Netscape
wtr05323.itso.ral.ibm.com
OK
Exit
Document: Done

Serial Options for Serial Printer

Port 1

Data bits	8
Stop bits	1
Parity	None
Error flow	None
Hangup	None
TCP/IP port	☑ (use default) (1-65535)
Use serial protocol	No
Baud rate	9600

Figure 436. Serial Options

17.5 Printing to the Network Station printer from remote systems

The Network Station uses LPR/LPD so any remote system with LPR capabilities can print to the Network Station printer, including another Network Station (Figure 437 on page 564). For example, you can add the Network Station printer as a remote printer to other Network Stations or as an LPR printer to Windows NT.

In addition, the SERIALD daemon responsible for controlling the serial and parallel interfaces has its own IP ports, which can be accessed directly by remote systems. For new applications, it is preferable to use LPR requests. However, for special needs, SERIALD is available. For details on how to use this special interface, see the *IBM Network Station Printing Guide*, SG24-5212.

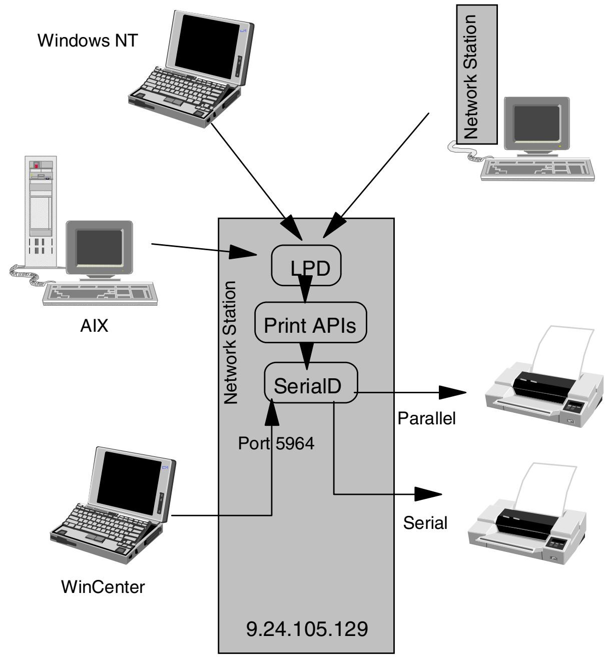


Figure 437. Printing remotely to a Network Station

17.5.1 Setting up the printer on the Network Station

To set up a Network Station printer for use by remote hosts, you first define the printer as a local printer to the Network Station to which it is attached. Actually, the printer will work as a remote printer even if you eliminate this step, but we couldn't think of a reason you would want to do that. This is described in more detail in 17.4, "Printing to a local printer from Network Station applications" on page 560.

In summary, to define the local Network Station printer using NSM, follow these steps:

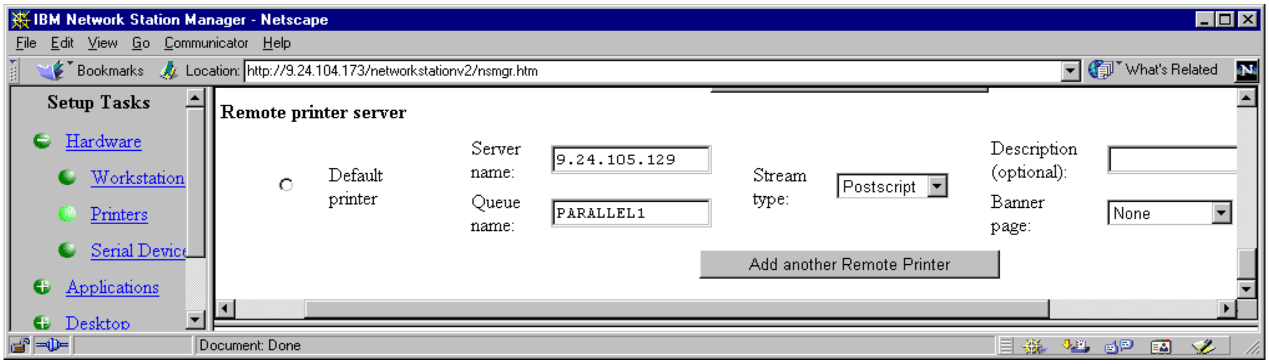
1. Set the preference level to system or workstation.
2. Select the **Printers** option under **Hardware**.
3. Modify the Print Services settings. Make sure remote systems are allowed to print to this printer (see 17.4.0.1, "Print Services Settings" on page 561).
4. Define a local printer in the Printer List (see 17.4.0.2, "Defining the local printer" on page 562).

The next step is to define the printer to the remote hosts.

17.5.1.1 Example: Defining the printer to other Network Stations

If the printer will act as a remote printer for other Network Stations, you need to define the printer as a remote printer using NSM. To do so, follow these steps:

1. Set the preference level to the desired level (for example system or group).
2. Select the **Printers** option under **Hardware**.
3. Modify the Print Services settings if necessary (they may have already been set at another preference level).
4. Define a remote printer in the Printer List (Figure 438).


IBM Network Station Manager - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://9.24.104.173/networkstationv2/nsmgr.htm
What's Related
Setup Tasks
Hardware
Workstation
Printers
Serial Device
Applications
Desktop
Add another Remote Printer
Document: Done

Remote printer server

○ Default printer

Server name: 9.24.105.129

Queue name: PARALLEL1

Stream type: Postscript

Description (optional):

Banner page: None

Figure 438. Defining a remote printer

The printer definitions for a remote printer are the same as for the local printer defined in , “Defining printer settings” on page 560, with a few exceptions:

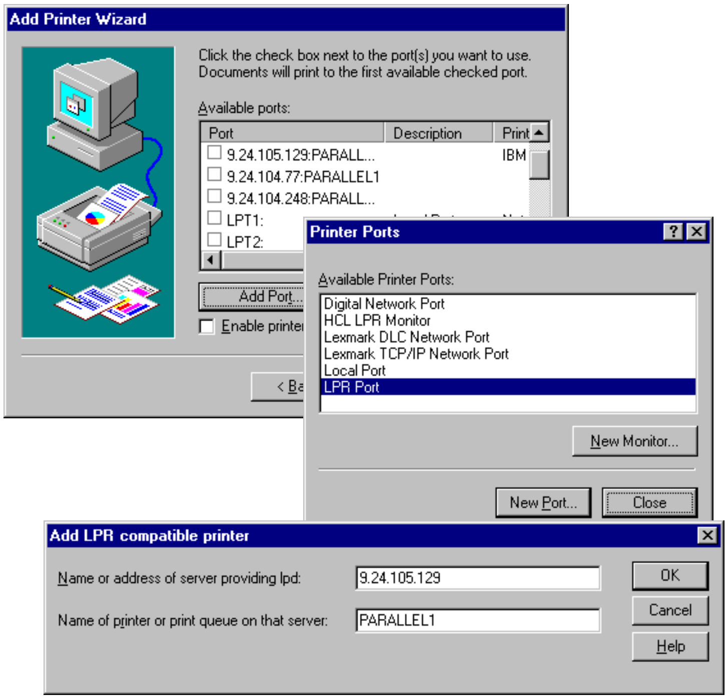
- **Server name:** The TCP/IP address of the remote printer.
- **Queue name:** The queue name, if applicable, for the printer at the remote site. In this case, we define a printer on another Network Station so the choice will be PARALLEL1 or SERIALx. If the printer was on a Windows NT system, this would be the printer name assigned on Windows NT.
- **Banner page:** For remote printers, you can specify whether to print a job separator page.

The printer will now be in the list of available printers for the users at the preference level used when defining the remote printer.

17.5.1.2 Example: Printing to the Network Station from Windows NT

Since the Network Station uses LPD/LPR to handle remote printing, any LPR capable device should be able to send print to the Network Station printer. For example, to use the printer as a remote printer to a Windows NT system, complete these steps:

1. Install Microsoft TCP/IP Printing Services.
2. Add the printer as an LPR printer by selecting **Start->Settings->Printers**.
3. Choose **Add printer**.
4. Select **My computer**, and click **Next**.
5. Click **Add port**. Choose **LPR port**, and click **New port**.
6. Enter the IP address of the network station and the queue name (PARALLEL1). See Figure 439 on page 566.
7. Click **OK->Close->Next**.
8. Follow the rest of the panels to choose the printer type, driver, printer name, and other properties.



Click the check box next to the port(s) you want to use. Documents will print to the first available checked port.

Available ports:

Port	Description	Print
□ 9.24.105.129:PARALL...		IBM
□ 9.24.104.77:PARALLEL1		
□ 9.24.104.248:PARALL...		
□ LPT1:		
□ LPT2:		

Available Printer Ports:

- Digital Network Port
- HCL LPR Monitor
- Lexmark DLC Network Port
- Lexmark TCP/IP Network Port
- Local Port
- LPR Port

Name or address of server providing lpd: 9.24.105.129

Name of printer or print queue on that server: PARALLEL1

Figure 439. Adding the Network Station printer to Windows NT as an LPR printer

17.6 Printing to remote printers from the Network Station

Local applications on the Network Station can send print requests to remote printers. A remote printer is defined as described in 17.5.1.1, “Example: Defining the printer to other Network Stations” on page 564. In that example, the remote printer was a printer on another Network Station, but the remote printer can be any system or printer that supports LPR/LPD.

17.6.1 Example: Printing to a remote IBM 4324

This example illustrates sending print data to a printer defined to a Windows NT system.

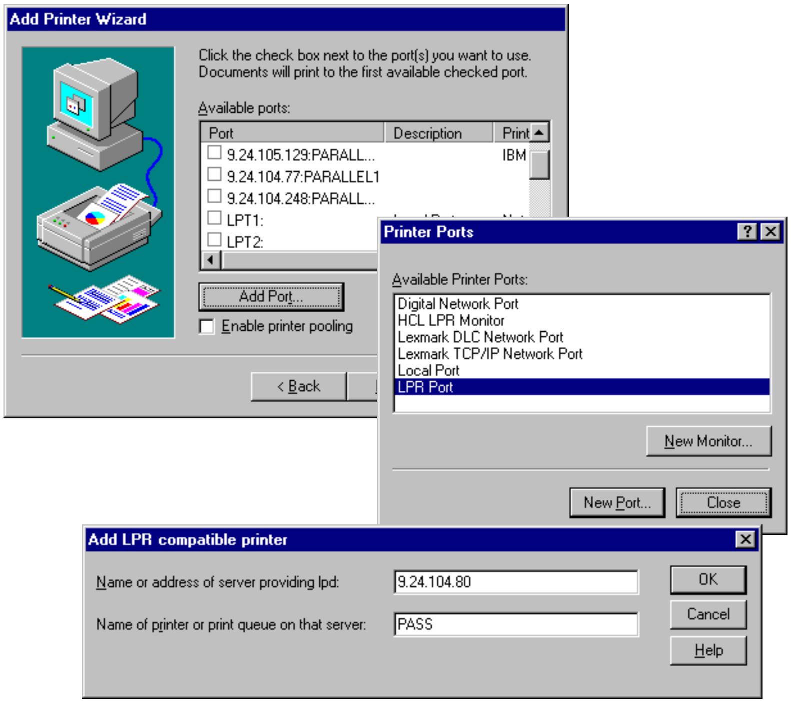
17.6.1.1 Defining the printer to Windows NT

The first step is to set up the printer as an LPR printer using Microsoft TCP/IP printing services on the Windows NT system. This is the same procedure shown in 17.5.1.2, “Example: Printing to the Network Station from Windows NT” on page 565. However, in this case, we define an IBM 4324 printer instead of a printer connected to a Network Station. An example like this, including details of installing the Microsoft TCP/IP Printing Services, is covered in the *IBM Network Station Printing Guide*, SG24-5212.

To define the printer to Windows NT, complete these steps:

1. Install Microsoft TCP/IP Printing Services. Make sure you start the TCP/IP Print Server service from the Control Panel services menu. It is installed for manual operation.
2. To define the printer, follow this path **Start->Settings->Printers->Add printer->My computer->Add port->LPR port**.

3. Enter the IP address of the printer (in this case, the IBM 4324) and the queue name (PASS for the 4324). See Figure 440.



Add Printer Wizard

Click the check box next to the port(s) you want to use. Documents will print to the first available checked port.

Available ports:

Port	Description	Print
□ 9.24.105.129:PARALL...		IBM
□ 9.24.104.77:PARALLEL1		
□ 9.24.104.248:PARALL...		
□ LPT1:		
□ LPT2:		

□ Enable printer pooling

Printer Ports

Available Printer Ports:

Digital Network Port
HCL LPR Monitor
Lexmark DLC Network Port
Lexmark TCP/IP Network Port
Local Port
LPR Port

Add LPR compatible printer

Name or address of server providing lpd: 9.24.104.80

Name of printer or print queue on that server: PASS

Figure 440. Adding IBM 4324 to the Windows NT server

We added a printer called TCP4324 to the Windows NT. The name was chosen at random and modified by clicking on the default name under the icon in Figure 441. The printer is now available for use by the Windows NT user and remote users.

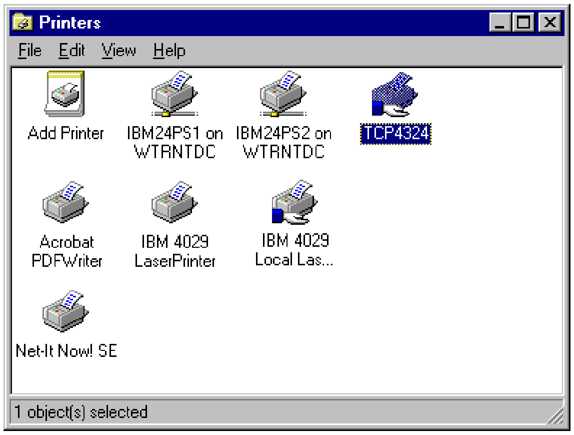
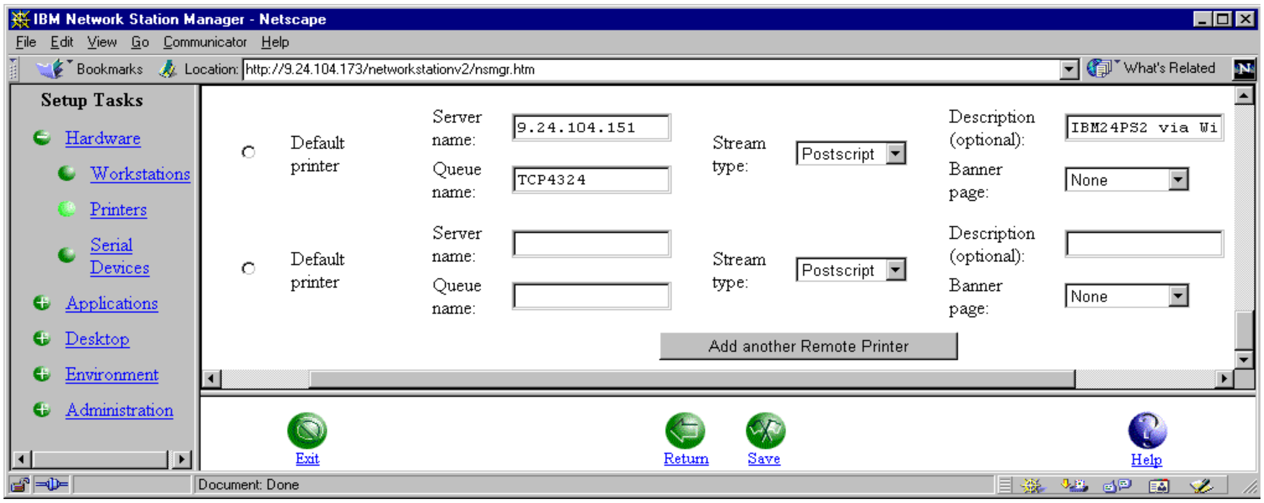


Figure 441. Windows NT printers

17.6.1.2 Defining the printer to the Network Station users

The next task is to define this printer as a remote printer for Network Station users. Using NSM, set the appropriate preference level and select **Printers** under the **Hardware** category. See Figure 442 on page 568.



Location: http://9.24.104.173/networkstationv2/nsmgr.htm

○ Default printer
Server name: 9.24.104.151
Queue name: TCP4324
Stream type: Postscript
Description (optional): IBM24PS2 via Wi
Banner page: None

○ Default printer
Server name:
Queue name:
Stream type: Postscript
Description (optional):
Banner page: None

Document: Done

Figure 442. Defining the remote printer to NSM

The IP address is the address of the Windows NT system. The queue name is the printer name (TCP4324) defined earlier in Windows NT.

The new printer will show up in the printer selection panels for users at the preference level to which the printer was defined. Selecting the printer sends the output to the Windows NT system, which has spooling capabilities. This is an advantage it the printer is backed up or temporarily out of service.

17.7 The lpr command

The `lpr` command is available from the diagnostic window on the Network Station. The format is:

```
lpr [-Pprinter] [-Kcopies] [-Ttitle] [-h] [-Uuser][-v] filename
```

Note the following points:

- `printer`: IPaddress:queuename
- `-h`: Suppress the printing of the burst page
- `-U`: User name to print on the burst page, also for accounting purposes. This option is only honored if the real user ID is daemon (or that specified in the printcap file instead of daemon), and is intended for those cases where print filters want to requeue jobs.
- `-v`: The files are assumed to contain a raster image for such devices as the Benson Varian.

Consider the following example to print the /etc/hosts file to the printer defined above:

```
lpr -P9.24.104.151:TCP4324 /etc/hosts
```

17.8 LU printing

The IBM Network Station supports host-directed print. This requires a 3270 emulation session and TN3270E support at the communications server or gateway. Printer sessions do not work with TN3270. Both LU1 and LU3 support are available:

- **LU Type 1**: This has an SNA Character String (SCS) data stream, which contains a series of characters, formatting commands, and attributes that can be translated from EBCDIC to ASCII and sent immediately to the printer.
- **LU Type 3**: This has a data stream that is similar to the data stream of a display. It is formatted by the host in a buffer, then sent to the printer.

An example of LU printing can be found in 17.8, “LU printing” on page 568.

17.9 Emulation PDT support

Support for Printer Definition Files (PDFs) and a Printer Definition Table (PDT) is provided for 3270 and 5250 emulator sessions on the Network Station Manager V2R1. The PDT basically acts as an index to PDFs that format print for a particular type of printer.

A PDF is a file that is used to format the datastream sent by the host application. The emulator converts the datastream from EBCDIC to ASCII (unless there is a passthru command in the datastream), formats the data according to controls specified in the datastream or in the PDF itself and sends the data to the printer. You can use a simple PDF that contains basic instructions. However, if you want to use some of the newer functions available in modern workstation printers, such as the ability to change fonts or paper drawers, the PDF may need to be customized for your printer (and the host application must send the necessary commands). You must use a PDF that is suitable for the emulation mode that the printer supports (HPPCL Level 3, IBM PPDS, and so on).

PDFs, using the correct printer language, support the basic functions of your printer. They can be modified by a user to use special features. You do not need a PDF for each different printer model. With the increasing number of models, manufactures will supply PDFs named for the printer language, not the printer mode.

Users will not usually require a PDT for emulator screen print. Emulator screen print can be done to any printer configured within IBM Network Station Manager (NSM). TN3270E host print is somewhat more likely to require tuning from a PDT.

For TN3270E host print, the target printer must be configured in NSM, the same as the emulator screen print. Also, a printer session must be configured on the 3270 startup line. NSM Startup Programs or Startup Menus, -PRINTER_GENERAL or -PRINTER_APP, are required).

If a PDT is going to be used, -PDT must also be entered into the same 3270 startup line as -PRINTER_GENERAL or -PRINTER_APP. -PDT does not have a parameter that follows it. -PRINTER_GENERAL and -PRINTER_APP have a parameter.

NSM does not provide PDF files or the PDT. If desired, they must be created or copied from another product. For example, IBMs Personal Communications (PCOMM) and Host On-Demand both have PDF files.

To use a PDF file, follow these steps:

1. Place the desired PDF source file (or files) in the "NSM_ADMIN_SYSDEFAULTS"/NS3270/PDT directory (the /PDT subdirectory may need to be created).
2. Create a PDT table and store it in the same directory as the PDF file. The PDT table file name must be PDT.819.

   The PDT.819 file must contain the following data:

   ```
   "Printer_desc" PDF_file_name *all
   ```

   There can be multiple lines in the PDT.819 file, if the PDF is to apply to multiple printer descriptions or multiple PDFs are required to multiple printers.

   "Printer_desc" is case sensitive and must be within double quotes. "Printer_desc" should exactly match the text entered into NSM Hardware/Printers in the Description (optional) entry field.

   PDF_file_name is the name of your PDF file.

   *all indicates that any user with a -PDT startup line should use the PDF when printing to the specified printer. If necessary, *all can be replaced by a user ID or user IDs that should use the PDF.

Then, when a 3270 print is done, if -PDT is specified in the 3270 Launch Bar settings in the Other Parameters field, the PDT.819 file is read. If a "Printer_desc" line in the file matches the printer to be used for the 3270 print, then the PDF file is read and used.

Note: The 5250 emulator reads PDTs from the 3270 directory, because the 3270 emulator is more likely to require use of a PDT than the 5250 emulator (because of TN3270E print).

17.10 TN3270E LU1/LU3 printing

TN3270 is a client/server protocol to support 3270 sessions across TCP/IP networks. The client function runs on TCP/IP (Telnet) client machines and the server function may run on workstations, network controllers, or System/390 hosts. If the server runs on a workstation or controller, it interfaces with System/390 hosts through the SNA network, which can also be overlaid on TCP/IP networks through Enterprise Extender or Data Link Switch.

The TN3270 basic function supports only 3270 workstations (LU2). The TN3270E function, an extension of TN3270, also supports 3270 printers (LU1 and LU3), thus offering complete support for SNA 3270 applications on an IP transport network.

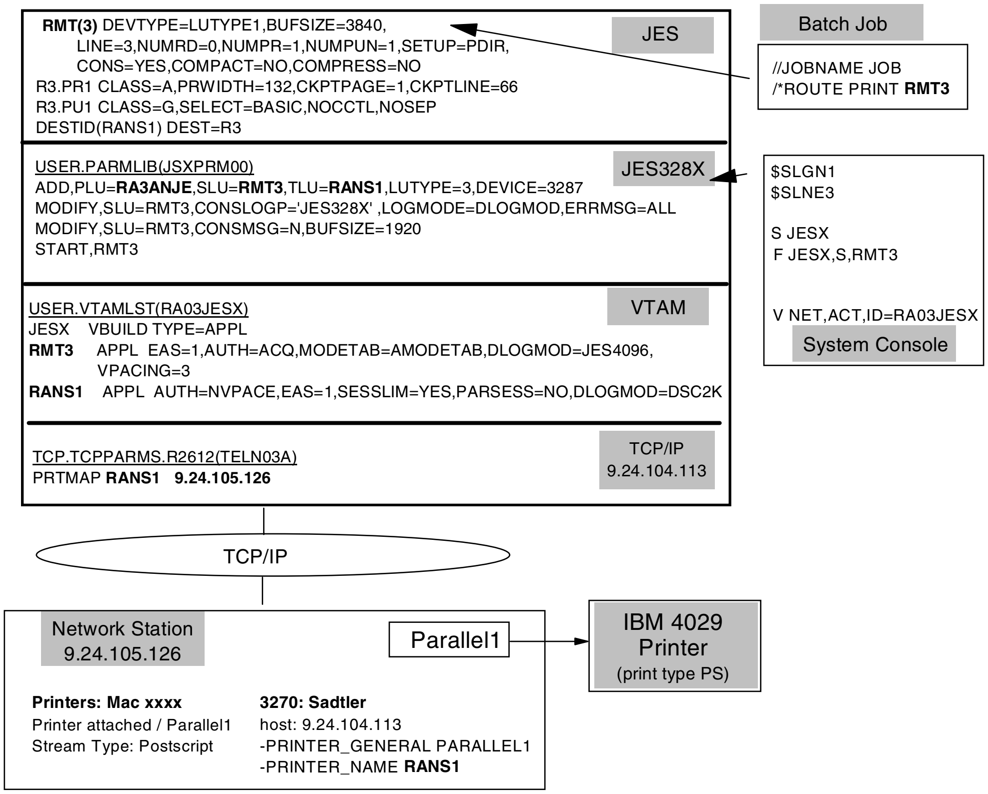
From the point of the TN3270E client, it is not always possible or easy to know device-names available on the network. The TN3270E server should assign the proper device to the client. This is accomplished by using a device pool that is defined on the TN3270E server. Basically, these device pools contain SNA network devices such as terminals and printers. In other words, the TN3270E implementation maps TN3270 sessions to specific SNA logical unit (LU) names, effectively turning them into SNA devices. The device pool not only defines SNA network devices, but also provides some other important functions for a TN3270E session. Some of these are:

- It is possible to assign one or more printers to a specific terminal device.
- It is possible to assign a group of devices to a specific organization.
- A pool can be defined that has access to only certain types of applications on the host.

TN3270E print example

This scenario is an example of LU1/LU3 printing to the Network Station. It shows printing to a 4029 connected to a Network Station. The host printing program was JES328X. The TN Server is TCP/IP 390.

With LU1/LU3 printing, the host node directs print output to an SNA LU, represented by a TN3270E server. The TN3270E server forwards the print output to the appropriate TCP/IP address (Figure 443).



```
 RMT(3) DEVTYPE=LUTYPE1,BUFSIZE=3840,
      LINE=3,NUMRD=0,NUMPR=1,NUMPUN=1,SETUP=PDIR,
      CONS=YES,COMPACT=NO,COMPRESS=NO
R3.PR1 CLASS=A,PRWIDTH=132,CKPTPAGE=1,CKPTLINE=66
R3.PU1 CLASS=G,SELECT=BASIC,NOCCTL,NOSEP
DESTID(RANS1) DEST=R3
```

```
USER.PARMLIB(JSXPRM00)
ADD,PLU=RA3ANJE,SLU=RMT3,TLU=RANS1,LUTYPE=3,DEVICE=3287
MODIFY,SLU=RMT3,CONSLOGP='JES328X' ,LOGMODE=DLOGMOD,ERRMSG=ALL
MODIFY,SLU=RMT3,CONSMSG=N,BUFSIZE=1920
START,RMT3
```

```
USER.VTAMLST(RA03JESX)
JESX    VBUILD TYPE=APPL
RMT3     APPL  EAS=1,AUTH=ACQ,MODETAB=AMODETAB,DLOGMOD=JES4096,
               VPACING=3
RANS1    APPL  AUTH=NVPACE,EAS=1,SESSLIM=YES,PARSESS=NO,DLOGMOD=DSC2K
```

```
TCP.TCPPARMS.R2612(TELN03A)
PRTMAP RANS1   9.24.105.126
```

```
//JOBNAME JOB
/*ROUTE PRINT RMT3
```

```
$SLGN1
$SLNE3

S JESX
 F JESX,S,RMT3


V NET,ACT,ID=RA03JESX
```

```
Printers: Mac xxxx              3270: Sadtler
Printer attached / Parallel1    host: 9.24.104.113
Stream Type: Postscript         -PRINTER_GENERAL PARALLEL1
                                -PRINTER_NAME RANS1
```

Figure 443. TN3270 printing

We do not cover the specific host printing implementation. The programs and configurations we used can be seen in Figure 443. They show the relationship of the JES and SNA parameters required to establish the printing connection to the printer on the Network Station. Depending on the host type, communications server you use (we used VTAM, but you can use any TN3270E server), and the print programs involved, the setup will be different. However, the same basic relationships must always exist.

To configure this scenario, complete these steps:

1. Define the printer to MVS JES. We defined the printer as RMT3 to JES.

2. Define the printer to JES328X. JES328X provides the interface between JES and VTAM and defines the relationship between the JES printer definition (RMT3) and the VTAM LU (RANS1).

3. Define the LUs to VTAM. JES328X requires an LU definition for both the JES printer (RMT3) and the VTAM printer (RANS1).

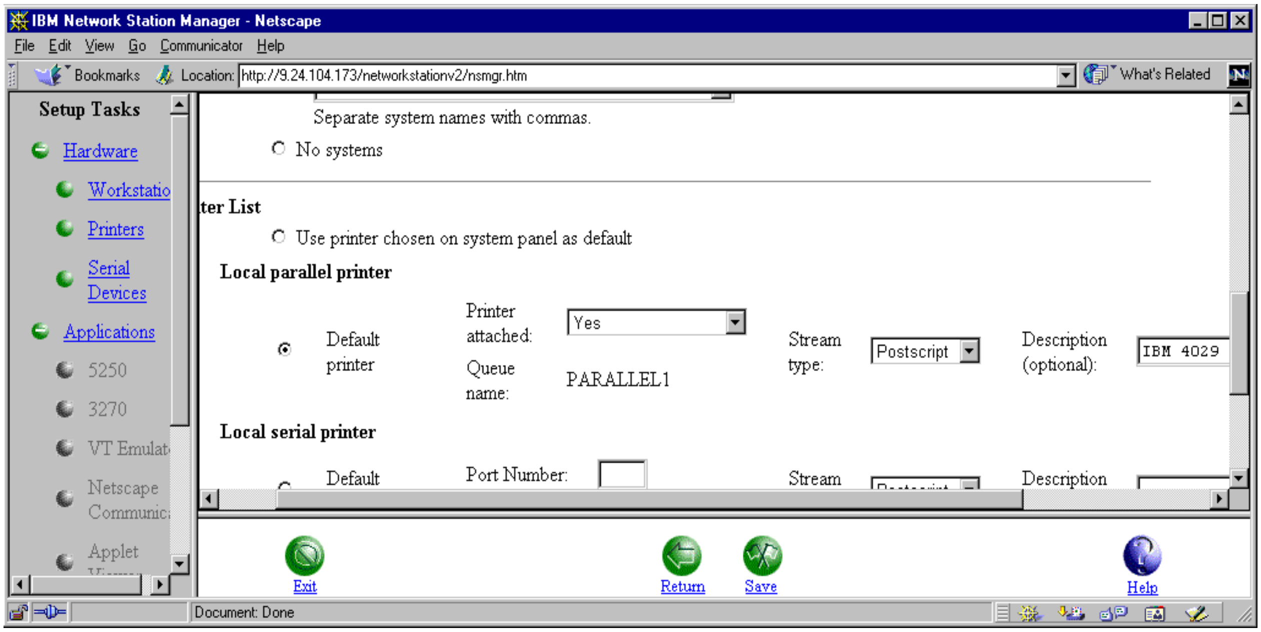
4. Update OS/390 TCP/IP Telnet parameters to map the LU name (RANS1) to the IP address of the Network Station.

5. Use NSM to define a local printer to the Network Station (Figure 444):

   a. Select the Network Station with the printer by setting the preference level at the workstation level.

   b. Click on **Printers** under the Hardware category.

   c. Define the local printer.



Location: http://9.24.104.173/networkstationv2/nsmgr.htm

Separate system names with commas.

○ No systems

ter List

○ Use printer chosen on system panel as default

Local parallel printer

● Default printer	Printer attached: Yes Queue name: PARALLEL1	Stream type: Postscript	Description (optional): IBM 4029

Local serial printer

○ Default   Port Number: Stream   Description

Figure 444. Defining the local printer

6. Use NSM to add the printer parameters to the 3270 session. To define the printer for LU1/LU3 printing, you must tell the TN3270 session which host LU to request and which printer to use. Select the preference setting (user, group, or system), and click **Launch Bar** under the Desktop category.

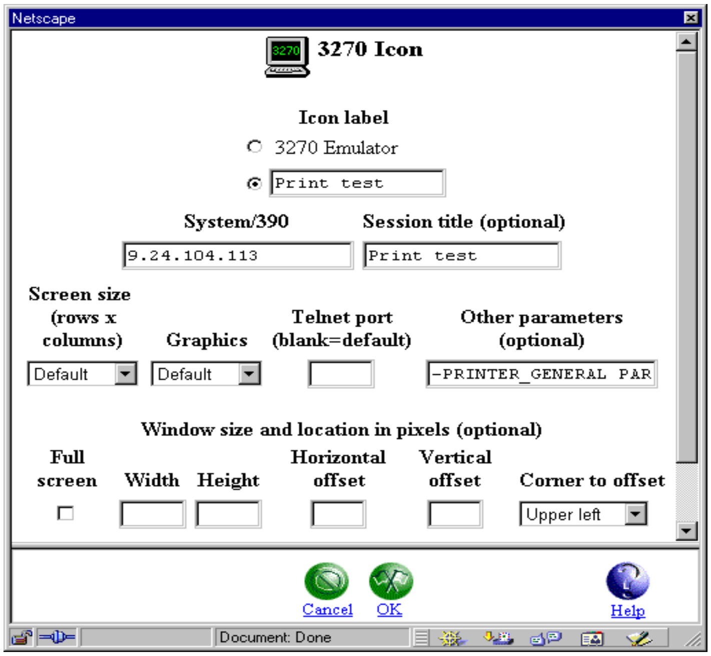
   In our example, the LU name reserved at the host for this printer is RANS1. The printer is local to the Network Station on the PARALLEL1 queue.

   The following parameter needs to be entered in the Other Parameters field as shown in Figure 445:

   ```
   -PRINTER_GENERAL PARALLEL1 -PRINTER_NAME RANS1
   ```

7. Start the TN3270 session on the Network Station. This establishes the TN3270E connection necessary for the LU1/LU3 print to work. The LU must be active (reachable) at the host.

The printout on the host destined for the JES2 RMT3 printer will now be sent to the Network Station printer.



3270 Icon

Icon label

○ 3270 Emulator

● Print test

System/390: 9.24.104.113

Session title (optional): Print test

Screen size (rows x columns)	Graphics	Telnet port (blank=default)	Other parameters (optional)
Default	Default		-PRINTER_GENERAL PAR

Window size and location in pixels (optional)

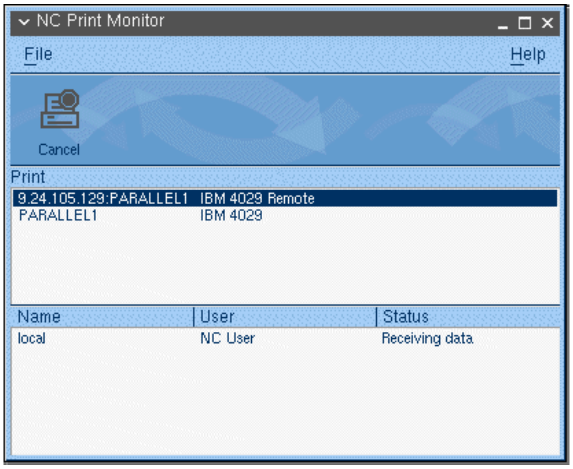
Full screen	Width	Height	Horizontal offset	Vertical offset	Corner to offset
□					Upper left

Document: Done

Figure 445. Updating the 3270 parameters for LU1/3 printing

17.11 Print monitor

NSM V2R1 introduced a print monitor, available to Network Station users. The print monitor is normally located in the Tool Kit icon. The print monitor (Figure 446) shows each printer defined to the Network station (local and remote) and the status of the jobs on each printer queue.



Print

9.24.105.129:PARALLEL1	IBM 4029 Remote
PARALLEL1	IBM 4029

Name	User	Status
local	NC User	Receiving data

Figure 446. Print Monitor

The print data stream can be seen on the print monitor briefly (only while being sent to the printer). Once it has been sent to the printer, it disappears.

Chapter 18. Problem determination hints and tips

This chapter offer hints and tips to the Network Station Manager administrator for resolving problems that correspond to the NSM V2R1 software. The latest version of the NSM has definitely moved to the UNIX world. The problem determination tools also are closely related to it. Administrators who are familiar with UNIX terminology and commands may find this chapter less useful. However, for those administrators who have just begun their adventure with Network Station hardware and software, in our opinion, you will find it helpful.

18.1 Telnet into the Network Station

The telnetd daemon (nctelnetd) is automatically started from the .profile file (in the $ProdBase/x86|ppc subdirectory), which seems to be the first file processed by the kernel. The kernel loads it from the directory $NC_CLIENT_BASE/bin/nctelnetd, where $NC_CLIENT_BASE, by default, points to /usr/local/nc.

Note

You can Telnet into the Network Station even if nobody is logged on at that time.

18.1.1 Security and authentication

When you Telnet into the Network Station, you are prompted for a user ID and password. If there is a *unit-global password* (it means administrator password), there will be no prompt for User ID, just a prompt for a password. In this case, the password is verified, and if typed correctly, you get access to a command prompt. In other cases, the user ID/password pair is checked at the authentication server by means of the Remote Authentication Protocol (RAP) protocol.

Important

The authentication server mentioned refers to the server specified in either the NVRAM setting for the authentication server, the server specified in DHCP option 98, or the one you can find under the NC_AUTH_URL environment variable (to be more precise what this environment variable contained just before starting the Telnet daemon).

What does this mean? It means that roaming is not taking into account, since the user can roam practically to any server in the world.

The auth file is responsible for determining who will be granted access to the Network Station using Telnet. It is located in the /usr/local/nc/boot/login/ directory and is shipped with just three values:

```
remote_shell_allow=qsecofr,root,administrator
```

You can add or remove values from the list, or if you want to open it for everybody, set it to (not recommended):

```
remote_shell_allow=all
```

Note

Remember that being on the `remote_shell_allow` list is a required condition but not sufficient. You still must be authenticated using the RAP protocol at the authentication server.

After a successful login, you are presented a command prompt. At this point, certain commands are restricted. To get full access as if using the advanced diagnostic session on the station itself, comment out from the .profile the RPATH statement that reads RPATH=/usr/diag.

There is also a second way to get access to the rest of the programs. The administrator can copy required programs into the /usr/diag directory. This way the administrator can control what commands will be available for a Telnet user.

The problem with this solution is that these applications cannot be directly PTFed. That is, when fixes become available from IBM or other parties, these copied binaries will not automatically be updated. For Windows NT, they always must be copied over by the administrator just to avoid having two copies of the same program at two different levels. On AIX and OS/400, it is easier, since these operating systems support hard links. Hard links are like symbolic links, only that they point directly to the file. Using hard links allows the programs to be PTFed and what is in /usr/diag automatically always has the latest version.

Note

Always remember to apply the above information in both the x86 and ppc directories.

More importantly for users of the OS/400 version of the NSM V2R1, certain tools need special permission set on them, independently where they will be used in Advanced Diagnostic window or Telnet session. To do that, you must log on at the Network Station as a QSECOFR and run only *once* the `as400auth` program. Without running it, only QSECOFR has the right authority to run them.

18.1.2 Starting applications

Once you have run Telnet from your workstation, you can execute line commands. To start any available X11 client application on the network computer, you need to export the display to your computer (or to any other accessible X server, including the network computer):

```
export DISPLAY=ipaddressofXserver:0
```

Or, submit the display parameter each time, for example:

```
ncedit -display ipaddressofXserver:0
```

If coming from a Windows NT or OS/2 system, you need a program like Exceed from Hummingbird to allow the commands to work.

18.2 Advanced Diagnostics window

NSM V2R1 has a built-in diagnostic window. This window provides a direct interface with the Network Station operating system by providing a UNIX-type interface. Many UNIX commands such as `ls` (list the directory), `ps` (show tasks) and others, such as `ping`, `traceroute`, for example, are available. You can also specify Network Station hardware and software-related commands such as `ncregget`.

The Advanced Diagnostic window is nothing more than classical xterm window, running a shell program. This allows the users to run any available program.

To start it, log on to your Network Station. Open **Tool Kit -> Advanced Diagnostics**. You get a UNIX prompt. For your information, the command hidden under Advanced Diagnostics icon is as follows:

```
nsm_wrapper xterm -sb -sl 1000 -rv -name Advanced_Diagnostics
```

Here, `nsm_wrapper` is a shell script that performs environment variable substitution for applications (not needed in this case, but its nature is generic so you can always use it).

Usability features include:

- A scroll bar to the left of the window, allowing you to move back and forth through the console commands and output. Press the left and right mouse buttons down simultaneously and drag the bar up or down (the `-sl 1000` parameter tells that you can scroll through the last 1000 lines).
- Ctrl + right mouse button shows a font menu.
- Ctrl + left mouse button show an menu of options.
- Type the command `set -o emacs` to use the arrow up and down buttons to scroll through the last issued commands.

Many UNIX commands work in the Advanced Diagnostics screen. Appendix C, “UNIX commands” on page 613, has a list of many of the commands available.

The UNIX interface can also be used to start applications, usually for debugging and programming purposes. A list of the native application commands can be found in Appendix B, “Native application commands” on page 611.

18.2.1 System messages

One of the most important programs for resolving problems concerned with Network Station is `dmesg`. This program is only the user interface for the background working daemon called `syslogd`. It is located in the /usr/sbin/syslogd directory and is started during the execution of the .profile file.

To see the Network Station system messages, enter the following command:

```
dmesg
```

Tip

If you want to capture output from a command, use:

```
command > ~/filename
```

This pipes the output into a file called filename on your home drive (tilde “~” in UNIX is an alias for your home drive).

For example, the server is a Windows NT system, and you enter:

```
dmesg > ~/debugmsg
```

The output of the `dmesg` command (Network Station messages) is put into the \NetworkStationV2\userbase\home\<user name>\debugmsg file.

You should also know that you have access to only the last 100 messages. We tested that during normal startup process when everything was working fine. The syslogd daemon recorded more than 100 messages. To get all of them we had to capture them twice: once before login and once after login (before login, we did it by Telneting to the Network Station). You can see all messages logged after turning on the Network Station in the following sections.

From the beginning of running syslogd ...

```
NetBSD 1.3I-NCOS (CLIENT.HON) #0: Mon Aug 30 23:56:01 MDT 1999
buildmaster@buildi3862:/buildmaster/modules/NCOS/build-history/build-3.0.bet
a-199908301842/NCOS/os-src/sys/arch/i386/compile/CLIENT.HON
cpu0: family 5 model 8 step 1
cpu0: Intel Pentium (586-class)
real mem  = 66715648
avail mem = 63627264
using 96 buffers containing 393216 bytes of memory
mainbus0 (root)
pci0 at mainbus0 bus 0: configuration mode 1
pci0: i/o enabled, memory enabled
pchb0 at pci0 dev 0 function 0
pchb0: vendor 0x8086 product 0x7100 (rev. 0x01)
pcib0 at pci0 dev 5 function 0
pcib0: vendor 0x8086 product 0x7110 (rev. 0x02)
vendor 0x8086 product 0x7111 (IDE mass storage, interface 0x80, revision 0x01) a
t pci0 dev 5 function 1 not configured
vendor 0x8086 product 0x7112 (USB serial bus, revision 0x01) at pci0 dev 5 funct
ion 2 not configured
smbus0 at pci0 dev 5 function 3
smbus0: vendor 0x8086 product 0x7113 (rev. 0x02)
smbeeprom0 at smbus0 addr 0xa4 esize 4Kbits
nvram0 at smbeeprom0
 IBM PCI tokenring card detected  (DD = 1.1d )
tcs0 at pci0 dev 2 function 0: IBM PCI Tokenring Card
tcs0: Tokenring address 00:20:35:5f:20:0f
tcs0: new mtu 0x1493
vgafb0 at pci0 dev 1 function 0: 1024 x 768, 8bpp
wsdisplay0 at vgafb0: console (std, vt100 emulation)
isa0 at pcib0
com0 at isa0 port 0x3f8-0x3ff irq 4: ns16550a, working fifo
com1 at isa0 port 0x2f8-0x2ff irq 3: ns16550a, working fifo
lpt0 at isa0 port 0x278-0x27b irq 7
pckbc0 at isa0 port 0x60-0x64
pckbd0 at pckbc0 (kbd slot)
pckbc0: using irq 1 for kbd slot
wskbd0 at pckbd0: console keyboard
psm0 at pckbc0 (aux slot)
pckbc0: using irq 12 for aux slot
wsmouse0 at psm0
wslpn0 at psm0
pcppi0 at isa0 port 0x61
sysbeep0 at pcppi0
isapnp0 at isa0 port 0x279: ISA Plug 'n Play device support
```

```
npx0 at isa0 port 0xf0-0xff: using exception 16
isapnp0: read port 0x203
wss0 at isapnp0 port 0x534/4,0x388/4,0x220/16 irq 5 drq 1,0
wss0: Crystal Codec WSS/SB: CS4236/CS4236B
audio0 at wss0
isapnp0: <Crystal Codec, CSC0001, , GAME> port 0x200/8 not configured
isapnp0: <Crystal Codec, CSC0010, , CTRL> port 0x120/8 not configured
isapnp0: <Crystal Codec, CSC0003, , MPU> port 0x330/2 irq 9 not configured
biomask 0 netmask 800 ttymask 1882
RFS root not mounted. errno=53 (9.5.92.58:/NetworkStationV2/prodbase/x86)
tcs0: SIOCSIFFLAGS bringing interface down.
nfs server 9.5.92.58:/NetworkStationV2/prodbase/x86: not responding
nfs server 9.5.92.58:/NetworkStationV2/prodbase/x86: is alive again
root on 9.5.92.58:/NetworkStationV2/prodbase/x86
WARNING: CHECK AND RESET THE DATE!
root file system type: nfs
Sep 29 15:31:09 actlogin: nc/actlogin started; build timestamp: Aug 28 1999 07:5
3:40
Sep 29 15:31:09 actlogin: Environment Variable FFDC is not defined.
Sep 29 15:31:09 actlogin: Current Working Directory is /
Sep 29 15:31:09 actlogin: LC_ALL = en_US
Sep 29 15:31:10 actlogin: Using LANG : /nls/en_US/Login
```

... To the moment when a user logs on, and from the moment of login ...

```
Sep 29 15:33:18 actlogind: nc/actlogind started; build timestamp: Aug 28 1999 07
:54:01
Sep 29 15:33:18 actlogind: LC_ALL = en_US
Sep 29 15:33:18 actlogind: mounting [HOME]
Sep 29 15:33:18 actlogind: mountfilesystem(): MOUNT_TCP_NFS
nfs server 9.5.92.58:/networkstationv2/userbase/home: not responding
nfs server 9.5.92.58:/networkstationv2/userbase/home: is alive again
Sep 29 15:33:18 actlogind: mounting [PROFILES]
Sep 29 15:33:18 actlogind: mountfilesystem(): MOUNT_TCP_NFS
Sep 29 15:33:18 actlogind: Load "/userbase/profiles/allusers.nsm" succeeded.
Sep 29 15:33:18 actlogind: Do not load allusers.ovr.
Sep 29 15:33:18 actlogind: Load "/userbase/profiles/groups/NSMUser.nsm" failed.
 Status = 1
Sep 29 15:33:18 actlogind: Do not load group override xml file.
Sep 29 15:33:18 actlogind: Load "/userbase/profiles/users/Administrator.nsm" suc
ceeded.
Sep 29 15:33:18 actlogind: Do not load user override xml file.
Sep 29 15:33:18 actlogind: SET TRACE = ON
Sep 29 15:33:18 actlogind: SET CLASSPATH = /usr/local/java/J118/lib/classes.zip:
.
Sep 29 15:33:18 actlogind: SET NPX_PLUGIN_PATH = /usr/local/java/J118/plugins/:/
usr/local/netscape/plugins/
Sep 29 15:33:18 actlogind: SET BOOTHOST = 9.5.92.58
Sep 29 15:33:18 actlogind: SET NSM_NAV_PREF_VERSION = V2R1M0
Sep 29 15:33:18 actlogind: SET NSM_NS3270_PREF_VERSION = V2R1M0
Sep 29 15:33:18 actlogind: SET NSM_NS5250_PREF_VERSION = V2R1M0
Sep 29 15:33:18 actlogind: SET NSM_NSTERM_PREF_VERSION = V2R1M0
Sep 29 15:33:18 actlogind: SET PRODUCT_TYPE = IBM
Sep 29 15:33:18 actlogind: SET NSM_HTTP_PORT = 80
Sep 29 15:33:18 actlogind: PREF nsm-numlock false
Sep 29 15:33:18 actlogind: SET NSM_HTTP_PORT = 80
Sep 29 15:33:18 actlogind: SET TRACE = ON
Sep 29 15:33:18 actlogind: SET RUNWM = YES
Sep 29 15:33:18 actlogind: NumLock should be turned OFF.
Sep 29 15:33:18 actlogind: Received SIGCHLD signal (20).
Sep 29 15:33:18 actlogind: LC_ALL = en_US
Sep 29 15:33:18 actlogind: Setting MRIPATH=/nls/en_US
Sep 29 15:33:18 actlogind: Setting NLSPATH=/nls/en_US/%N
Sep 29 15:33:19 actlogind: Load "/nls/en_US/desktop.mri" succeeded.
Sep 29 15:33:19 actlogind: Execute command = "/usr/bin/startwm" 50 -> 64
Sep 29 15:33:26 ns5250: [ INFORMATIONAL ]: Build Date: Aug 16 1999.
Sep 29 15:33:26 ns5250: [ INFORMATIONAL ]: Build Date: Aug 16 1999.
Sep 29 15:33:26 actlogind: NS Manager says mount NSM_MOUNT.
Sep 29 15:33:26 actlogind: Mounting NSMShared
Sep 29 15:33:26 actlogind: mountfilesystem(): MOUNT_TCP_NFS
Sep 29 15:33:27 actlogind: Received SIGCHLD signal (20).
```

...To the moment when the desktop is displayed for the end user

If you do the same, you should obtain very similar results. Keep in mind that we included this printout to show you what kind of information is recorded during startup. Do not expect that all lines will be the same.

18.2.2 Starting applications from the command prompt

The main purpose of the Advanced Diagnostic window is to give to the end user the ability to start all of the network computer applications manually. It is also possible to perform it from a Telnet session, but there are registry limitations (see 18.9, “Investigating the NC Registry” on page 600). Remember that the network computer’s applications read most of their settings from the registry. The second limitation of a Telnet connection is if your station is not an X Server, you cannot redirect the display to your monitor. The difference between starting applications manually and from an icon is that doing so manually, you can submit any supported option and see the output messages on the screen or capture them to the log file.

Here are examples of manually started programs:

- **5250 Emulation**

  ```
  ns5250 192.168.0.1 -debug -options > ~/5250.log &
  nsm_wrapper ns5250 ${SALES_AS400) -debug -options > ${HOME}/5250-1.log &
  ```

- **3270 Emulation**

  ```
  ns3270 192.168.0.1 -debug -options > ~/3270.log &
  nsm_wrapper ns3270 ${SALES_S390} -debug -options > ${HOME}/3270-1.log &
  ```

- **Java**

  ```
  java -verbose -classpath $CLASSPATH$:. -options  MyApplication &
  ```

  Note: See also Chapter 11., “Java environment” on page 305.

- **Netscape**

  ```
  netscape -options  -java_args -classpath ... -verbose -verbosegc ... &
  ```

Here, *-options* are all allowed parameters for given application.

18.3 Remote reboot

There are two ways to reboot the network computer remotely by means of software command.

The first method uses a program called `reboot`, which is installed by default with the Network Station Manager V2R1. To cause a remote reboot, you must Telnet (or use Advanced Diagnostic window if you work locally) to the network computer. Then, at the command prompt line, type:

```
reboot
```

The Telneted network computer reboots immediately with no regards whether somebody was logged on it. In this moment, you lose your TCP/IP connection. However, after a while when the rebooted network computer finishes its startup cycle, you are able to login again.

Restriction

To use the reboot utility, you must be logged as a user with uid (user ID) 0 (zero). By default, only three users have such a user ID:

- NSM_NFSROOT (Windows NT)
- QSECOFR (OS/400)
- root (AIX)

To use the NSM_NFSROOT as a Telnet user ID, you have to perform two required steps:

1. Add the NSM_NFSROOT name to the remote_shell_allow list in the auth file.
2. Change the password for the NSM_NFSROOT by means of the Windows NT 4.0 User Manager for Domains. By default, the NSM_NFSROOT user has random, system generated password.

For your information, the following commands can also be executed only by a user with uid 0:

```
halt
mount
umount
```

When the administration password was set up on the network computer, there ma not be a prompt for a user ID or password for the Telnet user. To get interactive access, the user must submit an administration password, so there is no means to log as a user with uid 0. If this situation applies to your environment, please follow the second method of rebooting of the network computer.

The second method is described in the following section and requires basic knowledge of SNMP protocols and associated tools.

18.4 Managing Network Stations using SNMP protocol

This section briefly discusses the Simple Network Management Protocol (SNMP) and its implementation in the V2R1 Network Station Manager. We start with an introduction and follow with a short description of the supported Management Information Bases (MIBs). At the end, we show you some examples of how to take advantage of the SNMP agent that comes with the Network Station Manager.

18.4.1 Introduction

SNMP is a transaction-oriented protocol that allows network elements to be queried directly. It is a simple protocol that allows management information for a network element to be inspected or altered by a system administrator at a network management station. SNMP is a TCP/IP network management protocol and is based on a manager-agent interaction. The SNMP manager (such as Nways Manager 2.0 or Tivoli NetView - IT Director Edition) communicates with its agents. Agents gather management data, while the managers solicit this data and process it. An agent can also send unsolicited information, called a *trap*, to a managing system to inform it of an event that has taken place at the agent system. For example, an agent can send a linkDown trap to the manager to inform it about the loss of a communication link with a particular device.

Important

The current version of the SNMP agent in the Network Station does not support trap messages.

18.4.1.1 The SNMP architecture

The SNMP architectural model is a collection of network management stations and network elements, such as gateways, routers, bridges, hosts, and network computers. These elements act as servers and contain management agents, which perform the network management functions requested by the network management stations. The network management stations act as clients. They run the management applications that monitor and control network elements. SNMP provides a means of communicating between the network management stations and the agents in the network elements to send and receive information about network resources. This information can be status information, counters, identifiers, and more.

The SNMP manager polls the agents for error and statistical data. The performance of the network depends on the level at which the polling interval is set. The physical and logical characteristics of network objects make up a collection of information called a *Management Information Base (MIB)*. The individual pieces of information that comprise an MIB are called MIB objects, and they reside on the agent system. These objects can be accessed and changed by the agent at the manager’s request. Unsolicited data, called *traps*, can also be sent from the agent to the manager under certain conditions.

18.4.1.2 Goals of the SNMP architecture

The SNMP architecture explicitly minimizes the number and complexity of management functions realized by the management agent itself. This goal is attractive in that among other benefits, it allows for:

- Reduced costs in developing management agent software to support the protocol
- Few restrictions on the form and complexity of management tools
- Simplified, easier to implement management functions

A second goal of the protocol is that the functionality can be extended to accommodate additional, possibly unanticipated, aspects of network management. A third goal is that the architecture be, as much as possible, independent of the architecture and mechanisms of particular hosts or gateways.

18.4.1.3 SNMP model

The SNMP model is made up of the following components:

- At least one network element to be managed (agent system) containing an agent.
- At least one network managing station (NMS), containing one or more network management applications.

- A network management protocol for use by the NMS and the agent system to exchange network management information.
- At least one MIB defining the information to be managed on the agent system.

18.4.1.4 Asynchronous request or response protocol

Managing systems generate SNMP requests, and agent systems generate responses to these requests. After a request message has been sent, SNMP does not need to wait for a response. SNMP can send other messages or realize other activities. These attributes make SNMP an asynchronous request or response protocol.

An agent system can also generate SNMP messages, called traps, without a prior request from the managing system. The purpose of a trap message is to inform the managing system of an extraordinary event that has occurred at the agent system. It must be noted that all request and response transactions are subject to the time delays inherent to all networks. Typical SNMP request/response primitives take place in the following manner:

1. The manager polls an agent with a REQUEST for information.
2. The agent supplies the information, which is defined in an MIB, in the form of a RESPONSE.

18.4.1.5 SNMP agent

The SNMP agent has the following two responsibilities:

- To gather error and statistical data defined by MIB objects
- To react to changes in certain MIB variables made by a managing application

In summary, the following steps describe the interactions that take place in an SNMP-managed network:

1. The SNMP agent gathers vital information about its respective device and networks.
2. The SNMP manager polls each agent for MIB information and can display this information at the SNMP manager station. In this manner, a network administrator can manage the network from a management station.
3. An agent also has the ability to send unsolicited data to the SNMP manager in the form of a trap. A trap is generally a network condition detected by an SNMP agent that requires immediate attention by the network administrator.

18.4.1.6 SNMP manager

An SNMP manager refers to a network management station that runs a network management protocol and network management applications. SNMP is the network management protocol that provides the mechanism for management. Several different network management applications exist that can be used, such as Nways Manager 2.0 or Tivoli NetView. The network management application provides the policy to be used for management.

The network management applications rely on Management Information Base (MIB) objects for information regarding the managed system, also called the agent system. Management systems generate requests for this MIB information, and an SNMP agent on the managed system responds to these requests. A request can either be the retrieval or modification of an MIB variable.

The agent system makes network and system information available to other systems by accessing the MIB objects and allowing configuration, performance, and problem management data to be managed by the SNMP manager.

For example, a network manager can access the system description of a particular agent system by using the network management application to gain access to the agent system's sysDescr MIB object. To do this, the managing application builds a message that requests an MIB object called sysDescr. This request is sent to the agent system where the agent decodes the message and then retrieves the information related to the sysDescr MIB object. The agent constructs a response with this information and sends it back to the managing application. When the application has decoded the response, the SNMP manager can then display the agent system′ s description information to the user.

18.4.1.7 Understanding MIBs

The physical and logical characteristics of a system make up a collection of information which can be managed through SNMP. The individual pieces of information make up MIB objects. A Management Information Base (MIB) is comprised of MIB objects that reside on the agent system, where they can be accessed and changed by the agent at the manager′ s request.

The administrative policy established by the Internet Activity Board (IAB), results in a classification of MIBs according to their applicability and purpose. Therefore, MIBs are classified as follows:

- **Standard MIB:** All devices that support SNMP are also required to support a standard set of common managed object definitions of which a MIB is composed. The standard MIB object definition, MIB-II, enables you to monitor and control SNMP managed devices.
- **Enterprise-specific MIB:** SNMP permits vendors to define MIB extensions or enterprise-specific MIBs, specifically for controlling their products. An enterprise-specific MIB must follow certain definition standards just as other MIBs must, to ensure that the information they contain can be accessed and modified by SNMP agents.
- **Experimental MIB:** Generally, new ideas and activities related to the Internet result in the definition of MIB objects. An experimental MIB is comprised of such objects. This approach offers the advantage that all new ideas must be proven while under experiment before they can be proposed for standardization.

18.4.1.8 Representation of management information

Since SNMP is used to manage a broad range of MIB objects, each and every one of these needs to be uniquely identified to provide unambiguous management capabilities. The following sections provide brief discussions on the guiding mechanisms through which MIB objects are uniquely identified for management purposes and by which MIBs are structured.

Abstract Syntax Notation.1 (ASN.1)

ASN.1 is a formal language originated by the International Standards Organization (ISO) that is used to define information exchanged by protocols, in the form of an abstract syntax, meaning that data is defined without regard to a specific machine architecture. ASN.1 is very useful because it does not allow any ambiguities in the information it represents. ASN.1 is used to define managed objects, as well as the Protocol Data Units (PDUs) exchanged by the protocols that manage those objects. ASN.1 provides two representations of the information defined by it. One representation can be read by humans, and the other representation is an encoded version of the same information, which is used by the communications protocols.

Each managed object is described using an ASN.1 notation called OBJECT-TYPE. An OBJECT-TYPE definition consists of five fields represented in the following example, which describes an MIB object called hrSystemUptime (from the Host group in the MIB-II):

```
hrSystemUptime OBJECT-TYPE
    SYNTAX TimeTicks
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
          "The amount of time since this host was last
          initialized. Note that this is different from
          sysUpTime in MIB-II (RFC 1213) because sysUpTime is
          the uptime of the network management portion of the
          system."
    ::= { hrSystem 1 }
```

The following is a description of each of the fields that define an OBJECT-TYPE:

- **OBJECT DESCRIPTOR (Name):** A textual name for the OBJECT-TYPE. For example, hrSystemUptime, and sysUpTime are OBJECT DESCRIPTORS or names for an OBJECT-TYPE.
- **SYNTAX:** Defines the data type associated with the OBJECT-TYPE. ASN.1 constructs are used to define this structure, although the full generality of ASN.1 is not permitted.

  The ASN.1 type ObjectSyntax defines three categories of object syntax: simple, application-wide, and simply constructed. INTEGER, OCTET STRING, NetworkAddress, Counter, Gauge, TimeTicks, SEQUENCE, and SEQUENCE OF are all examples of these types of syntax.
- **ACCESS:** Defines the level of access permitted for the managed object. It can be one of the following levels:
  - **read-only**: Object instances may only be read, not set.
  - **read-write**: Object instances may be read or set.
  - **write-only**: Object instances may only be set, not read.
  - **not-accessible**: Object instances may not be read or set.
- **STATUS:** Defines the managed objects' implementation requirement in terms of one of the following statuses:
  - **mandatory**: A managed node must implement this object.
  - **optional**: A managed node may implement this object.
  - **obsolete**: A managed node does not need to implement this object anymore.
- **DESCRIPTION:** A textual description of the semantics of the OBJECT-TYPE. In the case of non-enterprise-specific MIB implementations, take care to ensure that instances of the managed object fulfills its description since the

MIB is intended for use in multi vendor environments. As such, it is vital that objects have consistent meanings across all machines.

18.4.1.9 MIB naming conventions

An MIB object has a label derived from its location in the tree structure. A label is a pairing of a brief textual description and an integer. An OBJECT IDENTIFIER is a sequence of non-negative integers that traverse a global tree for the purpose of identifying an object. The tree consists of a root, which branches to connect to a number of labeled nodes, also called subordinates. Each node may, in turn, have children of its own that are labeled. In this case, we may term the node a subtree or intermediate node. If a node does not have children, it is called a leaf node.

A fully qualified OBJECT IDENTIFIER for a particular MIB object contains all nodes, starting at the root and traversing the tree to an arbitrary level of depth, until the desired leaf object is reached. The nodes are concatenated and separated by periods, in a format known as ASN.1 notation. For example, the mib-2 subtree is iso.org.dod.internet.mgmt.mib-2, which is concisely written in ASN.1 notation as 1.3.6.1.2.1.

The OBJECT IDENTIFIER for the sysContact object contained in the MIB-II is 1.3.6.1.2.1.1.4, as you can see in Figure 447, by following the labels from the root down to the leaf object.

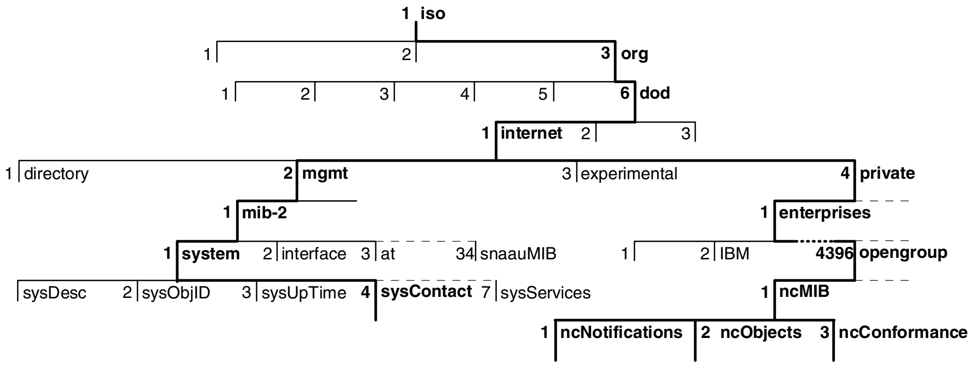


Figure 447. View of the MIB tree structure

The standard MIB-II is registered in the mib-2(1) subtree. Experimental MIBs are registered in the experimental(3) subtree. Enterprise-specific MIBs are registered in the private(4) subtree. Each enterprise is assigned a number. IBM is assigned the enterprise number 2. Therefore, all IBM enterprise-specific MIB objects have an OBJECT IDENTIFIER starting with 1.3.6.1.4.1.2, corresponding to the tree structure iso.org.dod.internet.private.enterprises.ibm. Open Group is assigned the enterprise number 4396, and within it, the number 1 is assigned to the network computer MIB. By analogy, all Open Group NC-specific MIB objects have an OBJECT IDENTIFIER starting with 1.3.6.1.4.1.4396.1, corresponding to the tree structure iso.org.dod.internet.private.enterprises.opengroup.ncMIB.

Note

You can find the e numbers assigned to a specific enterprise at the following URL: `ftp://ftp.isi.edu/in-notes/iana/assignments/enterprise-numbers`

18.4.1.10 SNMP operations

To be consistent with its simplicity objective, SNMP contains few commands to execute its operations. SNMP supports two commands that managing systems can use to retrieve information from a managed system and one command to store a value into a managed system. All other operations are considered to be side-effects of these three commands.

As an example, SNMP does not contain an explicit reboot command. However, this action may be invoked by simply setting a parameter indicating the number of seconds until system reboot. In addition to these commands, SNMP supports an event-driven mechanism used to alert managing stations of the occurrence of extraordinary events at a managed system.

The approach that SNMP is based on for network management makes it a simple, stable, and flexible protocol. It can accommodate new operations as side-effects of the same SNMP commands acting upon new MIB variables, without requiring SNMP to be modified.

SNMP also specifies that if a single SNMP message specifies operations on multiple variables, the operations will either be performed on all variables or on none of them. No operation will be performed if any of the variables are in error.

Each SNMP operation is defined in a particular PDU. A brief description of each operation follows:

GET This is a request originated by a managing application to retrieve an instance of one or more MIB objects. The specified instance is retrieved for each variable in the request, provided that community profile authentication has been successful.

GETNEXT This is a request originated by a managing application to retrieve the next valid instance following the specified instance of one or more MIB objects, provided that community profile authentication has been successful.

SET This is a request originated by a managing application to store a specific value for one or more MIB variables. All variables must be updated simultaneously, or none of them are update.

GET-RESPONSE

This is response data that is originated by an agent application and is sent back to the originator of a GET, GETNEXT, or SET request.

TRAP This is an unsolicited message originated by an agent application that is sent to one or more managing systems within the correct community, to alert them of the occurrence of an event. Traps include the following types:

- coldStart (0)
- warmStart (1)
- linkDown (2)
- linkUp (3)
- authenticationFailure (4)
- egpNeighborLoss (5)
- enterpriseSpecific (6)

18.4.2 Supported MIBs

The following standard MIB is supported at the NSM V2R1:

- **MIB-II (RFC1213):** MIB-II describes those objects that are implemented by managed nodes running the Internet suite of protocols. The network computer implements 9 of the 10 MIB-II groups. The Exterior Gateway Protocol (EGP) group is not supported by the operating system. The network computer does not provide Exterior Gateway Protocol support.

  Examples of some of the MIB-II objects supported are:

  - **sysContact:** This MIB-II object belongs to the system group. It provides the identification of the contact person for this managed node; it can also contain information on how to contact this person.
  - **ipInReceives:** This MIB-II object belongs to the IP group. It provides the total number of input datagrams received, including those received in error.
  - **tcpInSegs:** This MIB-II object belongs to the TCP group. It provides the total number of segments received, including those received in error.

- **NCP-MIB**: Additionally to RFC-1213 (MIB-II), the latest software for the network computer implements the support for the NCP-MIB. NCP-MIB was developed by the Open Group, more precisely by the network computer working group and Network Computer System Management group. Open Group is an independent body and was chosen by leading vendors as central resource to manage all network computer standardization. NCP stands for the Network Computer Profile (currently we have Version 2 of this reference).

  The following are examples of some of the NCP-MIB objects supported:

  - **ncSysManuf:** Manufacturer of the system hardware.
  - **ncSysModelId:** System hardware model identifier.
  - **ncSysMemTotal:** Physical size of system memory in kilobytes.
  - **ncSysProcessorType:** Processor type. Vendor specific.
  - **ncUserName:** The name of the user who last logged on.

For complete list of all objects contained in the NCP MIB, see Appendix H, “NCP-MIB Version 1 definition file” on page 629.

18.4.3 Installing, configuring, and using MIB browser

For our test environment, we chose Windows NT 4.0 Workstation and a third-party SNMP software kit called MIB Browser Professional Edition with MIB Compiler Version 5B (Evaluation edition) produced by MG-SOFT Corporation. This software is intended to work on any Microsoft 32-bit software (Windows 95, Windows 98, Windows NT). At the time this redbook was written, there was no mention about Windows 2000. Always check the latest available version and information at: `http://www.mg-soft.com/download.html`

18.4.3.1 Installation on the network computer

The SNMP daemon in normal conditions should start automatically after a successful boot from the NSM V2R1 as it starts from the .profile file. During its startup, it creates a log file. You can find it in the /tmp/log temporary directory. Its name is snmpd.log and usually contains the information, shown in Figure 448.

```
Start Time = Mon Oct 11 15:27:17 1999
snmpd in free(): warning: junk pointer, too high to make sense.
Opening port(s): 161
Desktop socket opened.. ready to receive events..
```

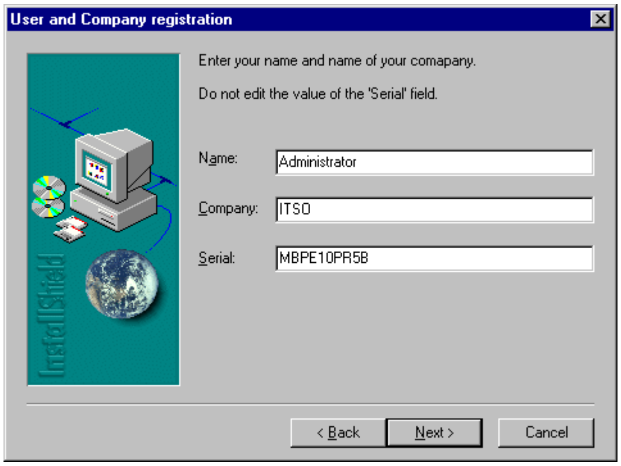
Figure 448. Information extracted from the snmpd.log file

18.4.3.2 Installation on Windows NT 4.0

To install the MG-SOFT MIB browser on Windows NT, follow these steps:

1. Download the required software from the Web site at: `http://www.mg-soft.com/download.html`.
2. Extract the content of the zip file to any directory.
3. Log on as a user with administrator privileges.

   During installation, there is a window with a serial number (Figure 449). Do not change it. Follow the installation procedure. If you encounter any problem, for example, with registering OCX components, let the installation program to finish. Then, carefully read the readme.txt file included in the package.



User and Company registration

Enter your name and name of your comapany.

Do not edit the value of the 'Serial' field.

Name: Administrator

Company: ITSO

Serial: MBPE10PR5B

Figure 449. Window with a serial number prompt

Now you are ready to start and configure your SNMP component.

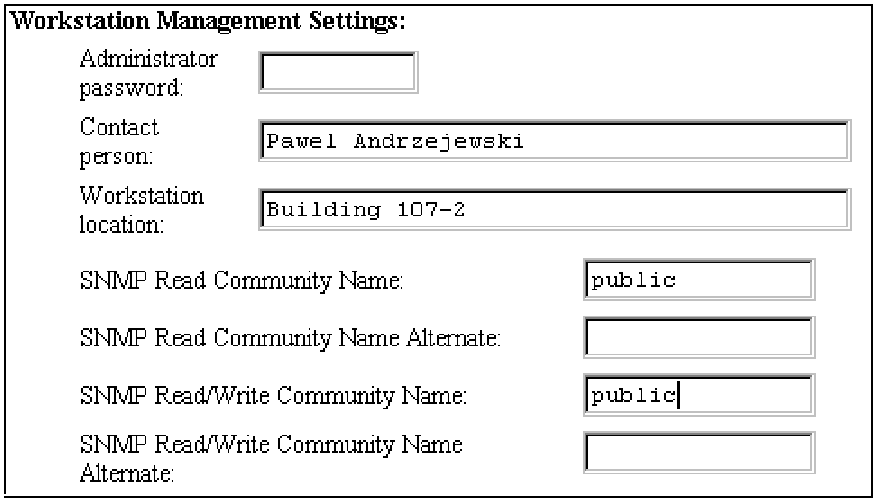
18.4.3.3 Configuring MIB browser

Before configuring SNMP MIB browser, you must first set up community names in all Network Stations you want to manage. You can do it using the NSM graphical user interface or the NSM command line utility. To set the community names, follow these steps:

1. Connect to your NSM V2R1 server from your browser. You must choose the preference level. A valid choice may include system (all NCs) or workstation preference level (particular NC).
2. Select the preference level.
3. From Setup Task window, select **Hardware -> Workstations**.
4. Press the Page Down button several times until you reach the bottom of the page.

5. Enter your community names. Try to avoid well-known names, because the SNMP Community Name is part of the security provided with SNMP and can be thought of as a type of password.

   We use public just for simplicity (Figure 450).



Workstation Management Settings:

Administrator password:

Contact person: Pawel Andrzejewski

Workstation location: Building 107-2

SNMP Read Community Name: public

SNMP Read Community Name Alternate:

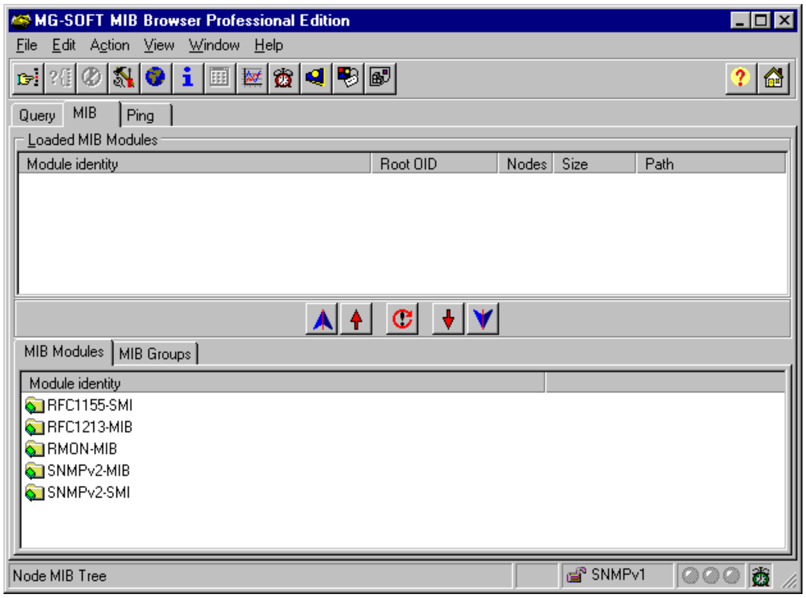
SNMP Read/Write Community Name: public

SNMP Read/Write Community Name Alternate:

Figure 450. Setting up the community names in the NSM V2R1

The changes to take effect require the workstation to reboot.

In the second part of the configuration, we focus on our Windows MIB browser. The initial window after starting the application should look like the example in Figure 451.

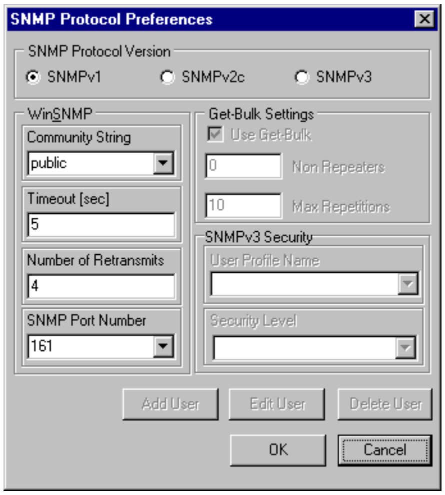

MG-SOFT MIB Browser Professional Edition
File Edit Action View Window Help
Query MIB Ping
Loaded MIB Modules
Module identity Root OID Nodes Size Path
MIB Modules MIB Groups
Node MIB Tree
SNMPv1

Module identity
RFC1155-SMI
RFC1213-MIB
RMON-MIB
SNMPv2-MIB
SNMPv2-SMI

Figure 451. The initial MIB browser display

Perform the following steps:

1. Click **Edit -> SNMP Protocol Preferences**. The window shown in Figure 452 should appear.


SNMP Protocol Preferences

SNMP Protocol Version: ● SNMPv1 ○ SNMPv2c ○ SNMPv3

WinSNMP
- Community String: public
- Timeout [sec]: 5
- Number of Retransmits: 4
- SNMP Port Number: 161

Get-Bulk Settings
- ☑ Use Get-Bulk
- 0 Non Repeaters
- 10 Max Repetitions

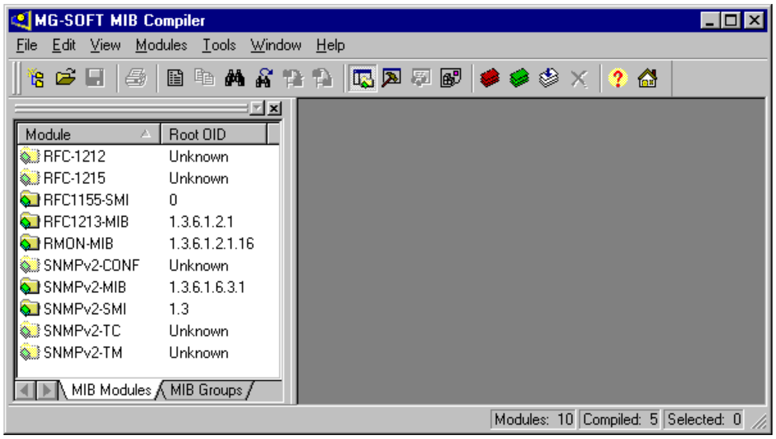
SNMPv3 Security
- User Profile Name:
- Security Level:

Figure 452. Preferences window from MG-SOFT MIB browser

2. Check the values, and select the protocol version. We select SNMPv1. Select **OK**.

Compile the NCP-MIB. Compiling the MIB converts it from a standard text version into the MG-SOFT's proprietary SMIDB format. Initially five MIBs are supplied in SMIDB format. Follow these steps:

1. To access the compiler menu, select **Action -> Run MIB Compiler** from the main menu. The display shown in Figure 453 should appear.


MG-SOFT MIB Compiler

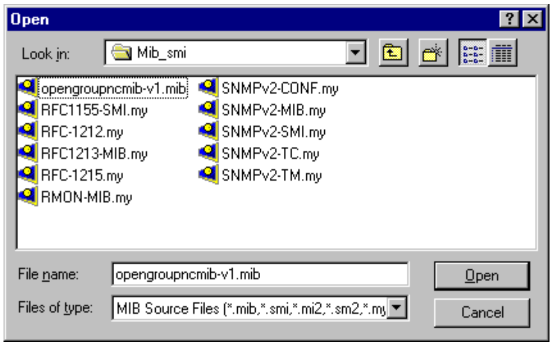
Module	Root OID
RFC-1212	Unknown
RFC-1215	Unknown
RFC1155-SMI	0
RFC1213-MIB	1.3.6.1.2.1
RMON-MIB	1.3.6.1.2.1.16
SNMPv2-CONF	Unknown
SNMPv2-MIB	1.3.6.1.6.3.1
SNMPv2-SMI	1.3
SNMPv2-TC	Unknown
SNMPv2-TM	Unknown

Modules: 10 Compiled: 5 Selected: 0

Figure 453. Compiler display

2. Copy $PRODBASEV2\x86\usr\share\snmp\mibs\opengroupncmib-v1.mib into the C:\Program Files\MG-SOFT\MIB Browser\MIB_SMI directory.

3. Select **File -> Compile**. Select **opengroupncmib-v1.mib**. See Figure 454 on page 592.



Look in: Mib_smi

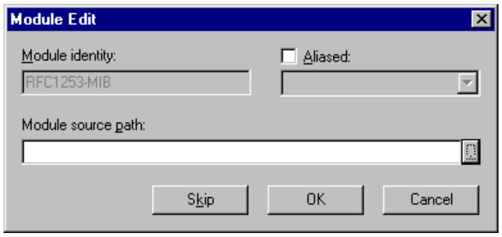
opengroupncmib-v1.mib
RFC1155-SMI.my
RFC-1212.my
RFC1213-MIB.my
RFC-1215.my
RMON-MIB.my
SNMPv2-CONF.my
SNMPv2-MIB.my
SNMPv2-SMI.my
SNMPv2-TC.my
SNMPv2-TM.my

File name: opengroupncmib-v1.mib

Files of type: MIB Source Files (*.mib,*.smi,*.mi2,*.sm2,*.my

Figure 454. Select MIB to compile display

During compilation, we encountered the following situation. The window shown in Figure 455 appeared because the compiler needed direct access to all MIB databases specified in the import section of the currently compiled MIB.



Module identity: RFC1253-MIB

□ Aliased:

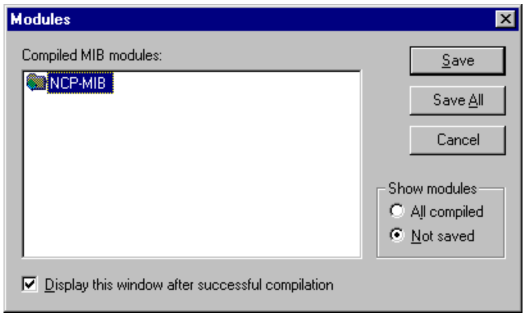
Module source path:

Figure 455. Request for missing MIB file

In our case, there were two MIBs missing: RFC1253-MIB and SYSAPPL-MIB. To find them, we used the World Wide Web (WWW) search engine `http://www.altavista.digital.com` with search keyword `RFC1253-MIB.my`. From the obtained list, we chose the first item: `http://www.cisco.com/public/mibs/v2-to-v1/`

From this directory, we downloaded the missing RFC1253-MIB.my file. We obtained the second MIB from `http://www.snmpinfo.com/ftp/st-mibs/nst-mibs.zip` file. After downloading the nst-mibs.zip file, we extracted SYSAPPL-MIB.my module to the C:\Program Files\MG-SOFT\MIB Browser\MIB_SMI directory.

Now we have all we need to successfully compile the NCP-MIB. Reload the compiler and compile again. When it ends successfully, the window shown in Figure 456 displays the proposition to save the just compiled MIB.



Compiled MIB modules:

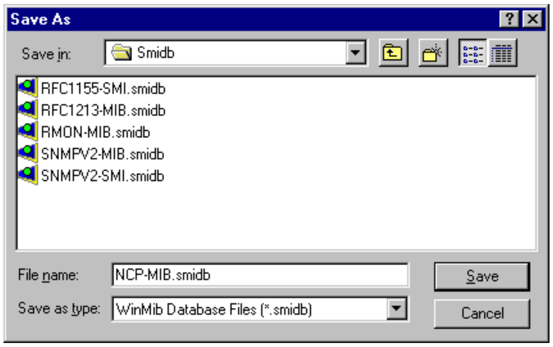
NCP-MIB

Show modules
○ All compiled
● Not saved

☑ Display this window after successful compilation

Figure 456. Message after successful compilation

Select **Save**, and choose the destination directory (Figure 457).



Save in: Smidb

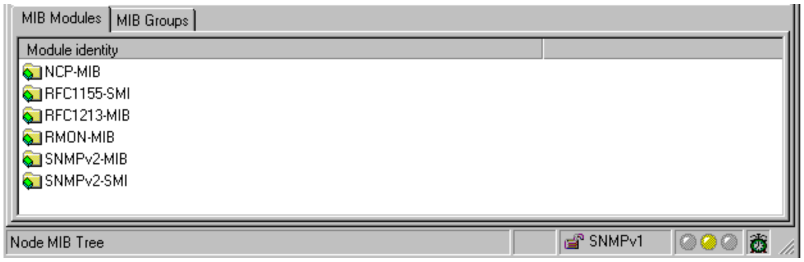
- RFC1155-SMI.smidb
- RFC1213-MIB.smidb
- RMON-MIB.smidb
- SNMPV2-MIB.smidb
- SNMPV2-SMI.smidb

File name: NCP-MIB.smidb

Save as type: WinMib Database Files (*.smidb)

Figure 457. Destination prompt window

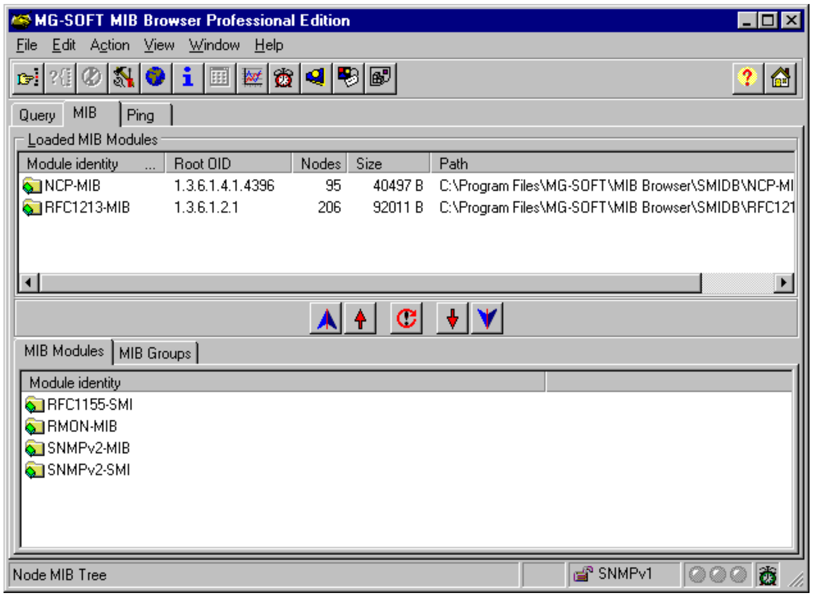
Select the proposed directory, and click **Save**. Then exit the compiler and the MIB browser. Start the MIB browser again. Now at the lower part of the displayed window, you see six MIB modules, five old ones and one new (NCP-MIB). See Figure 458.



Module identity
NCP-MIB
RFC1155-SMI
RFC1213-MIB
RMON-MIB
SNMPv2-MIB
SNMPv2-SMI

Figure 458. MIB browser with the just compiled NCP-MIB module

Load the desired modules that you will use for browsing. Do it by double-clicking the MIBs modules NCP-MIB and RFC1213-MIB (Figure 458).



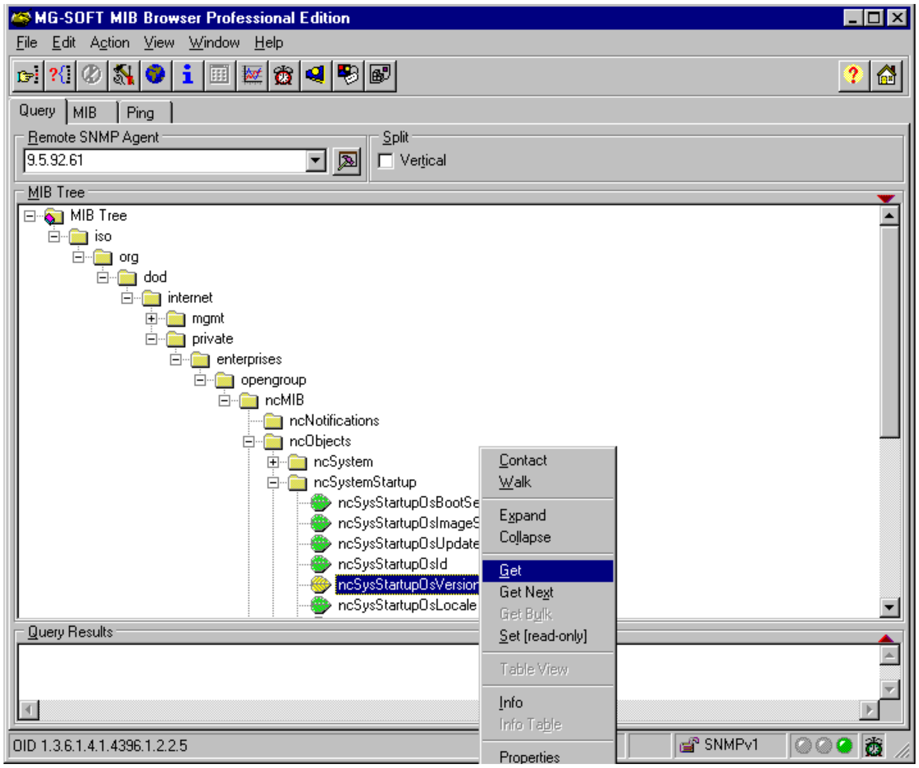
Module identity ...	Root OID	Nodes	Size	Path
NCP-MIB	1.3.6.1.4.1.4396	95	40497 B	C:\Program Files\MG-SOFT\MIB Browser\SMIDB\NCP-MI
RFC1213-MIB	1.3.6.1.2.1	206	92011 B	C:\Program Files\MG-SOFT\MIB Browser\SMIDB\RFC121

Module identity
RFC1155-SMI
RMON-MIB
SNMPv2-MIB
SNMPv2-SMI

Figure 459. Correctly prepared browser

To start browsing, click the **Query** tab. Enter manually the IP address of the target network computer. Or, let the program discover it automatically by selecting **Window->Discover Window**.

The main Query window consists of two parts: MIB Tree and Query Results. Expand the MIB tree to the desired level and right-click and select Get (Figure 460).



Remote SNMP Agent: 9.5.92.61

OID 1.3.6.1.4.1.4396.1.2.2.5

Figure 460. Available actions against a given Object Identifier (OID)

You can perform the following actions based on the type of given Object Identifier (OID):

- **Contact**: Queries the remote SNMP agent for the SysUpTime value using the current SNMP protocol settings.
- **Walk**: Performs SNMP walk operation starting at the selected OID. When performing the SNMP walk operation, MIB Browser actually repeatedly queries the remote SNMP agent by using the GET NEXT operation (or GET BULK operation in SNMPv2c and SNMPv3, if required in the SNMP Protocol Preferences window).

  If the Walk Until No-Such Or End-Of-Mib-View checkbox is selected in the Query Results tab of the MIB Browser Preferences, the MIB Browser will perform the walk operation until it queries all OIDs in the remote SNMP agent.
- **Expand**: Expands the right-clicked MIB Tree node. To keep the expanding node in the visible area of the MIB Tree panel, select the node to select it.
- **Collapse**: Collapses the right-clicked MIB Tree node. In order to keep the collapsing node in the visible area of the MIB Tree panel, first select the node by left-clicking it.

- **Get**: Performs the GET operation querying the selected OID.
- **Get Next**: Performs the GET NEXT operation querying the selected OID.
- **Get Bulk**: Performs the GET BULK operation querying the selected OID. This operation is available only when using SNMPv2c or SNMPv3 protocols.
- **Set**: Displays the SET dialog window.
- **Table View**: Displays the Table View window. This operation is available only for a Table or Entry node in the MIB tree.
- **Info**: Displays the selected OID in the Info window.
- **Info Table**: Displays the Select Table Indexes window where you can select any number of available indexes. Afterwards, table OIDs with the selected indexes are displayed in the Info window. This operation is available only for a Table node in the MIB tree.
- **Properties**: Displays the MIB Node Properties window for the selected MIB tree node.

18.4.4 Remote boot using SNMP

We show you how to remotely reboot desired network computer. You have to find in the ncMIB tree the ncSysStatusVitalState Object Identifier. Its Object Identifier number is 1.3.6.1.4.1.4396.1.2.3.2. See Figure 461.

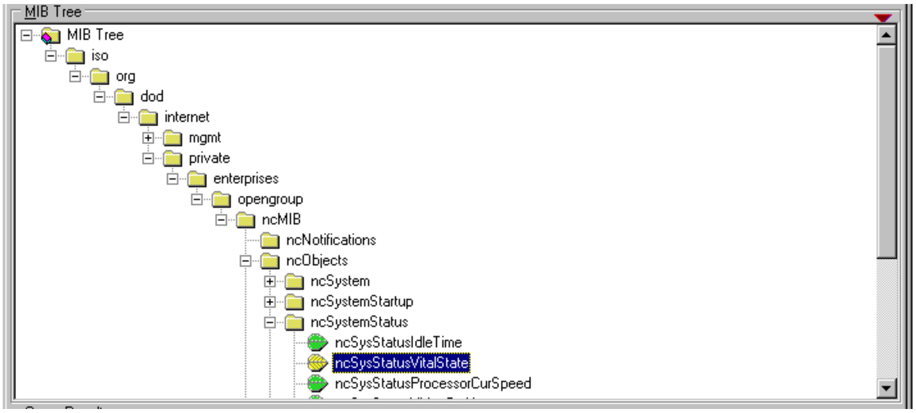
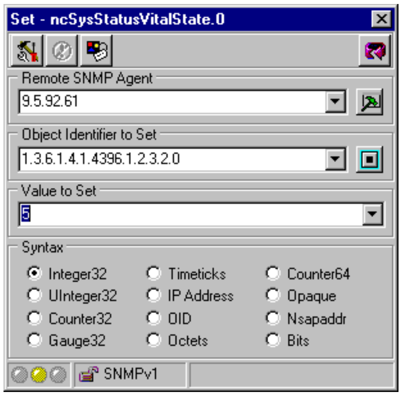


Figure 461. Selecting an OID for rebooting

Right-click, and select **Set**. The window shown in Figure 462 on page 596 should appear. Select five (5) under Value to set it, and click the most left upper icon.



Set - ncSysStatusVitalState.0

Remote SNMP Agent: 9.5.92.61

Object Identifier to Set: 1.3.6.1.4.1.4396.1.2.3.2.0

Value to Set: 5

Syntax:

● Integer32	○ Timeticks	○ Counter64
○ UInteger32	○ IP Address	○ Opaque
○ Counter32	○ OID	○ Nsapaddr
○ Gauge32	○ Octets	○ Bits

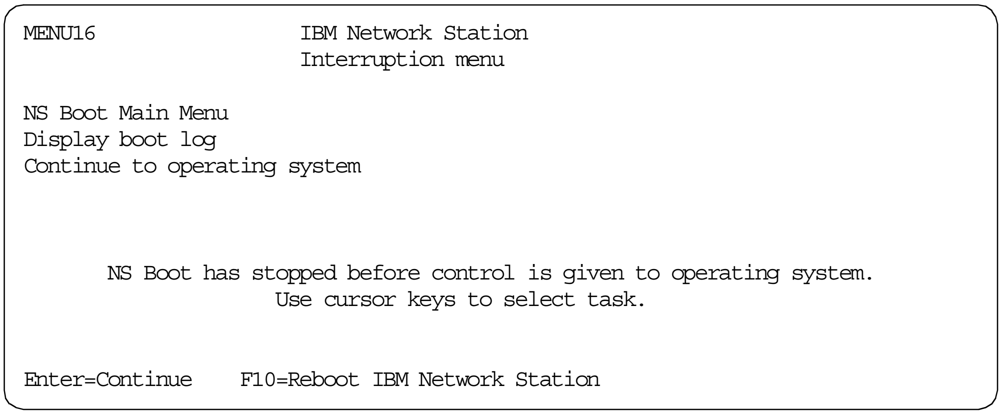
SNMPv1

Figure 462. Performing set operation causing remote NC to reboot

18.5 Boot monitor tools

For a detailed description about boot utilities for all supported hardware, see *Using IBM Network Station Manager V2R1,* SC41-0690. In addition to the information included in that book, this section tells you how to get access to functions described in Appendix F, “Boot monitor service aid menu” on page 625.

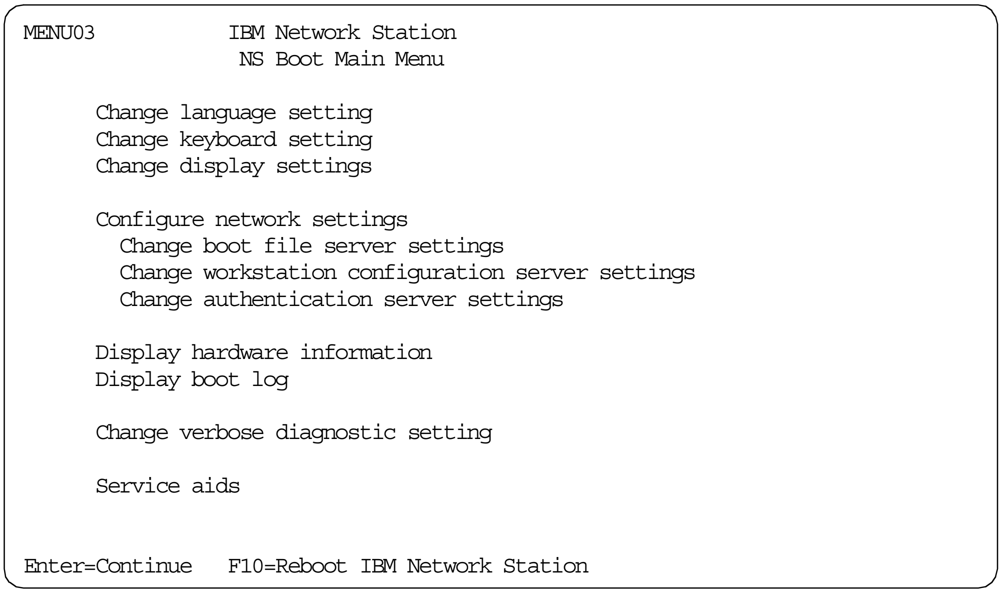
When your network computer starts or is being rebooted, press Alt+F9 while loading the kernel file (you can recognize this phase by seeing changing a byte counter in text mode or a moving dashed line in graphics mode). As a result, you obtain the MENU16 menu (Figure 463).



```
MENU16                 IBM Network Station
                       Interruption menu

NS Boot Main Menu
Display boot log
Continue to operating system



       NS Boot has stopped before control is given to operating system.
                     Use cursor keys to select task.


Enter=Continue    F10=Reboot IBM Network Station
```

Figure 463. Interruption menu

Select **NS Boot Main menu**. As a result, the menu shown in Figure 464 is presented.



```
MENU03           IBM Network Station
                  NS Boot Main Menu

      Change language setting
      Change keyboard setting
      Change display settings

      Configure network settings
        Change boot file server settings
        Change workstation configuration server settings
        Change authentication server settings

      Display hardware information
      Display boot log

      Change verbose diagnostic setting

      Service aids


Enter=Continue   F10=Reboot IBM Network Station
```

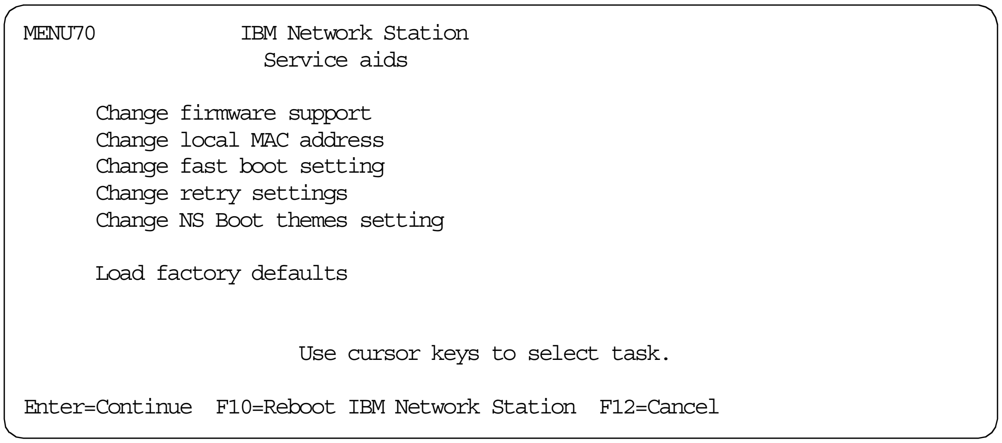
Figure 464. Network Station Boot Main Menu

Select the **Service aids** menu.

Note

You can directly enter the menu shown in Figure 464 by pressing Esc during the startup sequence. If you have enabled the password control, you must enter the case-sensitive administrator password.

The Service aids menu appears as shown in Figure 465.



```
MENU70            IBM Network Station
                    Service aids

      Change firmware support
      Change local MAC address
      Change fast boot setting
      Change retry settings
      Change NS Boot themes setting

      Load factory defaults


                       Use cursor keys to select task.

Enter=Continue  F10=Reboot IBM Network Station  F12=Cancel
```

Figure 465. Service aids menu

From this menu (MENU70) and only from this menu, you can enter the specialized Network Station hardware related menu (Figure 466 on page 598).

To do this, press Ctrl+F9**.**

```
Main Menu

 1. Memory test.
 2. Dump PCI Configuration Register to serial port.
 3. Cache control.
 4. Video test.
 5. Test all.
 6. I/O (serial and parallel).
 7. Toggle auto test.
 8. Configuration menu
 9. Misc menu
 0. Exit
```

Figure 466. Hardware settings menu

18.6 Remote Shell Program command

It was possible to run Remote Shell Program (RSH) against Network Station in the NSM V1R3. This method of invoking programs was useful for an administrator for testing and debugging purposes. There was no real command line prompt for starting applications just by typing a command. There is a very detailed description of how to do this in Section 19.5 of *IBM Network Station Manager Release 3 Guide for Windows NT*, SG24-5221.

Designers of the NSM V2R1 have introduced a fully functioning Telnet daemon, which loads into Network Station memory while executing .profile file. Having this ability, it becomes unnecessary to support the RSH daemon in the NSM V2R1. Of course there is still strong support for accessing remote applications in the opposite direction, from Network Station as a display (X server) to a remote host executing required application (X client).

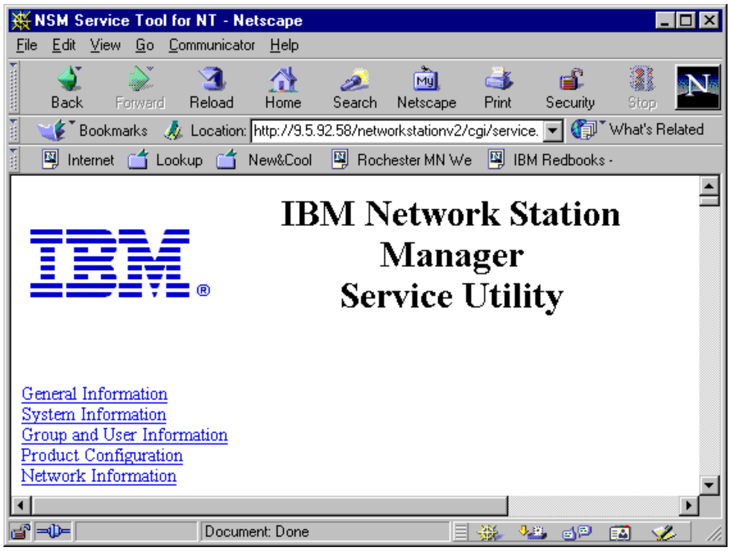
For more information about Telnet, see 18.1, “Telnet into the Network Station” on page 575.

18.7 NSM Service Tool for Windows NT

Like the NSM V1R3 for Windows NT, the NSM V2R1 includes specialized software that delivers a lot of important information concerning the server side of the NSM V2R1 for the Windows NT platform. The latest version of IBM Network Station Manager Service Utility for Windows NT can be found in two places in the Windows NT directory structure:

- **c:\networkstationv2\servbase\bin\ntnsmver.exe**: This is the binary to execute on the NSM V2R1 Windows NT command line prompt. To save the output, redirect it to any file, for example `ntnsmver > nsmv2r1_nt.html` To see the result, since an output generated by this software is in HTML style, simply double-click on the **nsmv2r1_nt** file in the Windows NT Explorer, or set it as the input parameter for your browser, for example `netscape d:\<path>\nsmv2r1_nt.html`.
- **c:\networkstationv2\servbase\cgi-bin\service.exe**: This is the binary to execute directly from any browser on any computer that has a TCP/IP connection the with tested NSM V2R1.

Because the output is usually multi-page, we show only the first few lines (Figure 467).


NSM Service Tool for NT - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://9.5.92.58/networkstationv2/cgi/service. What's Related
Internet Lookup New&Cool Rochester MN We IBM Redbooks -
Document: Done

IBM Network Station Manager Service Utility

General Information
System Information
Group and User Information
Product Configuration
Network Information

Figure 467. Executing the IBM NSM Service Utility from Netscape browser

There are always five sections in the report, plus two options, if you choose extended output:

- **General Information:** Contains such information as the date of execution, version level, build level, active locale, and type of server.
- **System Information:** Shows information about active and stopped services, as well as disk information.
- **Group and User Information:** Lists all local groups and members of the two main NSM V2R1 related groups: NSMAdmin and NSMUser.
- **Product Configuration:** Includes information taken from registry database, regarding different components of the NSMV2R1.
- **Network Information:** Informs you about the current TCP/IP configuration and shows all active connections and open ports.

The next two options are present in the report only if you choose Extended Output:

- **Web Server Environment Variables**: Shows what is embedded in the Web server environment variables.
- **Module Version Information:** Gives detailed information about each important binary used by the NSM V2R1 and network computers.

18.8 Screen captures

There may be times when documenting problems that you may find it useful to create graphics of the windows on the Network Station. You can capture screens with two different commands:

- **Alt+Shift+PrintScreen**: Captures the entire Network Station screen and stores it in a bitmap (.bmp) file.
- **Alt+Shift+ScrollLock**: Captures the active window only.

The resulting bmp files are stored in the /NetworkStation2/userbase/home/<user name>/registry/documents directory.

18.9 Investigating the NC Registry

The `ncregget` command can be used to view information in the NC Registry. The syntax for the command is `ncregget key:value`, where *key* is the registry key you want to view and *value* is the value you want to extract. This is an important tool because it shows what information the registry was populated. For a given workstation and user, the information should be the same as seen in their eXtensible Markup Language (XML) configuration profiles.

The possible registry keys are:

- boot/termids
- boot/nvram
- boot/dhcp
- boot/unique
- config
- desktop/preferences
- ns5250/preferences
- ns3270/preferences
- nsterm/preferences
- netscape/preferences
- java/appletviewer
- login/session
- login/rules
- login/groups
- ica/connections

Example registry keys are:

- ncregget config
- ncregget config:boot-test-ram
- ncregget netscape/preferences:lockPref.java.user_plugin

Note: Everything is case sensitive.

The second tool for displaying information from the registry is `ncpkgget`. This utility extracts the XML format of the registry that defines the desktop icons and command parameters to the programs. This is helpful in determining why something is not launching, or launching with the wrong information. You can use the `grep` application that filters the output from the `ncpkgget` command. For example, the following command produces the output (desktops.txt):

```
ncpkgget /desktops/default | grep command > desktops.txt
```

You can see this output here:

```
<FIELD NAME="command">nsm_wrapper ns5250</FIELD>
<FIELD NAME="command">nsm_wrapper ns3270</FIELD>
<FIELD NAME="command">run_netscape</FIELD>
<FIELD NAME="autocommand">run_netscape</FIELD>
```

```
<FIELD NAME="command">nsm_wrapper nsterm</FIELD>
<FIELD NAME="command">launchnsmv2</FIELD>
<FIELD NAME="command">nsm_wrapper  /usr/lib/ICAClient/wfcmgr</FIELD>
<FIELD NAME="command">nsm_wrapper ncdocmgr</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper ncedit</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper ncscheduler</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper ncpaint</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper rvplayer</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper calibrate</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper nccalc</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper ncaudio</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper ncxanim</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper xterm -sb -sl 1000 -rv -name Advanced_Diagnostics</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper ncprmonitor</FIELD>
<FIELD NAME="autocommand"/>
<FIELD NAME="command">nsm_wrapper ns5250 abc.mycompany.com</FIELD>
<FIELD NAME="command">nsm_wrapper ns5250 xyz.mycompany.com</FIELD>
<FIELD NAME="command">nsm_wrapper ns5250</FIELD>
```

These lines define the command string (and all parameters) that will be run when the icon is clicked on the launch bar. All information displayed by `ncregget` and `ncpkgget` strictly reflect the current status of the locally memory-handled registry. If you change any value using NSM or the command line, you must log off or reboot depending on which value you altered (in the session specific profile or in the network computer specific profile).

Limitation

There is one important limitation you should know about it. Using both `ncregget` and `ncpkgget` commands in the *Telnet* window, you will see different result than when using them in the Advanced Diagnostic window. The reason is that Telnet daemon, which starts well before user can log on, creates its own registry object that reflects only information taken from the Workstation Configuration server. This means from the following files: shipped.nsm, allncs.nsm, and if they exist from terminal level, specific configuration profiles <nc-id>.nsm.

As you know, a lot of information is loaded from session specific profiles, which are loaded when a user logs on to the network computer (allusers.nsm and, if they exist, from <group name>.nsm and <user name>.nsm).

Starting Telnet after the user logs on to the network computer does not help. If somebody is connected by Telnet to the network computer, using a `ps` program, you can see that there is an another `ncregistryd` program running. If you kill it, using `kill -kill <pid>`, you will not be able to gather any information using the `ncregget` and `ncpkgget` utilities from your Telnet session. On the other hand, it does not interfere with gathering registry information in the Advanced Diagnostic window in the same time.

18.10 Core dumps

The operating system of the Network Station has the ability to store core dumps. By default, they will be written to the user home directory. For example, if ns3270 crashes, then a file named ns3270.core will be created in the user home directory. This file has practically no value for the end user, so it should be sent to the service or development team to process. It is an easy task if we have in one place, just a few Network Station. But with many users across many systems, it may be a real chore to gather them. In such situation we should use the *coreserver*. The coreserver is a background application (daemon) that runs on a Network Station and processes all core dumps sent to it by correctly configured peer Network Stations. The final result is that you have all core dumps in one place. To enable this feature, you need to modify the .profile file. In the following example, you can see the fragment of .profile file prior to modification:

```
# The coreserver can store/process core dumps
#if [ $IPADDRESS = "a.b.c.d" ]; then
#mount server:/hostpath /mnt
#coreserver --coreroot /mnt --allow-all
#fi
#Config everybody to send their cores to a.b.c.d
#ncsetcore a.b.c.d
```

The following sections provide two examples of enabling the coreserver in both the RFS and NFS environment.

RFS environment

```
# The coreserver can store/process core dumps
if [ $IPADDRESS = "192.168.0.10" ]; then
mount -t rfs 192.168.0.1:/QIBM/Service/NetworkStation/FFDC /mnt
coreserver --coreroot /mnt --allow-all
fi
#Config everybody to send their cores to 192.168.0.10
ncsetcore 192.168.0.10
```

NFS environment

```
# The coreserver can store/process core dumps
if [ $IPADDRESS = "192.168.0.10" ]; then
mount 192.168.0.1:/coredumps /mnt
coreserver --coreroot /mnt --allow-all
fi
#Config everybody to send their cores to a.b.c.d
ncsetcore 192.168.0.10
```

Note

Remember to export /coredumps with read/write access in your NFS server.

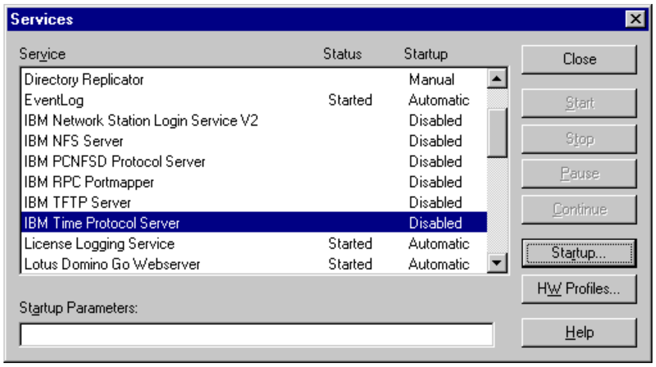
In the above examples, the unit with the IP address 192.168.0.10 becomes the coreserver for the entire network and stores all the dump cores in one place. This way, the administrator can look in that one place to see if any of the Network Stations had any problems.

18.11 Manually removing NSM V2R1 from a Windows NT server

This procedure can be used if the normal way (Add/Remove Programs from the Control Panel doesn't work). Make sure no users are connected to the NSM server from which you're removing NSM.

> **Note**
>
> This method of completely removing NSM V2R1 may not be the most optimum method. However, it worked when we had to completely remove the NSM V2R1 beta code from our lab servers. It also assumes you have not installed the IBM DHCP and IBM DDNS servers.

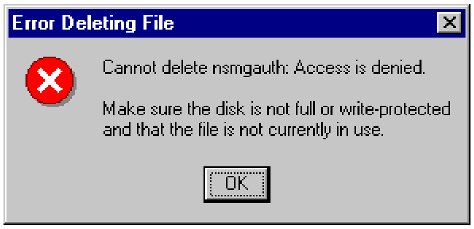
1. Stop and disable all the eNetwork On-Demand-related services by using the Services function in the Control Panel (Figure 468).



Service	Status	Startup
Directory Replicator		Manual
EventLog	Started	Automatic
IBM Network Station Login Service V2		Disabled
IBM NFS Server		Disabled
IBM PCNFSD Protocol Server		Disabled
IBM RPC Portmapper		Disabled
IBM TFTP Server		Disabled
IBM Time Protocol Server		Disabled
License Logging Service	Started	Automatic
Lotus Domino Go Webserver	Started	Automatic

Figure 468. Stopping and disabling the eNetwork On-Demand services

2. Remove the x:\OnDemand directory.
3. Remove the x:\NetworkStationV2 directory. If you see the error message shown in Figure 469, rename nsmgauth.dll file in the x:\NetworkStationV2\servbase\bin directory to something else. Continue deleting all *other* files and directories in the x:\NetworkStationV2 directory again.



Cannot delete nsmgauth: Access is denied.

Make sure the disk is not full or write-protected and that the file is not currently in use.

Figure 469. Cannot delete the nsmgauth file

4. Start `regedit` and delete the following keys:

   From **HKLM\SOFTWARE**:
   IBM\eNetwork On-Demand Server
   IBM\IBM Network Station Manager V2

From **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths:**
enodscfg.exe
Uninstall\eNetwork On-Demand Server
IBM Network Station Manager V2
nsm.exe

From **HKLM\SYSTEM\CurrentControlSet\Services**:
NFSD
nsldv2
PCNFSD
PORTMAP
Tftpd
Timed

From **HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application**:
eNoDInstall
NFSD
NFSSTAT
nsldv2
nsmv2cgi
PCNFSD
TFTPD
TIMED
USRUTIL

5. Click **Control Panel->System**. Click the **Environment** tab, and delete the **LOCPATH** environment variable. Also remove the x:\OnDemand\SERVER\Bin; (at the beginning) and x:\NetworkStationV2\servbase\bin (at the end) statements from the Path variable.
6. Start User Manager for Domains and remove the NSMUser and NSMAdmin groups and the NSM_NFSROOT user ID.
7. Remove the IBM Network Station Manager V2 icon from your desktop (if you had one created during the installation).
8. Reboot your server.
9. Delete the rest of the x:\NetworkStationV2 directory.
10. Delete the eNetwork On-Demand Server and IBM Network Station Manager V2 Start->Programs folders from the All Users profile.
11. Uninstall the prerequisite software: Lotus Domino Go or MS Internet Information Server Web servers.

After these steps, your server should be fairly clean from any Network Station Manager programs and configuration.

Tip

To find Network Station Manager V2 and eNetwork On-Demand Server in the registry, search for OnDemand and Network Station.

Chapter 19. Network Station as a Windows-based terminal

One very common setup for the Network Station is to use it exclusively to access a Windows NT Terminal Server Edition server with Citrix MetaFrame, often referred to as a Windows-Based Terminal (WBT). This chapter guides you through the steps necessary to configure the Network Station as a WBT. We do not go into depth on how the ICA client works, what the download profiles are, how to use NSM, and so on. These topics are covered in other chapters of this redbook. We only give you the necessary steps to set up a Network Station as a WBT. The entire setup takes about an hour.

Before we begin, we make these assumptions:

- We assume that you have a Windows NT Terminal Server Edition server installed with either Citrix MetaFrame or Citrix Device Services (CDS).
- We assume you have created a published application called NTDesktop, which is the entire Windows NT desktop, if you are planning to connect using the published application name. If you want, you can use Citrix Load Balancing and publish this “application” on multiple servers.
- We assume all Network Stations booting from your NSM server will only run the ICA client to connect to your Windows NT Terminal Server Edition-MetaFrame server (therefore, all are setup as WBTs).
- We assume you want to use DHCP.

When setting up kiosk mode, you need to modify one configuration file manually. Since this file is in UNIX format, you should not modify it with a Windows editor such as Notepad. We found that the PFE editor (free from the site `http://www.lancs.ac.uk/people/cpaap/pfe`) works well. This editor is aware of the differences between UNIX and DOS or Windows text file formats.

Here are the steps you need to perform to setup the Network Station as a WBT:

1. Install Network Station Manager V2R1 on a separate Windows NT 4.0 server or your Windows NT Terminal Server Edition server. If you install it on your Windows NT Terminal Server Edition server, remember to first run the `change user /install` command. The prerequisites for NSM V2R1 are Windows NT 4.0 Server (or Windows NT Terminal Server Edition) with Service Pack 4, Microsoft IIS 4.0, or Lotus Domino Go 4.6. When installing the Web server, you can use a *typical* installation.
2. After installing NSM, create one common kiosk file to be used by all your Network Stations. Copy the x$ServBase\defaults\ica.ksk file to $UserBase\profiles and call it allncs.nsm. This file is read by all Network Stations during startup.

   Use the PFE editor (or similar, *not* Notepad) and locate the following line in the file (all on one line):

   ```
   <PROPERTY NAME="desktop_command">nsm_wrapper /usr/lib/ICAClient/wfica -host
   ${SERVER_ADDRESS} -geometry fullscreen</PROPERTY>
   ```

   If you want to run a published application called NTDesktop, modify the line so it reads (all on one line):

   ```
   <PROPERTY NAME="desktop_command">nsm_wrapper /usr/lib/ICAClient/wfica
   -geometry fullscreen -lb -- NTDesktop</PROPERTY>
   ```

Note that there are two dashes (-) and a space before the name NTDesktop (which is case sensitive). The `-lb` parameter stands for load balancing. You should use this even if you have not installed the Citrix Load Balancing services since this causes the ICA client to do a broadcast for the ICA Master Browser server. You don't have to specify it yourself (using the `-host` parameter).

If you only want to connect to a single MetaFrame server or a server running Citrix Device Services (that does not support published applications), modify the line so it reads (all on one line):

```
<PROPERTY NAME="desktop_command">nsm_wrapper /usr/lib/ICAClient/wfica -host
9.24.104.159 -geometry fullscreen</PROPERTY>
```

Here, you replace *9.24.104.159* with the IP address of your MetaFrame server.

3. Launch Network Station Manager using a Web browser. The URL is `http://servername/NetworkStationV2/Admin`

   Logon with a user ID that is a member of the local NSMAdmin group (Administrator is by default). Make sure **System** is selected in the right panel. Then, go to **Hardware->Workstation** in the left panel, and select your keyboard language from the **Keyboard mapping language** drop-down menu. Click the **Save** button at the bottom of the screen when done.

4. Configure your DHCP server with the options shown in Table 88 in *addition to* what you already have in your DHCP server.

Table 88. Additional DHCP options

DHCP option	Value
66	9.24.104.252
67	/NetworkStationV2/prodbase/x86/kernel.2800
211	nfs

Option 66 is the IP address of your NSM server.

Option 67 is the path to the Network Station's kernel file (the operating system). The list in Table 89 describes the values you should use.

Table 89. Path to the Network Station kernel file

Network Station model	Value
S300	/NetworkStationV2/prodbase/ppc/kernel.300
S1000	/NetworkStationV2/prodbase/ppc/kernel.1000
S2200	/NetworkStationV2/prodbase/x86/kernel.2200
S2800	/NetworkStationV2/prodbase/x86/kernel.2800

Option 211 is the protocol to be used when downloading the kernel file. For Windows NT, this should be `nfs`.

Note: If these three options do not exist in your DHCP server (for example, the Microsoft Windows NT 3.51 DHCP server has none of them and the Microsoft Windows NT 4.0 DHCP server has option 66 and 67 only), you must create them manually. They should be of `string` type.

If you do not want to use DHCP, you should configure the corresponding information in the Network Station's NVRAM setup utility.

Note: The pre-release driver we used when writing this did not launch the initial kiosk application borderless, which it should. Therefore, using Alt+F4 closed the ICA client rather than the Windows application in focus. Using Alt+Tab did not switch between Windows applications as Windows users are used to doing. We do not know if this will also be the case when the application runs without borders, or if these keyboard sequences will then be passed to the applications running within the ICA client.

To remedy this problem, we added the lines shown in Figure 470 to our allncs.nsm file. We show the entire file here for your convenience and highlight the added lines.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCREGISTRY SYSTEM "ncregistry.dtd" >
<!-- ICA Sample Profile for Single Application (kiosk) Mode -->
<NCREGISTRY>
<OBJECT NAME="/config">
<CATEGORY NAME="WORKSTATION">
<PROPERTY NAME="xserver-keyboard-type">167</PROPERTY>
</CATEGORY>
</OBJECT>
<OBJECT NAME="/desktop/preferences">
<CATEGORY NAME="DESKTOP">
<PROPERTY NAME="desktop_command">nsm_wrapper /usr/lib/ICAClient/wfica -geometry fullscreen -lb --
NTDesktop</PROPERTY>
<PROPERTY NAME="lock_screen">no</PROPERTY>
<PROPERTY NAME="key_window_kill" TYPE="STRING">nil</PROPERTY>
<PROPERTY NAME="key_window_switch_back" TYPE="STRING">nil</PROPERTY>
<PROPERTY NAME="key_window_switch" TYPE="STRING">nil</PROPERTY>
<PROPERTY NAME="key_window_close" TYPE="STRING">nil</PROPERTY>
<PROPERTY NAME="key_print_screen" TYPE="STRING">nil</PROPERTY>
<PROPERTY NAME="key_print_window" TYPE="STRING">nil</PROPERTY>
</CATEGORY>
</OBJECT>
<OBJECT NAME="/login/session">
<CATEGORY NAME="KIOSK">
<PROPERTY NAME="commands" TYPE="LIST" ACTION="APPEND">
<ELEMENT>
<FIELD NAME="op">SET</FIELD>
<FIELD NAME="arg1">NSM_KIOSK_MODE</FIELD>
<FIELD NAME="arg2">ON</FIELD>
</ELEMENT>
</PROPERTY>
</CATEGORY>
</OBJECT>
</NCREGISTRY>
```

Figure 470. Kiosk file for Network Station as a WBT

As you see, we have unmapped some important keys to pass their keyboard sequences to the Windows applications running within the ICA session. We also set the keyboard language using NSM (which wrote xserver-keyboard-type 167 to the allncs.nsm file).

Now, you are done. Power on your Network Stations, and they should come up in the WBT mode.

If you experience any performance problems with this setup, look at your DNS setup and your local Network Station hosts file (in the x:\{float}\NetworkStationV2\prodbase\{CPU}\etc directory).

Appendix A. File names and paths

Throughout the book, you see file names and paths referred to with a $ notation. The $ sign is intended to be substituted with the path name appropriate for the server platform. For example, if the text refers to $UserBase/home/user1, the actual file name on an AIX server would be /usr/NetworkStationV2/userbase/home/user1.

Table 90 helps you translate, for example, $UserBase, into the actual file or path name for the system on which you are working.

Table 90. Substitute path names

Substitution variables	Value
$ProdBase (AS/400)	/QIBM/ProdData/NetworkStationV2
$HttpBase (AS/400)	/QIBM/ProdData/HTTP/Protect/NetworkStationV2
$ServBase (AS/400)	/QIBM/ProdData/NetworkStationV2/NSM
$UserBase (AS/400)	/QIBM/UserData/NetworkStationV2/
$ProdBase (RS/6000)	/usr/NetworkStationV2/prodbase
$ServBase (RS/6000)	/usr/NetworkStationV2/servbase
$UserBase (RS/6000)	/usr/NetworkStationV2/userbase
$ProdBase (Windows NT)	<float>\NetworkStationV2\prodbase
$ServBase (Windows NT)	<float>\NetworkStationV2\servbase
$UserBase (Windows NT)	<float>\NetworkStationV2\userbase
float> (Windows NT)	Directory where IBM Network Station Manager is installed
<user>	User name from login
<group>	Group name
<ncid>	IBM Network Station host name, IP address, or MAC address
<locale>	Specific locale for cultural conventions
<application>	Application name
<x86|ppc>	Indicates x86 or ppc directory

Appendix B. Native application commands

The commands shown in Table 91 can be issued locally from the Advanced Diagnostic session to start local native applications.

Table 91. Native application commands

Command	Description
`appletviewer [-debug] [-J<javaflag>] [-encoding<character encoding type>] urlfile`	Applet Viewer
`remote_app`	Invoke `rsh` (see UNIX commands in Appendix C, “UNIX commands” on page 613)
`ncedit`	Text Editor
`ncdocmgr`	File Manager
`ncscheduler`	Calendar
`ncpaint`	Paint
`nccalc`	Calculator
`ncaudio`	Audio Player
`ncprmonitor`	Print Monitor
`rvplayer`	RealPlayer
`calibrate`	Touch-screen calibration utility
`helpviewer`	Help viewer
`nsm_wrapper ncxadmin`	Video player
`xterm -sb -sl 1000 -rv`	Advanced diagnostic
`nsm_wrapper wfcmgr`	ICA client
`launchnsm`	Launch NSM R3
`launchnsmv2`	Launch NSM V1R2
`nsm_wrapper nsterm`	VT emulator
`run_netscape`	Netscape browser
`remote_app -window`	Remote program
`nsm_wrapper ns3270`	3270 emulator
`nsm_wrapper ns5250`	5250 emulator
`miscpref3270`	3270 miscellaneous preferences
`miscpref5250`	5250 miscellaneous preferences
`nsmrun app [app...]`	Loads application resources from the NC registry object "/<app>/preferences"
`miscpref_nsterm`	VT emulator miscellaneous preferences
`playedit`	Playback file editor

Command	Description
`keypad`	Keypad customizer
`keymapper`	Keyboard remapping
`startwm`	Start window manager

Appendix C. UNIX commands

Table 92 lists some of the UNIX commands and their general purpose you will find available in the Advanced Diagnostic window. You may find these useful for debugging or application development purposes. The list is not comprehensive, and you may find that some options normally associated with these commands are not available. For general help in these commands, you can refer to the NetBSD man pages found via the NetBSD home page at: `http://www.netbsd.org`

Note: The description may be an over simplification. We only listed the function for which we found each command most useful. Please refer to the NetBSD main Web pages for a complete description of each command and its parameters.

Table 92. UNIX commands

Command	Description
`cat`	Concatenates and prints files. Especially useful for printing a file to the screen (cat *filename*).
`cd`	Changes directory
`chmod`	Changes file modes
`clear`	Clears the terminal screen
`compress, uncompress`	Compresses or decompresses files
`cp`	Copies a file
`date`	Displays the date and time
`df`	Reports information about space on file systems: `df -k` Shows used/free disk space on server
`dmesg`	Displays messages
`domainname`	Displays the name of the current Network Information Service (NIS) domain
`echo`	Shows the value of a variable: `echo $`*variable_name*
`export`	Sets a variable for this session: `export` *variable=value*
`find`	Finds files with a matching expression, for example: find / -name *filename*
`ftp`	File transfer
`grep`	Searches a file for a pattern. For example: `ls	grep ifc` finds all files with the characters "ifc" in the current directory.
`gunzip, zcat`	Compresses or decompresses files
`hostname`	Shows the TCP/IP host name for this station
`id`	Displays the system identification of a specified user

Command	Description
`ifconfig`	Configures and displays network interface parameters. To display the network interfaces (suggested usage): `ifconfig-a`
`iostat`	Reports Central Processing Unit (CPU) statistics and input/output statistics for TTY devices, disks, and CD-ROMS.
`java`	Runs a Java program
`javac`	Compiles a Java program
`kill`	Kills (ends) a process ID
`ksh`	Starts the Korn shell
`ln`	Links files
`lp`	Sends requests to a line printer (invokes lpr with parameters)
`lpr`	Sends output to a printer. For example, to send /etc/hosts to the printer on the TCP4324 queue on workstation 9.24.104.151, enter: `lpr -P9.24.104.151:TCP4324 /etc/hosts`
`ls`	Lists files and directories
`mkdir`	Makes a directory

`mount,`
`(unmount)`
	Makes a file system (assumes nfs) available for use (and removes it from use)

`mv`	Moves a file or files
`netstat`	Shows the network status
`nfsstat`	Displays statistical information about the Network File System (NFS) and Remote Procedure Call (RPC) calls
`ping`	Pings an application (ICMP echo). Check to see if an IP address is reachable.
`ps`	Lists active processes and status
`pstat`	Interprets the contents of the various system tables and writes it to standard output.
`pwd`	Displays current working directory
`rlogin`	Connects a local host with a remote host: rlogin -l *username hostname*
`rm`	Removes directory entries
`rmdir`	Removes a directory
`route`	Modifies or displays the IP routing table. Use `route show` to see the current settings.
`rsh`	Executes the specified command at the remote host or logs into the remote host. For example, to login to a remote host: rsh -l *username hostname*

Command	Description
`tar`	Manipulates archives
`telnet`	Connects the local host with a remote host, using the Telnet interface
`traceroute`	Prints the route that IP packets take to a network host
`uname`	Displays the name of the current operating system
`vi`	Edits a file using the vi editor
`vmstat`	Reports virtual memory statistics
`which`	Locates a program file, including aliases and paths: `which` *filename*

Table 93. UNIX commands

UNIX commands	Use

`ksh`
`set -o vi`
	To set the session up so Esc+k retrieves previous commands

`ksh`
`set -o emacs`
	To use the up and down arrow keys to retrieve previous commands

`command > ~/filename`	Captures output from a command and puts it in your home directory under *filename*.

`mkdir dir1 dir2 dir3`
`rmdir dir1 dir2 dir3`
	Creates and removes multiple directories if specified on the command line:

C.1 Basic terminology

The UNIX interface is much more exposed in the new Network Station operating system. For uninitiated Windows NT users, Table 94 offers few simple comparisons between Windows NT and UNIX.

Table 94. Comparison of NT and UNIX terminology

Windows NT term	UNIX term
Shares	Exports
Uses	Mounts
Uses drive letters: (c:, d:)	Uses /dirname (and is happily unaware of drive partitions)
Uses backslash, c:\dir1\dir2	Uses forwardslash, /dir1/dir2
Is not case sensitive	Is case sensitive
Has a command prompt	Has a shell
Runs services	Runs daemons

Appendix D. User verses administrator configurable settings

This appendix lists all settings available in NSM. All settings listed are available to NSM administrators and all settings in bold are available to NSM users.

D.1 Hardware

- **Workstation**
  - **Mouse Settings:**
    - **Button configuration:**
    - **Pointer speed:**
  - **Keyboard Settings:**
    - **Repeat rate:**
    - **Repeat delay:**
    - Keyboard mapping language:
    - **Num Lock key:**
  - **Monitor Settings:**
    - Preferred monitor resolution:
    - **Minutes before screen saver turns on:**
    - **Screen saver:**
      - **Custom screen saver path:**
      - Minutes before monitor standby:
      - Minutes before monitor suspend:
      - Minutes before monitor power down:
    - **Desktop background:**
      - **Custom background image path:**
      - **Background color**
      - **Foreground color**
    - Color depth:
    - Smooth Character Drawing (anti-aliasing):
  - **Local Services:**
    - **Allow remote X Clients:**
  - Domain Name Server:
    - Update Network Station Manager DNS file
  - Boot Parameters:
    - Language to be used during boot sequence:
    - Enable memory test:
    - Number of times to retry loading operating system:
    - Enable Boot using BOOTP or DHCP:
    - Enable Broadcast boot:
    - Check for Flash Image update:
    - Flash Image directory:
    - Update to boot code installed on the boot server:
  - Workstation Management Settings:
    - Administrator password:
    - Contact person:
    - Workstation location:
    - SNMP Read Community Name:
    - SNMP Read Community Name Alternate:
    - SNMP Read/Write Community Name:
    - SNMP Read/Write Community Name Alternate:

- **Printers**

  - Printer Services
    - Print client (LPR)
      - Maximum LPR buffer size:
    - Print server (LPD)
      - Maximum LPD buffer size:
      - Bypass print buffer when file exceeds buffer size:
    - Remote systems allowed to print on this workstation:
  - Printer List
    - Local parallel printer
    - Local serial printer
    - Remote printer server

- **Serial Devices**

  - Serial Device Services
    - Remote systems allowed to use these devices (Seriald):
  - Other Serial Devices
    - Port number
    - Mode
    - Baud rate
    - [Advanced]
      - Data bits
      - Stop bits
      - Parity
      - Error flow
      - Hangup
      - TCP/IP port
      - Use serial protocol

D.2 Applications

- **5250**

  - Keyboard mapping:
    - Key remapping capability:
    - Default keyboard files:
  - Keypad:
    - Keypad capability:
    - Keypads to make available:
  - Record/Playback:
    - Record/Playback capability:
    - Playback sequences to make available:
  - Colors:
    - Color customization capability:
    - Default color scheme:
    - Additional color schemes to make available:
  - **Appearance:**
    - **Screen size:**
    - Image/Fax display:
    - **Column separators:**
    - Desktop file:

Allow use of:
  Command menu:
  Edit menu:
  Option menu:
  Print menu:
  Help menu:
  Control menu:
  Miscellaneous preferences:
  Font menu list:
  New session window:
  Browser hotspot:
Additional parameters:

- **3270**

Keyboard mapping:
  Key remapping capability:
  Default keyboard files:
Keypad:
  Keypad capability:
  Keypads to make available:
Record/Playback:
  Record/Playback capability:
  Playback sequences to make available:
Colors:
  Color customization capability:
  Default color scheme:
  Additional color schemes to make available:
Appearance:
  Screen size:
  Telnet 3270 port to connect to:
  Key for Enter function:
  Desktop file:
Allow use of:
  Command menu:
  Edit menu:
  Option menu:
  Print menu:
  Help menu:
  Graphics:
  Miscellaneous preferences:
  Font menu list:
  New session window:
  Browser hotspot:
Additional parameters:

- **VT Emulator**

Keyboard:
  Key remapping capability:
  Default keyboard files:
Allow use of:
  Command menu:
  Edit menu:
  Option menu:

    - Print menu:
    - Help menu:
    - Control menu:
    - Miscellaneous preferences:
    - Font menu list:
  - Advanced settings:
    - Use Latin character set:
    - Eight bit input enable:
    - Eight bit emit enable:
    - Vertical scrollbar:
    - Start debug log:
    - Lines to save in buffer:
  - Additional parameters:

- **Netscape Communicator**
  - Proxy configuration:
  - Java:
    - Enable Java Applets:
    - Runtime Plug-in for Network Station, Java Edition:
  - Network:
    - Maximum memory cache:
  - Mail server type:
  - Netscape Java Classpath options:
  - Garbage collection:
  - Memory settings:
    - Maximum heap
    - Java stack size:
    - Native code stack size:
  - Properties (optional):

- **Applet Viewer**
  - Applet Viewer Java Classpath options:
    - Applet Viewer Java Classpath:
    - User classpath:
    - Verify classes:
  - Garbage collection:
  - Memory settings:
    - Maximum heap size:
    - Java stack size:
    - Native code stack size:
  - Properties (optional):

- **ICA Remote Application Manager**

D.3 Desktop

- **Display**
  - **Window appearance**
    - **Desktop theme:**
      - **Custom:**
    - **Icon location:**
    - **Constrained mode:**

    - **Enable desktop pop-up:**
  - **Launch bar options**
    - **Show memory meter:**
    - **Collapsed:**
  - **Fonts**
    - **Font size for icons and menus:**
    - **Enable web palette colors:**
  - Desktop buttons
    - Show Exit button:
    - Show Lock button:
    - Show Help button:

Launch Bar

D.4 Environment

- **General**
- **Network**

  - Personal
    - User's name:
    - EMail address:
    - Reply to address:
    - Home page:
  - Proxies:
    - FTP
    - HTTP
    - GOPHER
    - Security
    - SOCKS
  - Proxy exceptions
    - No FTP proxy for:
    - No HTTP proxy for:
    - No GOPHER proxy for:
  - Mail and News servers
    - Outgoing mail (SMTP) server:
    - Incoming mail (POP3) server:
    - News (NNTP) server:
  - Ports
    - Web server port on the boot host:
    - Applet launcher port:
  - Additional mount points
    - Mount point 1
      - Mount type:
      - Server address:
      - Remote mount point:
      - Local mount point:
      - Read blocksize:
      - Write blocksize:
      - Access permissions
    - Mount point 2
      - Mount type:
      - Server address:

Remote mount point:
Local mount point:
Read blocksize:
Write blocksize:
Access permissions

Mount point 3
Mount type:
Server address:
Remote mount point:
Local mount point:
Read blocksize:
Write blocksize:
Access permissions

Mount point 4
Mount type:
Server address:
Remote mount point:
Local mount point:
Read blocksize:
Write blocksize:
Access permissions

Mount point 5
Mount type:
Server address:
Remote mount point:
Local mount point:
Read blocksize:
Write blocksize:
Access permissions

- **Language**

D.5 Administration

User’s group
Group for this user:

Flash Manager

Appendix E. Keyboard shortcuts

We have outlined the various keyboard shortcuts for you in Table 95.

Table 95. Keyboard shortcuts

Shortcut	Action
Alt + F4	Closes the active window
Alt + Space	Displays the menu for the active window
Alt + F10	Activates the desktop menu
Ctrl + Alt + L	Displays who is logged into the Network Station
Alt + F10 + x	Logs you off the Network Station
Ctrl + Alt + V	Displays the Network Station desktop build date
Ctrl + Alt + I	Displays the root file system, host name, and domain name
Ctrl + Alt + Backspace	Displays logoff dialog
Alt + Shift + PrintScreen	Stores a screen capture of the entire Network Station screen in a .bmp file in \NetworkStationV2\userbase\home\{userid}\registry\documents.
Alt + Shift + ScrollLock	Captures the active window and stores it in a bitmap (.bmp) file in \NetworkStationV2\userbase\home\{userid}\registry\documents.
Ctrl + Left mouse button while in advanced diagnostics	Menu of options
Ctrl + Right mouse button while in advanced diagnostics	Font menu
Alt + Tab	Gives you a menu of open windows. Each Tab while holding the Alt key, cycles you through the menu to each window.
Drag left mouse over a string and hit the right mouse (while still holding the left)	Choose any string from the window and paste it back to the command line. Each right-click places another instance of the string. A double-click selects a word and if you hold the second click, hit the right mouse button to copy. It seems that anything that is highlighted (single character, word, line, multiple lines, etc) is copied each time that you right-click. If the selection is on or more line, it seems to even copy and press Enter as well.

Appendix F. Boot monitor service aid menu

The following structure shows the different functions that are now available through the boot monitor service aids menus.

- 1.Memory Test
- 2.Dump PCI Configuration Register to serial port
- 3.Cache Control
  - 1.Enable L1 cache
  - 2.Enable L1 & L2 cache
  - 3.Disable L1 & L2 cache
  - 4.Enable L2 cache
  - 5.Disable L2 cache
  - 0.Exit
- 4.Video Test
- 5.Test all
- 6.I/O (Serial and parallel)
  - 1.Wrap Serial 2
  - 2.Wrap parallel
  - 0.Exit
- 7.Toggle auto test
- 8.Configuration menu
  - 1.Set MAC address
  - 2.Debug mode
  - 3.Network adapter info
  - 4.Change blocksize
    - 1.Change to default 4096
    - 2.Change
    - o.Exit
  - 5.Display shadow NVRAM
  - 6.Change MTU size (TRN)
    - 1.Change to default 1492
    - 2.Change
    - 0.Exit
  - 7.Select keyboard language
  - 8.OS Boot selection
    - WSOD
    - Other
    - Auto
  - 9.TFTP subnet broadcast enable
  - 0.Exit
- 9.Misc menu
  - 1.Audio
    - 1.Beep with time
    - 2.Output sine to CODEC
    - 0.Exit
  - 2.SMBus
    - 1.Write normal mode settings to system clock
    - 2.Write POR settings to system clock
    - 3.Test SMBUS without writing to seeproms
    - 0.Exit
  - 3.Badger menu
  - 4.

  - 5.
  - 6.Network Menus
    - MENU 1
    - 1.Print ARP cache
    - 2.Print routing table
    - 3.Print boot configuration
    - 4.Print card statistics
    - 5.Print network statistics
    - 6.Packet log
    - 7.Bootp vendor specific/DHCP options
    - 8.DHCP responses
    - 9.More network menus=>MENU 2
    - 0.Exit
    - MENU 2
    - 1.Print Ethernet EEPROM data
    - 2.Display/set EThernet Auto Negotiate/Speed/duplex
    - 3.Ping command
    - 4.Duplicate network packets
    - 5.Host command
    - 6.Display/set TRN auto selection/speed selection
    - 7.Display subnet broadcast information
    - 8.Display subnet broadcast bitmap
    - 9.More network menus=>MENU 3
    - 0.Exit
    - MENU 3
    - 1.RPL Server discover
    - 2.Display/set boot protocol
    - 3.TFTP subnet boot protocol retry count
    - 4.TFTP retry and delay values
    - 5.NFS retry and delay values
    - 6.Menu interruption (Alt PF9)
    - 0.Exit
  - 7.Compact Flash
    - 1.Dump drive ID info
    - 2.Execute diagnostic
    - 3.Read compact flash
    - 4.Write compact flash
    - 0.Exit
  - 8.NVRAM
    - 1.Reset
    - 2.Display
    - 0.Exit
  - 9.Display memory
  - 0.Exit
- 0.Exit

Appendix G. Differences between NSM V1R3 and V2R1

This appendix identifies the differences that exist between the last release of Network Station Manager (V1R3) and this new V2R1 release. It is meant for users who were already familiar with the previous version, need to find out quickly how to perform functions similar to what they were used to in the previous release. For example, in V1R3, you could see the console messages by bringing up the console and clicking on Messages. What is the equivalent function in V2R1?

Because this is intended to be a quick reference list, we do not provide a lot of details on the new functions or on the new way of performing certain actions. Instead, we only provide a summary. Other parts of this document provide the detailed information.

Using a table format, we compare the V1R3 function and action with the V2R1 function and action. Table 96 identifies the most commonly used functions.

Table 96. Common tasks: V1R3 and V2R1 differences

Function	NSM V1R3	NSM V2R1
Display Messages	Use Console Messages. Automatically updated.	Use the `dmesg` command from the Advanced Diagnostics window. Not automatically updated
Retrieve Console Messages Remotely	Telnet to port 5998 of the station	Telnet into the station (no special port required and use the `dmesg` command
Execute a command remotely	Use `rsh` to the station	Telnet into the station and use the `dmesg` command on the command line
Access Configuration daemon remotely	Telnet to port 5999 of the station	Not available
Access Configuration dameon locally	Use the setup menu from the Console	Not available
Reset NVRAM	Use the nv command on the boot monitor command line	Select Load Factory Defaults from the Boot Monitor Service Aids Menu or Misc/NVRAM/Reset
Ping	Ping utility from the Console/Utilities	Use the `ping` command from the command line. Use Ctrl-C to stop. Can also use arp, traceroute, telnet, route, ifconfig, and netstat.
Start a telnet session	Terminal pulldown from console	Use `Telnet` from the command line
Information on version, MAC address, etc.	Show Version from the console	Ctrl+Alt+I gives is somewhat equivalent. Provides IP address, MAC, boot server address, and root file system
Check Free Memory	Show Memory from the console	Click on colored dots at the top of the launch bar. Colors, from green to red, indicate the status.

Table 97 identifies other common functions.

Table 97. Other common functions: V1R3 and V2R1 differences

Function	NSM V1R3	NSM V2R1
Display boot messages	Turn on verbose mode in boot monitor menu	Display Boot Log from main Boot Monitor Menu
Enable remote X clients	Use NSM configuration - Hardware/Workstation/Local Services	Same
Set Unit Global Password	Use NSM configuration	Same
Lock the screen	Screen Lock from the console utilities	From Desktop - Uses current session password automatically
File Extended Diagnostics	Turn on from the setup menu on the console	Not available
Display file system	Use console/setup to display the File Service Table	Use the Display File System (`df`) command.
Add mount points	Configure the File Service Table	Use NSM/Environment/Network and define additional mount points
Set time zone variable	Use NSM	Same
Display environment variables	Use Console/Setup/Preferences	Use set on the command line
Display statistics	Use console/statistics	Use the commands iostat, netstat, nfsstat, pstat, and vmstat
Display Connections	Console/Show Connections	netstat -n
Display IP routing table	Console/Setup	Use the `netstat -r` command.
Display current mounts	Display the file service table	Use the `mount` command with no options
Display the date/time		Use the `date` command

Appendix H. NCP-MIB Version 1 definition file

This appendix shows you the information that is kept in the NCP MIB version 1 definition file so that you can better understand it.

```
-- automatically generated by mosy 7.2 #166 (yukinojo), do not edit!

NCP-MIB DEFINITIONS ::= BEGIN

IMPORTS
    TruthValue
        FROM RFC1253-MIB
    TRAP-TYPE
        FROM RFC-1215
    DisplayString
        FROM RFC1213-MIB
    OBJECT-TYPE
        FROM RFC-1212
    TimeTicks, Gauge, IpAddress, enterprises
        FROM RFC1155-SMI
    Utf8String
        FROM SYSAPPL-MIB
    TDomain, DateAndTime
        FROM SNMPv2-TC;

opengroup OBJECT IDENTIFIER ::= { enterprises  4396 }

-- created from ncMIB (9804200000Z)

ncMIB OBJECT IDENTIFIER ::= { opengroup  1 }

NcpLocale ::=
    OCTET STRING

ncNotifications OBJECT IDENTIFIER ::= { ncMIB  1 }

ncObjects OBJECT IDENTIFIER ::= { ncMIB  2 }

ncConformance OBJECT IDENTIFIER ::= { ncMIB  3 }

ncSystem OBJECT IDENTIFIER ::= { ncObjects  1 }

ncSysMibVersion OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "The value of LAST-UPDATED from this module's MODULE-IDENTITY
       macro, preceded by a leading '19' or '20' to yield a four-digit
       year.  This object gives a Management Station an easy way of
       determining the level of the MIB supported by an agent."
    ::= { ncSystem  1 }

ncSysUuid OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "The UUID/GUID value for the system if one is available.  The
       zero-length string is returned if the system does not have a
        UUID/GUID value."
    REFERENCE
           "INTERNET-DRAFT, UUIDs and GUIDs [7]"
    ::= { ncSystem  2 }

ncSysMacAddress OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Hardware ('burned-in') MAC address assigned by the
        manufacturer.  Note this value is not necessarily
        the same as any logical MAC addresses in use as
        instrumented by ifPhysAddress in MIB-II; even if the system
        has a burned in address, an administrator may assign a
        different MAC address to the system that would be used
        as the logical MAC address in ifPhysAddress.
        The zero-length string is returned if the system does not
        have a hardware MAC address.
        A non-zero-length string must be returned by systems which
        do not support UUID/GUID."
    ::= { ncSystem  3 }

ncSysSerialNum OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "System hardware serial number (in a manufacturer-specific
        format).  Some manufacturers may choose to substitute the
        system MAC address when a serial number is not available."
    ::= { ncSystem  4 }

ncSysManuf OBJECT-TYPE
    SYNTAX  Utf8String
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Manufacturer of the system hardware."
    ::= { ncSystem  5 }

ncSysManufContact OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Contact information for the manufacturer of the system.
        The information can be a phone number, a URL, or another
        type of contact information. The zero-length string indicates
        that this information and support are not available."
    ::= { ncSystem  6 }

ncSysModelId OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "System hardware model identifier (vendor-specific)."
    ::= { ncSystem  7 }

ncSysModelVersion OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "System hardware model version (vendor-specific)."
    ::= { ncSystem  8 }

ncSysMemTotal OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS kilobytes
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Physical size of system memory, in kilobytes."
    ::= { ncSystem  9 }

ncSysProcessorType OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Processor type. Vendor specific"
    ::= { ncSystem  10 }

ncSysProcessorVersionInfo OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Processor version information. Vendor specific"
    ::= { ncSystem  11 }

ncSysProcessorMaxSpeed OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS megahertz
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Maximum processor speed (frequency in MHz)."
    ::= { ncSystem  12 }

ncSysProcessorL2CacheSize OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS kilobytes
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Size of processor level 2 cache in kilobytes."
    ::= { ncSystem  13 }

ncSysKeyboardType OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Identification of the keyboard type attached.  The string is
        vendor-unique.
        The zero-length string indicates that this information is
       not available to the SNMP agent.  The value 'none'
       indicates that there is no attached keyboard."
    ::= { ncSystem  14 }

ncSysKeyboardLangId OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Keyboard language identifier, using a two-character
        identifier from ISO 639/2.
        The zero-length string indicates that this information is
        not available to the SNMP agent.  The value 'none' is
        returned if there is no attached keyboard."
    ::= { ncSystem  15 }

ncSysVideoMemorySize OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS kilobytes
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Video memory size, in kilobytes."
    ::= { ncSystem  16 }

ncSysVideoMinRefresh OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS Hertz
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Minimum refresh rate supported by the
        video subsystem of the network computer."
    ::= { ncSystem  17 }

ncSysVideoMaxRefresh OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS Hertz
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Maximum refresh rate supported by the
        video subsystem of the network computer."
    ::= { ncSystem  18 }

ncSysSmartCardReaderId OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Smart card reader identifier.
        The zero-length string indicates that this information is
        not available to the SNMP agent. The value 'none' that there
        is no attached smart card reader. Any other non-zero length
        string is vendor unique."
    ::= { ncSystem  19 }

ncSysAssetID OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Asset identifier assigned by an administrator.
        The value of this object should be persistent across power
        off/on cycles. The value assigned by the administrator is
        unique to the management environment. The mechanism for
        assigning the identifier is unique to the implementation."
    ::= { ncSystem  20 }

ncSysReconfigRequested OBJECT-TYPE
    SYNTAX  INTEGER {
                 none(0),
                 reconfigure(1)
               }
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
       "Indicator that the SNMP agent should reconfigure itself
        by reloading the configuration information provided by
        the NCMP configuration service"
    ::= { ncSystem  21 }

ncSysPointingDeviceType OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Indicate type of pointing device attached, including the
        number of buttons on the device.
        The zero-length string indicates that this information is
        not available to the SNMP agent. The value 'none' that there
        is no attached pointing device. Any other non-zero length
        string is vendor unique."
    ::= { ncSystem  22 }

ncSysPowerManType OBJECT-TYPE
    SYNTAX  INTEGER {
                 other(1),
                 unknown(2),
                 apm-1-1(3),
                 apm-1-2(4),
                 acpi-1-0(5)
               }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
          "Defines what type of Power Management this system supports                  (i.e.,
APM 1.2, ACPI 1.0)"
    ::= { ncSystem  23 }

ncSysPowerManEvent OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Indicates system able to resume operation when a modem ring
        occurs on a serial port or a wakeup occurs on a LAN Card"
    ::= { ncSystem  24 }

ncSysPersistentStorageSize OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS kilobytes
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "Persistent storage size in kilobytes. This should be set to
         zero (0) if there is no persistent storage."
    ::= { ncSystem  25 }

ncSystemStartup OBJECT IDENTIFIER ::= { ncObjects  2 }

ncSysStartupOsBootServer OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "IP address of the system that served the operating system
        image at the most recent system startup. Note: this address can
        identify the local system if the system has a local
        persistent cache to store an OS image."
    ::= { ncSystemStartup  1 }

ncSysStartupOsImageServer OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "IP address of the system that served the operating system
        image the last time the image was updated.  Note:  the value
        returned by this object is different from the value of
        ncSysStartupOsBootServer only if the NC has a local persistent
        cache to store an OS image."
    ::= { ncSystemStartup  2 }

ncSysStartupOsUpdateTime OBJECT-TYPE
    SYNTAX  DateAndTime
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Date/time of the last OS update.  Note:  the value returned
        by this object is different from boot time (derivable
        from sysUpTime) only if the NC has a local persistent cache
        to store an OS image. If an NC cannot determine the time of
        the last OS update, this should be set to zero."
    ::= { ncSystemStartup  3 }

ncSysStartupOsId OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Operating system software name."
    ::= { ncSystemStartup  4 }

ncSysStartupOsVersion OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Operating system software version identification."
    ::= { ncSystemStartup  5 }

ncSysStartupOsLocale OBJECT-TYPE
    SYNTAX  NcpLocale
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Locale configured for operating system."
    ::= { ncSystemStartup  6 }

ncSysStartupBootSoftwareServer OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "IP address of the system that last updated boot software
        (aka BIOS).
        The address ff:ff:ff:ff indicates that no boot
        software update has occurred, or that it is not possible
        to determine if an update has occurred."
    ::= { ncSystemStartup  7 }

ncSysStartupBootSoftwareUpdateTime OBJECT-TYPE
    SYNTAX  DateAndTime
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Date/time of last boot software (aka BIOS)update.
        The value 00000000 is returned if no boot software
        update has occurred , or that it is not possible
        to determine if an update has occurred."
    ::= { ncSystemStartup  8 }

ncSysStartupBootSoftwareManuf OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Boot software (aka BIOS) manufacturer name.  On some systems
        the boot software is implemented by a BIOS ROM."
    ::= { ncSystemStartup  9 }

ncSysStartupBootSoftwareId OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "Boot software (aka BIOS) version identification information
       (vendor-specific)."
    ::= { ncSystemStartup  10 }

ncSysStartupBootSoftwareRelDate OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Release date of boot software (aka BIOS).
        Date is in the form dd/mm/yyyy."
    ::= { ncSystemStartup  11 }

ncSysStartupBootSoftwareSize OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS kilobytes
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Physical size of boot software (aka BIOS) in kilobytes."
    ::= { ncSystemStartup  12 }

ncSysStartupBootLocale OBJECT-TYPE
    SYNTAX  NcpLocale
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
         "Locale configured for boot software (aka BIOS), i.e., the
          startup language for the system."
    ::= { ncSystemStartup  13 }

ncSysStartupIpAddrSource OBJECT-TYPE
    SYNTAX  INTEGER {
                 other(0),
                 dhcp(1),
                 bootp(2),
                 ppp-ipcp(3),
                 manual(4)
               }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Source of the IP address assigned to this device. It can be
            other (0)    - information unavailable or other than
                           one of the specific values
            DHCP(1)      - DCHP
            BOOTP (2)    - BOOTP
            PPP/IPCP (3) - PPP/IPCP
            manual (4)   - manually entered by user, or from persistent
                           storage in the device
           "
    ::= { ncSystemStartup  14 }

ncSysStartupIpAddrServer OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "IP address of the server of the IP address assigned to this
        device. Zero if assigned manually."
    ::= { ncSystemStartup  15 }

ncSysStartupConfigServer OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "IP address of the system that provided the initial
```

```
        configuration for this NC."
    ::= { ncSystemStartup  16 }

ncSystemStatus OBJECT IDENTIFIER ::= { ncObjects  3 }

ncSysStatusIdleTime OBJECT-TYPE
    SYNTAX  TimeTicks   -- UNITS hundredths of a second
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Total amount of time the system CPU has been idle since
        system startup."
    ::= { ncSystemStatus  1 }

ncSysStatusVitalState OBJECT-TYPE
    SYNTAX  INTEGER {
                 none(1),
                 restart-requested(2),
                 powerdown-requested(3),
                 poweroff-requested(4),
                 restart-forced(5),
                 powerdown-forced(6),
                 poweroff-forced(7)
               }
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
       "Vital state of the system as requested or forced remotely
        (SNMP SET).
        For a 'request,' when no user is logged on the
        state change will take effect immediately; otherwise it
        will take effect only after the user logs off.  It is an
        implementation-specific matter as to whether a user is
        presented with a dialog requesting the user to log off
        so the state change may take effect.  The value set
        for this object persists until it is changed by another
        SET or it is reset to none(1) by a forced system vital state
        change, or the user logs off causing the request to be
        processed.
        For a 'force,' the state change is mandatory and processing
        begins immediately regardless of whether a user is logged on.
        Processing of the state change may include implementation-
        specific processing including a warning message to the user
        (if logged on), a waiting period before commencing the actual
        state change, etc.
          none(1)             - No state change is requested
          restart requested(2)- System restart requested remotely.
                                   The system will be restarted (coldstart
                                reboot such as after a power-on)
                                when the request is processed.
           powerDown requested(3)- System power down requested remotely.
                                  The system will be powered down when
                                  the request is processed.
           powerOff requested(4) - System power off requested remotely.
                                  The system will be powered off when
                                  the request is processed.

          restart forced(5) - System restart requested remotely.
                              The system will be restarted (coldstart
                              reboot such as after a power-on)
                              when the request is processed.
          powerDown forced(6) - System power down requested remotely.
                                The system will be powered down when
                                the request is processed.
          powerOff forced(7)  - System power off requested remotely.
                                The system will be powered off when
                                the request is processed.
        "
    ::= { ncSystemStatus  2 }

ncSysStatusProcessorCurSpeed OBJECT-TYPE
    SYNTAX  Gauge       -- UNITS megahertz
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Current processor speed (frequency in MHz)."
    ::= { ncSystemStatus  5 }
```

```
ncSysStatusVideoCurHor OBJECT-TYPE
    SYNTAX  Gauge
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Current number of horizontal pixels used by the
        video subsystem of the network computer."
    ::= { ncSystemStatus  6 }

ncSysStatusVideoCurVert OBJECT-TYPE
    SYNTAX  Gauge
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Current number of vertical pixels used by the
        video subsystem of the network computer."
    ::= { ncSystemStatus  7 }

ncSysStatusVideoCurRefreshRate OBJECT-TYPE
    SYNTAX  Gauge        -- UNITS Hertz
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Current refresh rate (in Hz) used by the
        video subsystem of the network computer."
    ::= { ncSystemStatus  8 }

ncSysStatusVideoCurBitsPerPixel OBJECT-TYPE
    SYNTAX  Gauge
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Current number of bits per pixel used by the
        video subsystem of the network computer."
    ::= { ncSystemStatus  9 }

ncSysStatusDateTime OBJECT-TYPE
    SYNTAX  DateAndTime
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Current date and time for this network computer."
    ::= { ncSystemStatus  10 }

ncSysStatusPersistentStorageUsed OBJECT-TYPE
    SYNTAX  Gauge
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "Indicates amount of persistent storage used."
    ::= { ncSystemStatus  11 }

ncUserStatus OBJECT IDENTIFIER ::= { ncObjects  4 }

ncUserName OBJECT-TYPE
    SYNTAX  Utf8String
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "The name of the user who last logged on. For security
        reasons, this should be set to 'null' when a user logs off."
    ::= { ncUserStatus  1 }

ncUserAuthServer OBJECT-TYPE
    SYNTAX  IpAddress
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "IP address of the most recent user's primary
       authentication server."
    ::= { ncUserStatus  2 }

ncUserLogonTime OBJECT-TYPE
    SYNTAX  DateAndTime
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Date/time of most recent user logon since system startup.
```

```
        The value 00000000 indicates that no user has logged on
        since system startup."
    ::= { ncUserStatus  3 }

ncUserLogoffTime OBJECT-TYPE
    SYNTAX  DateAndTime
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Date/time of most recent user logoff since system startup.
        The value 00000000 indicates that no user has logged off
        since system startup."
    ::= { ncUserStatus  4 }

ncAlertObjects OBJECT IDENTIFIER ::= { ncObjects  5 }

ncAlertConfig OBJECT IDENTIFIER ::= { ncAlertObjects  1 }

ncAlertTableMaxSize OBJECT-TYPE
    SYNTAX  Gauge
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Maximum number of entries in the alert table.  Once the
        maximum number has been reached, the oldest entry is
        deleted whenever a new entry is added. "
    ::= { ncAlertConfig  1 }

ncAlertTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF NcpAlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
       "A table containing alerts.  Table is empty at system
        startup.  Entries are added to the table as alerts occur,
        until ncAlertTableMaxSize is reached.  Thereafter the
        oldest entry in the table is removed each time a new
        alert is added.  Alerts may include system health events,
        system faults, authentication failures for power off and
        system restart requests, etc."
    ::= { ncAlertObjects  2 }

ncAlertEntry OBJECT-TYPE
    SYNTAX  NcpAlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
       "An entry in the alert table, reporting information
        related to a single alert."
    INDEX   { ncAlertIndex }
    ::= { ncAlertTable  1 }

NcpAlertEntry ::=
    SEQUENCE {
        ncAlertIndex
            Gauge,

        ncAlertType
            INTEGER,

        ncAlertSeverity
            INTEGER,

        ncAlertMessage
            DisplayString,

        ncAlertTimestamp
            DateAndTime
    }

ncAlertIndex OBJECT-TYPE
    SYNTAX  Gauge
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
       "Index that uniquely identifies an entry in the
        alert table.  Index values should not be reused
        between system restarts."
    ::= { ncAlertEntry  1 }

ncAlertType OBJECT-TYPE
    SYNTAX  INTEGER {
                 other(1),
                 diagnosticFailure(2),
                 hardwareFailure(3),
                 impendingDeviceFailure(4),
                 bootError(5),
                 osError(6),
                 commandAuthFailure(7),
                 remotePowerOffRequested(8),
                 remotePowerDownRequested(9),
                 remoteRestartRequested(10),
                 remotePowerOffForced(11),
                 remotePowerDownForced(12),
                 remoteRestartForced(13),
                 remotePowerUpProcessed(14),
                 remotePowerOffProcessed(15),
                 remotePowerDownProcessed(16),
                 remoteRestartProcessed(17),
                 userLogon(18),
                 userLogoff(19)
               }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Type of alert.  The following values are defined:

         other(1)                  - none of the specific alert
                                       types listed below
         diagnosticFailure(2)      - e.g., error detected during
                                       device power-on diagnostics
         hardwareFailure(3)        - hardware failure detected
         impendingDeviceFailure(4) - e.g., hard disk predicted failure
         bootError(5)              - error during boot process
         osError(6)                - operating system error
         commandAuthFailure(7)     - remote command requester failed
                                     authentication
                                       (alert message contains requester
                                     address)
          remotePowerOffRequested(8) - remote power off command accepted
                                       (alert message contains requester
                                     address)
          remotePowerDownRequested(9)- remote power down (low power)
                                       command accepted
                                           (alert message contains requester
                                       address)
          remoteRestartRequested(10) - remote restart command accepted
                                           (alert message contains requester
                                       address)
          remotePowerOffForced(11)   - forced power off command accepted
                                          (alert message contains requester
                                       address)
          remotePowerDownForced(12)  - forced power down (low power)
                                       command accepted
                                           (alert message contains requester
                                       address)
          remoteRestartForced(13)    - forced restart command accepted
                                           (alert message contains requester
                                       address)
          remotePowerUpProcessed(14) - remote power up command processed
                                          (alert message contains requester
                                      address)
          remotePowerOffProcessed(15)- remote power off command processed
                                         (alert message contains requester
                                      address)
         remotePowerDownProcessed(16)- remote power down (low power)
                                       command received
                                           (alert message contains requester
                                       address)
          remoteRestartProcessed(17) - remote restart command processed
                                          (alert message contains requester
                                      address)
         userLogon(18)            - user logged on (alert message
                                    contains user name and IP address
                                    of authentication server)
         userLogoff(19)           - user logged off (alert message
                                    contains user name and IP address
                                    of authentication server)
      "
    ::= { ncAlertEntry  2 }

ncAlertSeverity OBJECT-TYPE
    SYNTAX  INTEGER {
                 unknown(1),
                 monitor(2),
                 information(3),
                 ok(4),
                 nonCritical(5),
                 critical(6),
                 nonRecoverable(7)
               }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Severity of alert.  The following values are defined:

          unknown(1)         - unknown severity
          monitor(2)         - monitor information
          information(3)     - informational
          ok(4)              - ok
          nonCritical(5)     - non-critical
          critical(6)        - critical
          nonRecoverable(7)  - non-recoverable
          "
    ::= { ncAlertEntry  3 }

ncAlertMessage OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Alert message containing details about the event
        that occurred.  Contents vary depending on alert type
        and on vendor."
    ::= { ncAlertEntry  4 }

ncAlertTimestamp OBJECT-TYPE
    SYNTAX  DateAndTime
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Date/time the alert occurred."
    ::= { ncAlertEntry  5 }

ncTrapControl OBJECT IDENTIFIER ::= { ncObjects  6 }

ncTrapAlerts OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Object controlling whether a trap is to be sent for
        each alert."
    ::= { ncTrapControl  1 }

ncTrapUserStateChange OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Object controlling whether a trap is to be sent for
        any user state change event. User logon and logoff
        always generate alerts, and any alert generates a
        trap if ncTrapAlerts is true. This object can be used to
         prevent or allow additional traps specific to the user events."
    ::= { ncTrapControl  2 }

ncTrapUserLogon OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "Object controlling whether a trap is to be sent for
       each user logon event. ncTrapUserStateChange must be true
       for a trap to be sent."
    ::= { ncTrapControl  3 }

ncTrapUserLogoff OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "Object controlling whether a trap is to be sent for
       each user logoff event. ncTrapUserStateChange must be true
       for a trap to be sent."
    ::= { ncTrapControl  4 }

ncTrapSystemStatusGroupUpdate OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "Object controlling whether a trap is to be sent for
       each system status group update event."
    ::= { ncTrapControl  5 }

ncTrapVitalStateChange OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "Object controlling whether a trap is to be sent for
       each remote vital state change alert (remotePowerUp,
       remotePowerOff, remotePowerDown, and remoteRestart),
       whether the result of a requested or a forced change.
       This object and ncTrapAlerts must both be true for
       such traps to be sent."
    ::= { ncTrapControl  6 }

ncTrapBroadcast OBJECT-TYPE
    SYNTAX  TruthValue
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
       "Object controlling whether traps are broadcast or unicast.
        When 'true' all traps are broadcast. When false, traps are
        sent to the list of addresses in the trap target list."
    ::= { ncTrapControl  7 }

ncAlert TRAP-TYPE
    ENTERPRISE  ncNotifications
    VARIABLES   {
                 ncAlertType,
                 ncAlertSeverity,
                 ncAlertMessage,
                 ncAlertTimestamp
               }
    DESCRIPTION
      "Alert for system health and fault monitoring."
    ::= 1

ncUserLogon TRAP-TYPE
    ENTERPRISE  ncNotifications
    VARIABLES   {
                 ncUserName,
                 ncUserLogonTime,
                 ncUserAuthServer
               }
    DESCRIPTION
       "Notification that a user has logged on."
    ::= 2

ncUserLogoff TRAP-TYPE
    ENTERPRISE  ncNotifications
    VARIABLES   {
                 ncUserName,
                 ncUserLogoffTime,
                 ncUserAuthServer
               }
    DESCRIPTION
       "Notification that a user has logged off."
    ::= 3
```

```
ncSystemStatusGroupUpdate TRAP-TYPE
    ENTERPRISE  ncNotifications
    VARIABLES   { ncSysStatusLastChangeTime }
    DESCRIPTION
      "Notification that a change has occurred in the value
       of one or more objects in the system group.  This
       notification shall not be emitted more than once per
       minute."
    ::= 4

ncCompliances OBJECT IDENTIFIER ::= { ncConformance  1 }

ncGroups OBJECT IDENTIFIER ::= { ncConformance  2 }

ncCompliance OBJECT IDENTIFIER ::= { ncCompliances  1 }

ncSystemConfGroup OBJECT IDENTIFIER ::= { ncGroups  1 }

ncUserStatusConfGroup OBJECT IDENTIFIER ::= { ncGroups  2 }

ncAlertConfGroup OBJECT IDENTIFIER ::= { ncGroups  3 }

ncTrapControlConfGroup OBJECT IDENTIFIER ::= { ncGroups  4 }

ncTrapsNotifGroup OBJECT IDENTIFIER ::= { ncGroups  5 }

END
```

Appendix I. V2R1 memory requirements and network load

To download the latest document to help you determine the memory requirements and network traffic utilization, follow these steps:

1. Go to `http://www.ibm.com/nc`
2. Select your country.
3. Once inside the IBM Network Station home page, select **Support**. Then select **Online Publications** to find the document entitled *NSM V2R1 - Memory requirements and performance recommendations*. Download and view or print this document.

   It offers you help in determining basic main memory and flash memory footprint sizing. It uses “worst case” simultaneous booting scenarios (against real-world staggered booting) for Windows NT and AS/400 boot servers to identify boot time and performance bottlenecks to help you plan for increase boot performance and set performance expectations.

In summary, V2R1 delivers significant enhancements to terminal emulators and ICA capabilities, delivers the “Netscape Communicator 4.5 experience”, and provides additional Network Station Manager capabilities, including flash management. These improvements and a move to a virtual memory system require additional code to be transferred between the boot server and the Network Station. There may be up to a four-fold increase in the LAN traffic to boot a Network Station in NSM V2R1 as compared to NSM V1R3.4.

With additional functions (as provided by V2R1 of the IBM Network Station Manager) come the demand for additional main memory. How much memory depends on the mix of software that is currently running on your Network Station. For IBM Network Station Manager V2R1, any model of IBM Network Station must have at least 32 MB RAM. For details on how much memory each application will consume, see the *NSM V2R1 - Memory requirements and performance recommendations* document as mentioned earlier.

Appendix J. Migration details

This appendix describes the details behind the NSM migration. The migration is broken down into the migration of the different preference levels (system, group, user, terminal). For each level there is a list of V1R3 files that will be migrated, and for each file, there is a detailed list of how specific preferences will be migrated. If a specific preference or file is not described in this appendix, it is not being migrated by NSM.

“Backdoor” files (those files created outside of NSM by users) will be migrated, but in a slightly different manner than the normal NSM files. The migration of these files will use the NSM command line tool. Preferences contained in these files will be written as commands to update the download profiles in a single command script. An administrator then needs to run the command line tool against this script to get the changes to actually be made in the download profiles. There are no guarantees with the backdoor files. Because they can potentially contain anything, it is not always obvious how to migrate them. The NSM migration utility takes its “best shot” at migrating the contents. System administrators should review the command script created by NSM migration before running the command line tool to ensure that the updates they actually want are being made.

Since the migration can be run on individual users, groups, and terminals, the migration command script is always appended to and not overwritten. Any new commands will be added to commands in the script from a previous migration. You may not want to run the command line tool after each individual migration. By appending, the NSM migration utility allows you to build one overall migration script that only needs to be executed once. If you want to have a migration script that only contains commands from a single run of the migration, you should delete the script file before running the migration.

After writing out commands to the migration script, a “COMMIT” command is added. This command insures all the changes are saved to the download profiles. If you want to run the script in a “test” state with out saving the changes, you should remove or comment out the COMMIT command. There will be one COMMIT command added to the script for each run of the migration that results in the script being updated.

Because of the change in operating systems from V1R3 to V2R1, some preferences found in the V1R3 files may no longer be valid, or they may be valid but set to a value that is no longer supported. In both these cases, the preference in question will not be migrated. Instead, a message will be logged saying the preference was dropped. Separate messages will be used for the two different cases.

In this appendix, $UserBase is used to represent the base path for V1R3 files. This path can vary from platform to platform. On the AS/400 system, it is /QIBM/UserData/NetworkStation. $UserBaseV2 is used to represent the base path for V2R1 files. On the AS/400 system, it is /QIBM/UserData/NetworkStationV2.

J.1 Migration of system-level preferences

When migrating system-level preferences, the following V1R3 files need to be migrated. Specific actions are listed under each file. These actions must be selected for settings found in that file.

- $UserBase/StationConfig/defaults.nsm
  - All migrated preferences from this file (except where noted) should be stored in the $UserBaseV2/profiles/allncs.nsm file.
  - The following migrated preferences should reside in the category WORKSTATION of the /config object. Preferences marked with an * should be stored as a list property. Otherwise, they should be stored as a string property.

    anti-aliasing
    boot-enable-broadcast-boot
    boot-flash-update
    boot-persistent-loading
    boot-persistent-retry-count
    boot-prom-language
    boot-prom-update-file
    boot-test-ram
    boot-token-ring-update-file
    ip-use-address-discovery
    pref-mouse-acceleration
    pref-mouse-arrangement
    pref-keyboard-auto-repeat-rate
    pref-keyboard-auto-repeat-start
    pref-screensaver-enable
    pref-screensaver-time
    pref-screensaver-style
    pref-screensaver-bitmap-file
    pref-power-manage-powerdown-time
    pref-power-manage-standby-time
    pref-power-manage-suspend-time
    pref-screen-color-depth
    pref-screen-background-bitmap-background
    pref-screen-background-bitmap-file
    pref-screen-background-bitmap-foreground
    pref-screen-background-type
    unit-contact
    unit-global-password
    unit-location
    xserver-keyboard-type
    xserver-access-control-enabled

  - The following migrated preferences should reside in the category EXTERNAL of the /config object. Preferences marked with an * should be stored as a list property. Otherwise, they should be stored as a string property.

    boot-automatically
    boot-desired-source
    boot-prom-force-update

boot-tcpip-broadcast-boot-request
boot-second-source
boot-third-source
config-load-initial-file
config-unit-ethernet-address-file
config-unit-ip-address-file
config-unit-name-file
file-initial-server-1
file-initial-server-2
file-initial-protocol-1
file-initial-protocol-2
parallel-daemons-table* (Fields for each element are port-number, use-parallel-port, and tcp-port)
pref-screensaver-interval
pref-xserver-screen-resolution
snmp-trap-to-config-port
snmp-trap-to-config-server
snmp-read-only-community
snmp-read-only-community-alt
snmp-read-write-community
snmp-read-write-community-alt
unit-initial-locale
xserver-access-control-enabled-default
xserver-access-control-list* (Fields for each element are host and family)

– The following migrated preferences should reside in the category DEVICE of /config object. Preferences marked with an * should be stored as a list property. Otherwise, they should be stored as a string property.

print-access-control-enabled

print-access-control-list* (Fields for each element are host)

print-lprd-cache-size

print-lpd-cache-size

print-lpd-stream-large-jobs

print-lpr-servers* (Fields for each element are server, queue-name, datastream-type, description, transform-file, dbcs-type, print-resolution, dbcs-font-encoding, request-banner-page, and use-as-default)

serial-access-control-enabled

serial-access-control-list* (Fields for each element are host)

serial-interfaces-table* (Fields for each element are port-number, mode, current-mode, baud-rate, data-bits, stop-bits, parity, handshake, and hangup)

serial-daemons-table* (Fields for each element are port-number, use-serial-protocol, and tcp-port)

– The preference xserver-initialize-web-palette-colors should be migrated to the DESKTOP category of the object /desktop/preferences in the $UserDataV2/profiles/allusers.nsm file.

- The preference java-appletviewer-command should be migrated to the APPLETVIEWER category of the object /java/appletviewer in the $UserDataV2/profiles/allusers.nsm file.
- Any remaining preferences should not be migrated. A message will be logged for each preference saying it was dropped.
- The value of xserver-keyboard-type is changing from a string to a numeric value. The following list displays the old values and what the corresponding new value should be. If the preference is set to a value not in the list, it should not be migrated because that value is no longer supported. A message will be logged saying it was dropped.

  danish - 15
  dutch - 110
  belgian-uk - 6
  english-uk - 9
  ibm-ps/2 - 0
  english-iso - 112
  swedish/finnish - 13
  french - 5
  belgian-french - 44
  canadian-french-csa-1988 - 43
  canadian-french-csa-1992 - 45
  swiss-french - 46
  german - 4
  swiss-german - 7
  italian - 10
  portuguese - 14
  brazilian - 141
  spanish - 8
  spanish (latin-america) - 109
  swedish - 167

- If pref-screensaver-bitmap-file or pref-screen-background-bitmap-file are set to /netstation/prodbase/SysDef/ibmwall.xbm, change the value to ibmwall.xbm. If set to /netstation/prodbase/SysDef/tiles.xbm, the preference should be dropped since this value is no longer valid. Any other value should be migrated as is.
- If pref-screen-background-type is set to something other than bitmap, the preference should be dropped.
- If not set to nil, the value specified for boot-prom-update-file should be changed to /proms/bootm.
- If not set to nil, the value specified for boot-token-ring-update-file should be changed to /proms/trflash.
- If boot-prom-language is set to Japanese, it should not be migrated.
- Because the password encoding has changed from V1R3 to V2R1, the value of unit-global-password needs to be changed. It must be decoded using the V1R3 decoding algorithm (qytcmtpd) and re-encoded using the V2R1 encoding algorithm (qytcmten).
- For unit-initial-locale, the value needs to be updated so the first two characters are in lowercase instead of uppercase. Also, several of the values that were supported in V1R3 are no longer supported in V2R1. The

following list contains the valid values. If a value is not in the list, the preference containing the value should not be migrated. A message will be logged saying it was dropped.

da_DK
de_CH
de_DE
en_GB
en_US
es_ES
es_LA
fi_FI
fr_BE
fr_CA
fr_CH
fr_FR
it_CH
it_IT
nl_BE
nl_NL
no_NO
pt_BR
pt_PT
sv_SE

- $UserBase/SysDef/NCDwm/pref
  - All migrated preferences should reside in the category DESKTOP of the object /desktop/preferences in the $UserBaseV2/profiles/allusers.nsm file. Each preference should be stored as a string property.
  - Make the following updates to the following preference names or values.
    - Change the name of mwm*iconPlacement to icon_placement. A value of "left bottom" should be changed to 1. A value of "left top" should be changed to 0. A value of "right bottom" should be changed to 5. A value of "right top" should be changed to 4.
    - Change the name of mwm*fontList to winmgr_font_size. A value of *dt*interface*system*-medium-r*-xxs*: or -adobe-helvetica-bold-r-normal--11-80-100-100-p-60-iso8859-1 should be changed to 8. A value of *dt*interface*system*-medium-r*-xs*: or -adobe-helvetica-bold-r-normal--14-100-100-100-p-82-iso8859-1 should be changed to 10. A value of *dt*interface*system*-medium-r*-s*: or -adobe-helvetica-bold-r-normal--17-120-100-100-p-92-iso8859-1 should be changed to 12. A value of *dt*interface*system*-medium-r*-md:, *dt*interface*system*-medium-r*-md*: (the first value appears to be a bug in the V1R3 NSM and this is the correct value. However, we decided to migrate both since they both may appear in V1R3 files), or -adobe-helvetica-bold-r-normal--20-140-100-100-p-105-iso8859-1 should be changed to 14. A value of *dt*interface*system*-medium-r*-l*: or -adobe-helvetica-bold-r-normal--25-180-100-100-p-138-iso8859-1 should be changed to 18. A value of *dt*interface*system*-medium-r*-xxl*: or -adobe-helvetica-bold-r-normal--34-240-100-100-p-182-iso8859-1 should be changed to 24.

    - All remaining preferences should not be migrated. A message will be logged for each of these preferences saying it was dropped.

- $UserBase/SysDef/NS5250/pref
  - All migrated preferences should reside in category NS5250 of the object /ns5250/preferences in the $UserBaseV2/profiles/allusers.nsm file. Each preference should be stored as a string property.
  - For all the following preferences, update the file paths. Replace the portion of file paths that start with /netstation/userbase/users/<user>/ with this part /userbase/nsmshared/<user>/. The rest of the path and the file name should remain the same.
  - NS5250*KeymapXXXPath (where XXX is replaced by the type of keyboard)
  - NS5250*ColorMapPath
  - NS5250*DefaultColorMapPath
  - NS5250*PlayBackPath
  - For all remaining preferences that start with NS5250*, migrate as is (no name or value changes).
  - For all remaining preferences that do not start with NS5250*, do *not* migrate and log a message for each preference saying it was dropped.
- $UserBase/SysDef/NS3270/pref
  - All migrated preferences should reside in category NS3270 of the object /ns3270/preferences in the $UserBaseV2/profiles/allusers.nsm file. Each preference should be stored as a string property.
  - For all the following preferences, update the file paths. Replace the portion of file paths that start with /netstation/userbase/users/<user>/ with this part /userbase/nsmshared/<user>/. The rest of the path and the file name should remain the same.

    NS3270*KeymapXXXPath (where XXX is replaced by the type of
keyboard)
NS3270*ColorMapPath
NS3270*DefaultColorMapPath
NS3270*PlayBackPath
  - For all remaining preferences that start with NS3270*, migrate as is (no name or value changes).
  - For all remaining preferences that do not start with NS3270*, do *not* migrate and log a message for each preference saying it was dropped.
- $UserBase/SysDef/NAV/pref
  - All migrated preferences should reside in the category NETSCAPE of the object /netscape/preferences in the $UserBaseV2/profiles/allusers.nsm file. Each preference should be stored as a string property.
  - Make the following updates to the following preference names or values.
    - Change the name of Navio.proxyMode to lockPref.network.proxy.type, and if its value is 0, change it to 3.
    - Change the name of Navio.autoconfigUrl to lockPref.network.proxy.autoconfig_url.

        - Change the name of Navio.disableJava to lockPref.security.enable_java. A value of 0 should be changed to a value of true, and a value of 1 should be changed to a value of false.
        - Change the name of Navio.memCacheSize to lockPref.browser.cache.memory_cache_size.
    - All remaining preferences should not be migrated. A message will be logged for each of these preference saying it was dropped.
- $UserBase/SysDef/envvars.nsm
    - The environment variables found in this file will be stored under a single object, /login/session, in $UserBaseV2/profiles/allusers.nsm. However, not all variables in the file will be stored under the same category. Within each category, there will be a single list property called "commands". Each element within the property will consist of three fields, op, arg1, and arg2, along with the information for the environment variable. The op field will have a value of SET, the arg1 field will have a value of the environment variable name, and the arg2 field will have a value of the environment variable value.
    - The following migrated preferences should reside in the LANGUAGE category.

      LANG
      LC_TIME
      LC_MONETARY
      LC_NUMERIC
      LC_CTYPE
      LC_MESSAGES
    - The LANGUAGE variables need to have their values updated, so the first two characters are in lowercase instead of uppercase.
    - Several of the values that were supported in V1R3 are no longer supported in V2R1. The following list contains the valid values. If a value is not in the list, the preference containing that value should not be migrated, and a message will be logged saying it was dropped.

      da_DK
      de_CH
      de_DE
      en_GB
      en_US
      es_ES
      es_LA
      fi_FI
      fr_BE
      fr_CA
      fr_CH
      fr_FR
      it_CH
      it_IT
      nl_BE
      nl_NL
      no_NO
      pt_BR

pt_PT
sv_SE

- – Any remaining environment variables should not be migrated. A message will be logged for each of these preference saying it was dropped.
- – Any SOURCE or VERSION commands found in the file should be ignored.

- $UserBase/SysDef/startup.nsm
  - – For SET commands (environment variables):
    - The environment variable NSM_LOGOUT should be migrated to a desktop preference. If found in the file, it should be added as a string property to the DESKTOP category of the object /desktop/preferences in the $UserBaseV2/profiles/allusers.nsm file. The property should be called show_logout_button. If a value of YES was specified, it should be changed to “yes”. A value of NO should be changed to “no”.
    - The environment variable NSM_LOCK should be migrated to a desktop preference. If found in the file, it should be added as a string property to the DESKTOP category in the /desktop/preferences object. The property should be called show_lock_button. If a value of YES was specified, it should be changed to “yes”. A value of NO should be changed to “no”.
    - Any of the following environment variables should *not* be migrated. A message will be logged for each of these preference saying it was dropped.

JITC_COMPILER
JITC_ENABLED
JITC_OPTIMUM_BUFFER_SIZE
JITC_REQUIRED_BUFFER_SIZE
NSB_ENCRYPTION
NSM_ADMIN_SYSDEFAULTS
NSM_GROUP_PREFS
NSM_GROUP_SYSDEFAULTS
NSM_HIDE
NSM_NCDWM_PREF_VERSION
NSM_PROD_SYSDEFAULTS
NSM_TASKBAR
NSM_TOPBOTTOM
NSM_USER_PREFS
NSM_WMN_PREF_VERSION
NSM_NAV_PREF_VERSION
NSM_NS3270_PREF_VERSION
NSM_NS5250_PREF_VERSION
NSM_NSTERM_PREF_VERSION
RUN_WM
WNN_USING_IM
WNN_JSERVER
WNN_JS_PORT_NO
WNN_XW_PORT_NO
XMODIFIERS

- All migrated environment variables will be stored under a single object, /login/session, in $UserBaseV2/profiles/allusers.nsm. However, not all variables in the file will be stored under the same category. Within each category, there will be a single list property called "commands". Each element within the property will consist of three fields, op, arg1, and arg2, and will contain the information for the environment variable. The pop field will have a value of SET, the arg1 field will have a value of the environment variable name, and the arg2 field will have a value of the environment variable value.

- The environment variable AUTHENTICATION_HOST should be migrated to the HIDDEN category of the /login/session object.
- The following environment variables should be migrated to the INTERNET category for the /login/session object.

  FULL_NAME
  EMAIL_USERID
  REPLY_TO
  HOME_PAGE
  FTP_PROXY_HOST
  FTP_PROXY_PORT
  HTTP_PROXY_HOST
  HTTP_PROXY_PORT
  GOPHER_PROXY_HOST
  GOPHER_PROXY_PORT
  HTTPS_PROXY_HOST
  HTTPS_PROXY_PORT
  SOCKS_HOST
  SOCKS_PORT
  SMTP_SERVER
  POP3_SERVER
  NNTP_SERVER
  NNTP_SERVER_PORT
  FTP_PROXY_OVERRIDES
  HTTP_PROXY_OVERRIDES
  GOPHER_PROXY_OVERRIDES
  NSM_HTTP_PORT
  DESKTOP_LAUNCHER_PORT

- The remaining environment variables should be migrated to the ENVVARS category for the /login/session object.

– For MENUITEM commands:

- All MENUITEMs should be added to a menu called MIG_OLD_APPS-FOLDER. This menu will need to be created, but should only be created when migrating preferences at the system level. Its fields should be set to:

  nsm_type - FOLDER
  name - No value should be specified
  resource - OLD_APPS
  normal_icon - customn.xpm
  active_icon - customa.xpm
  highlight_icon - customh.xpm
  pressed_icon - customp.xpm
  minimized_icon - customm.xpm
  icon-priority - Determined at migration time

- Each MENUITEM will have a corresponding item created for it in the LAUNCHBAR category of the /desktops/default package in the $UserBaseV2/profiles/allusers.nsm file. Each item should specify the oldapps menu as the menu to which it belongs.
- The name of ITEM representing a MENUITEM (or RUN) command is derived as follows: <name_field_value>-<nsm_type_field_value>-<level>-<index>.

  If no value is specified for the name field, the value for the nsm_type field is used instead. The level represents the level of the download profile the item resides in, and the index represents an incrementing count of the number of items of this application type in this download profile. Consider the example where the item was for the NS5250 application, had a name of “nsdev”, was in the user-level download profile, and was the second NS5250 application item to appear in the file. In this case, the name generated would be nsdev-5250-user-2. If no name field was specified, it would be 5250-5250-user-2.

  Note: This applies to the NAME attribute in the ITEM XML element. It should not be confused with the name field element contained within the item.
- The menu item label specified for each MENUITEM should be used as the name field for the ITEM.
- The icon_priority field determines in what order the items will appear in the menu. The item with the highest priority will appear first in the menu, and the item with the lowest priority will appear last in the menu. Menu items found in the startup.nsm file will be added to the menu in the order that they appear. Therefore, the first menu item in the file should have the highest priority.
- The command field for all applications described here should start with NSMRUN followed by the command contained in the menu item.
- For MENUITEMs that launch the `ns5250` command, create an item for it with the following fields and values:

  nsm_type - 5250
  name - Use the menu item label
  resource - 5250
  type - application/native-module
  normal_icon - 5250n.xpm
  active_icon - 5250a.xpm
  highlight_icon - 5250h.xpm
  pressed_icon - 5250p.xpm
  minimized_icon - 5250m.xpm
  icon_priority - Determined at migration time
  kill_priority - 4
  command - ns5250 command specified in the MENUITEM
  activate_class - NULL String
  x11_class - NS5250
  memory_size - 3072
  save_size - no
  save_position - no

If the -LANG_ID parameter is specified in the ns5250 command, update its value so the first two characters are in lowercase instead of uppercase. Also, several of the values that were supported in V1R3 are no longer supported in V2R1. The list of valid values is the same list specified for the LANGUAGE environment variables. If a value is specified that is not valid, the -LANG_ID parameter should be dropped from the command.

- For MENUITEMs that launch the `ns3270` command, create an item for it with the following fields and values:

  nsm_type - 3270
  name - Use the menu item label
  resource - 3270
  type - application/native-module
  normal_icon - 3270n.xpm
  active_icon - 3270a.xpm
  highlight_icon - 3270h.xpm
  pressed_icon - 3270p.xpm
  minimized_icon - 3270m.xpm
  icon_priority - Determined at migration time
  kill_priority - 4
  command - ns3270 command specified in the MENUITEM
  activate_class - NULL String
  x11_class - NS3270
  memory_size - 2970
  save_size - no
  save_position - no

  If the -LANG_ID parameter is specified in the ns3270 command, update its value so the first two characters are in lowercase instead of uppercase. Also, several of the values that were supported in V1R3 are no longer supported in V2R1. The list of valid values is the same list specified for the LANGUAGE environment variables. If a value is specified that is not valid, the -LANG_ID parameter should be dropped from the command.

- For MENUITEMs that launch the `nsterm` command, create an item for it with the following fields and values:

  nsm_type - VT_EMULATOR
  name - Use the menu item label
  resource - VT_EMULATOR
  type - application/native-module
  normal_icon - vtn.xpm
  active_icon - vta.xpm
  highlight_icon - vth.xpm
  pressed_icon - vtp.xpm
  minimized_icon - vtm.xpm
  icon_priority - Determined at migration time
  kill_priority - 4
  command - nsterm command specified in the MENUITEM
  activate_class - NULL String
  x11_class - NSTerm
  memory_size - 2253

save_size - no
save_position - no

If the -LANG_ID parameter is specified in the nsterm command, update its value so the first two characters are in lowercase instead of uppercase. Also, several of the values that were supported in V1R3 are no longer supported in V2R1. The list of valid values is the same list specified for the LANGUAGE environment variables. If a value is specified that is not valid, the -LANG_ID parameter should be dropped from the command.

If the -tn flag is specified in the nsterm command, change it to be a -ti flag. The value should remain the same.

If the -xrm flag is specified in the nsterm command, the following changes need to be made to its value.

If the NCDterm*appCursorMode preference is specified, change the name to NSTerm*appCursorDefault.

If the NCDterm*appKeypadMode preference is specified, change the name to NSTerm*appKeypadDefault.

If the NCDterm*cursorType preference is specified, change the name to NSTerm*charCursorStyle.

If the NCDterm*logFile preference is specified, change the name to NSTerm*logDirectory.

If the NCDterm*termName preference is specified, change the name to NSTerm*termId.

If the NCDterm*scrollBar preference is specified, change the name to NSTerm*scrollBar. A value of “Left” or “Right” should be changed to “True” and a value of “None” to “False”.

Any remaining preferences starting with a “NCDterm” prefix should be updated to use a “NSTerm” prefix.

- For MENUITEMs that launch the `loadb navio` command, create an item for it with the following fields and values:

nsm_type - NETSCAPE
name - Use the menu item label
resource - NETSCAPE
type - application/native-module
normal_icon - netscapen.xpm
active_icon - netscapea.xpm
highlight_icon - netscapeh.xpm
pressed_icon - netscapep.xpm
minimized_icon - netscapem.xpm
icon_priority - Determined at migration time
kill_priority - 4
command - Command specified (updated) in the MENUITEM
activate_class - NULL String
x11_class - Netscape
application_name - browser
memory_size - 17408
autocommand - /usr/local/bin/netscape -noclonk
save_size - NULL String

save_position - NULL String
accept_types - application/url, text/html, text/plain, image/gif,
    image/jpeg, image/pjpeg, image/x-xbitmap
accept_extensions - htm, html, txt, text, gif, jpg, jpeg, jpe, jfif, xbm

Update the command name from `loadb navio` to `run netscape`.

The -install parameter should be removed from the netscape command. It has no value.

- For MENUITEMs that launch the `appletviewer` command, create an item for it with the following fields and values:

  nsm_type - APPLET_VIEWER
  name - Use the menu item label
  resource - APPLET_VIEWER
  type - application/native-module
  normal_icon - javaappn.xpm
  active_icon - javaappa.xpm
  highlight_icon - javaapph.xpm
  pressed_icon - javaappp.xpm
  minimized_icon - javaappm.xpm
  icon_priority - Determined at migration time
  kill_priority - 4
  command - appletviewer command specified in the MENUITEM
  activate_class - NULL String
  x11_class - NCJava
  application_name - NULL String
  memory_size - 3072
  autocommand - NULL String
  save_size - NULL String
  save_position - NULL String
  accept_types - NULL String
  accept_extensions - NULL String

- For MENUITEMs that launch the `java` command, create an item for it with the following fields and values:

  nsm_type - JAVA_APPLICATION
  name - Use the menu item label
  resource - JAVA_APPLICATION
  type - application/native-module
  normal_icon - javan.xpm
  active_icon - javaa.xpm
  highlight_icon - javah.xpm
  pressed_icon - javap.xpm
  minimized_icon - javam.xpm
  icon_priority - Determined at migration time
  kill_priority - 4
  command - java command specified in the MENUITEM
  activate_class - NULL String
  x11_class - NCJava
  application_name - NULL String
  memory_size - 3072
  autocommand - NULL String
  save_size - NULL String
  save_position - NULL String

accept_types - NULL String
accept_extensions - NULL String

- For MENUITEMs that launch the `rsh localhost` command, create an item for it with the following fields and values:

  nsm_type - LOCAL_PROGRAM
  name - Use the menu item label
  resource - LOCAL_PROGRAM
  type - application/native-module
  normal_icon - lclpgmn.xpm
  active_icon - lclpgma.xpm
  highlight_icon - lclpgmh.xpm
  pressed_icon - lclpgmp.xpm
  minimized_icon - lclpgmm.xpm
  icon_priority - Determined at migration time
  kill_priority - 2
  command - Program specified in the MENUITEM (don't include `rsh localhost`)
  activate_class - NULL String
  x11_class - NULL String
  memory_size - 3072
  save_size - NULL String
  save_position - NULL String

  If the command invokes ICA, the program name needs to be changed from icaclnt to wfica, and the value specified for the password parameter (-password or -p) needs to be encoded using the NSM password encoding algorithm.

- For MENUITEMs that launch the `rsh` (without localhost) command:, create an item for it with the following fields and values:

  nsm_type - REMOTE_PROGRAM
  name - Use the menu item label
  resource - REMOTE_PROGRAM
  type - application/native-module
  normal_icon - rmtpgmn.xpm
  active_icon - rmtpgma.xpm
  highlight_icon - rmtpgmh.xpm
  pressed_icon - rmtpgmp.xpm
  minimized_icon - rmtpgmm.xpm
  icon_priority - Determined at migration time
  kill_priority - 2
  command - RUN xhost <host> and rsh command specified in the MENUITEM
  activate_class - NULL String
  x11_class - NCPromptBox
  memory_size - 3072
  save_size - NULL String
  save_position - NULL String

– For RUN commands:

- All RUN commands need to be added to the Startup folder in the launch bar. Therefore, all commands need to be added to category LAUNCHBAR and specify a menu of Startup-FOLDER-system-1.

    - They also need to be added to the STARTUP category of the /startup package. The same fields that were specified for the command in the LAUNCHBAR category should be specified here. There should be no menu specification.
  - Any SOURCE or VERSION commands found in the file should be ignored.
- $UserBase/StationConfig/defaults.dft
  - The following are restrictions imposed on the contents of this file:

    There is a restricted syntax allowed for the configd backdoor files. NCDi/OS allowed for a very rich syntax in the specification of its configd preferences. For the NSM-managed files (non-backdoor), we restricted this syntax to make parsing easier. However, because NSM did not read the backdoor files, any valid configd syntax was allowed. For migration, we cannot support the full syntax. However, we allow a richer syntax than was allowed in the NSM-managed files. We allow items we thought were most likely to be used in existing backdoor files. Here is the list of items we do *not* allow:

    - All lines must end with a linefeed (either just LF or CRLF). Ending a line with just a carriage return will not work as the file will not be parsed correctly.
    - Only SET commands will be processed. All other commands will be ignored. This includes the read command used to "pull in" preferences from another file.
    - Preference names and values must be in lowercase. Values can be in mixed case if they represent a string.
    - Comments will be ignored. If a comment appears on the same line as a preference setting, the comment will be taken as part of the setting.
    - For indicating a preference has no value, the value "nil" should be used. The value "null" should not be used.
    - Integer values should be specified in decimal.
    - The value of "default" should not be used to set the preference to its default value.
    - Boolean values should be specified with a true/false value (not on/off or yes/no).
  - All migrated preferences found in this file need to be built into a NSM script file that may be processed by the NSM command line tool. The script file should be built is $UserBaseV2/profiles/migrate.scr. Single-valued preferences (non-tables) should be formatted into an INSERT command of the following format:

    ```
    INSERT IBMNSM/SYSTEM/DEFAULT/<category>/<preference_name>/
    <preference_value>
    ```

  - If a multi-valued preference (table) appears without an index, the following command should be added to the script:

    ```
    INSERT IBMNSM/SYSTEM/DEFAULT/<category>/<preference_name>/SET ACTION
    REPLACE
    ```

  - If a multi-valued preference (table) appears with a [-1] index and this preference has not appeared in the file before, the following command should be added to the script:

```
INSERT IBMNSM/SYSTEM/DEFAULT/<category>/<preference_name>/SET ACTION
APPEND
```

Then each value of the multi-valued preference (table) should be formatted into an INSERT command of the following format:

```
INSERT IBMNSM/SYSTEM/DEFAULT/<category>/<preference_name>/
-<field_name1> <field_value1> -<field_name2> <field_value2>...
```

– If a multi-valued preference (table) appears with an [X] index (where X represents an integer value) and this preference has not appeared in the file before, the following command should be added to the script:

```
INSERT IBMNSM/SYSTEM/DEFAULT/<category>/<preference_name>/SET ACTION
INSERT
```

Then each value of the multi-valued preference (table) should be formatted into an INSERT command of the following format:

```
INSERT IBMNSM/SYSTEM/DEFAULT/<category>/<preference_name>/
-<field_name1> <field_value1> -<field_name2> <field_value2>...
```

– Same changes to preferences as described for file $UserBase/StationConfig/defaults.nsm.

- $UserBase/SysDef/pref.dft
  - This file must be in ASCII. In V1R3, the file could be in ASCII or UCS-2. However, determining the encoding of this file proved too difficult, so we will assume that the file is in ASCII. It is expected that most of these files will be in ASCII anyway.
  - All migrated preferences found in this file need to be built into a NSM script file that may be processed by the NSM command line tool. The script file should be built is $UserBaseV2/profiles/migrate.scr. Each preference should be formatted into an INSERT command of the following format:

    ```
    INSERT IBMNSM/SYSTEM/DEFAULT/<category>/<preference_name>/
    <preference_value>
    ```

  - For preferences that start with Navio:
    - Migrated preferences should be inserted into the NETSCAPE category.
    - The same changes to Navio preferences apply as described for file $UserBase/SysDef/NAV/pref.
  - For preferences that start with NS5250:
    - Migrated preferences should be inserted into the NS5250 category.
    - The same changes to NS5250 preferences apply as described for file $UserBase/SysDef/NS5250/pref.
  - For preferences that start with NS3270:
    - Migrated preferences should be inserted into the NS3270 category.
    - The same changes to NS3270 preferences apply as described for file $UserBase/SysDef/NS3270/pref.
  - For preferences that start with NCDterm:
    - Migrated preferences should be inserted into the NSTERM category.
    - If the preference is NCDterm*appCursorMode, change the preference name to NSTerm*appCursorDefault.

    - If the preference is NCDterm*appKeypadMode, change the preference name to NSTerm*appKeypadDefault.
    - If the preference is NCDterm*cursorType, change the preference name to NSTerm*charCursorStyle.
    - If the preference is NCDterm*logFile, change the preference name to NSTerm*logDirectory.
    - If the preference is NCDterm*termName, change the preference name to NSTerm*termId.
    - If the preference is NCDterm*scrollBar, change the preference name to NSTerm*scrollBar. If the value is “Left” or “Right”, change value to “True”. If the value is “None”, change value to “False”.
    - All other preferences starting with NCDterm should have this prefix replaced with NSTerm. The rest of the preference name stays the same.
  - For preferences that start with NSTerm:
    - Migrated preferences should be inserted into category NSTERM.
    - All preferences should be added to the NSM script as is.
  - For preferences that start with mwm:
    - Migrated preferences should be inserted into category DESKTOP.
    - The same changes to mwm preferences apply as described for the $UserBase/SysDef/NCDwm/pref file.
  - For all remaining preferences that do not fall into one of the categories described above, do *not* migrate the preference.

Note: We will *not* be migrating the backdoor file $UserBase/SysDef/startup.dft for two reasons. First, this file functions differently than all other backdoor files. All other backdoor files are just another file downloaded in addition to the system, group, user, and terminal files managed by NSM. The preferences defined in them combine with the preferences from the NSM-managed files with any duplication preferences being overridden by the backdoor files. However, startup.dft is a total replacement for the NSM-managed files. If this file is found, only it is downloaded. None of the NSM-managed files are downloaded. There is no good way to support this functionality in V2R1. Second, the NSM command line tool does not support configuration of the desktop launch bar. Therefore, the current method of migrating backdoor files would not work for startup.dft.

J.2 Migration of group-level preferences

When migrating group-level preferences, the following V1R3 files need to be migrated. Specific actions are listed under each file. These actions must be taken for settings found in that file.

- $UserBase/groups/<group>/NCDwm/pref
  - All migrated preferences should reside in the DESKTOP category of the /desktop/preferences object in the $UserBaseV2/profiles/groups/<group>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NCDwm/pref file.

- $UserBase/groups/<group>/NS5250/pref
  - All migrated preferences should reside in the NS5250 category of the /ns5250/preferences object in the $UserBaseV2/profiles/groups/<group>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NS5250/pref file.
- $UserBase/groups/<group>/NS3270/pref
  - All migrated preferences should reside in the NS3270 category of the /ns3270/preferences object in the $UserBaseV2/profiles/groups/<group>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NS3270/pref file.
- $UserBase/groups/<group>/NAV/pref
  - All migrated preferences should reside in the NETSCAPE category of the /netscape/preferences object in the $UserBaseV2/profiles/groups/<group>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NAV/pref file.
- $UserBase/groups/<group>/envvars.nsm
  - All migrated preferences should reside in the category as described for the system-level envvars.nsm file. They should be stored in the $UserBaseV2/profiles/groups/<group>.nsm file.
  - Requires the same migration as the system-level envvars.nsm file.
- $UserBase/groups/<group>/startup.nsm
  - All migrated preferences should reside in the category as described for the system-level startup.nsm file. They should be stored in the $UserBaseV2/profiles/groups/<group>.nsm file.
  - Requires the same migration as the system-level startup.nsm file.
- $UserBase/groups/<group>/<group>.nsg
  - All migrated preferences should reside in the category as described for the defaults.nsm file. They should be stored in the $UserBaseV2/profiles/groups/<group>.nsm file.
  - Requires the same migration as the system-level defaults.nsm file.
- $UserBase/groups/<group>/<group>.grp
  - The same syntax restrictions as for defaults.dft apply to this file.
  - Requires the same migration and command script format as described for the system-level defaults.dft file, except the INSERT commands should specify GROUP as the level and the group name as:

    ```
    INSERT IBMNSM/GROUP/<group>/...(rest of the command)
    ```

J.3 Migration of user-level preferences

When migrating user-level preferences, the following V1R3 files need to be migrated. Specific actions are listed under each file. These actions must be followed for the settings found in that file.

- $UserBase/users/<user>/NCDwm/pref
  - All migrated preferences should reside in the DESKTOP category of the /desktop/preferences object in the $UserBaseV2/profiles/users/<user>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NCDwm/pref file.
- $UserBase/users/<user>/NS5250/pref
  - All migrated preferences should reside in the NS5250 category of the /ns5250/preferences object in the $UserBaseV2/profiles/users/<user>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NS5250/pref file.
- $UserBase/users/<user>/NS3270/pref
  - All migrated preferences should reside in the NS3270 category of the /ns3270/preferences object in the $UserBaseV2/profiles/users/<user>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NS3270/pref file.
- $UserBase/users/<user>/NAV/pref
  - All migrated preferences should reside in the NETSCAPE category of the /netscape/preferences object in the $UserBaseV2/profiles/users/<user>.nsm file. Each preference should be stored as a string property.
  - Requires the same migration as the system-level NAV/pref file.
- $UserBase/users/<user>/envvars.nsm
  - The language environment variables should be placed in the category and object should be described for the system-level envvars.nsm file. They should be stored in the $UserBaseV2/profiles/users/<user>.nsm file.
  - The migration of the language environment variables should be the same as described for the system-level envvars.nsm file.
  - The user-level envvars.nsm file will include the migration of an additional environment variable called GROUP. This variable will be migrated to the system-level profile $UserBaseV2/profiles/allusers.nsm. This variable will be migrated to the USERGROUP category in the /login/groups object as a string property. The name of the property will be the name of the user whose file the V1R3 variable was found in, and the value of the property will be the value of, the GROUP variable (name of the group).
- $UserBase/users/<user>/startup.nsm
  - All migrated preferences should reside in the category as described for the system-level startup.nsm file. They should be stored in the $UserBaseV2/profiles/users/<user>.nsm file.
  - Requires the same migration as the system-level startup.nsm file.

- $UserBase/users/<user>/<user>.nsu
  - All migrated preferences should reside in the category as described for the defaults.nsm file. They should be stored in the $UserBaseV2/profiles/users/<user>.nsm file.
  - Requires the same migration as the system-level defaults.nsm file.
- $UserBase/users/<user>/<user>.usr
  - The same syntax restrictions as for defaults.dft apply to this file.
  - Requires the same migration and command script format as described for the system-level defaults.dft file, except the INSERT commands should specify USER as the level and the user name as:

    ```
    INSERT IBMNSM/USER/<user>/...(rest of the command)
    ```

J.4 Migration of terminal-level preferences

When migrating terminal-level preferences, the following V1R3 files need to be migrated. Listed under each file are specific actions that must be performed for settings found in that file.

- $UserBase/StationConfig/<ncid>.nst
  - All migrated preferences should reside in the category as described for the defaults.nsm file. They should be stored in the $UserBaseV2/profiles/ncs/<nc>.nsm file.
  - Requires the same migration as the system-level defaults.nsm file.
- $UserBase/StationConfig/<ncid>.trm
  - The same syntax restrictions as for defaults.dft apply to this file.
  - Requires the same migration and command script format as described for the system-level defaults.dft file, except the INSERT commands should specify TERMINAL as the level and the terminal (nc) name as follows:

    ```
    INSERT IBMNSM/TERMINAL/<nc>/...(rest of the command)
    ```

Appendix K. ICA error messages

Table 98 shows the possible ICA error messages with a short description of the possible problem.

Table 98. ICA error messages and resolutions

Error message	Description
1: An internal error occurred in the ICA client	An internal error has occurred. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
2: unused	
3: The option "..." is not valid	Option "..." is not valid in this context.
4: Missing argument for the option "..."	Option "..." requires an argument.
5: The option "..." has an invalid argument: "..."	The configuration file has been edited directly or is corrupt.
6: Insufficient memory available	The client does not have enough memory to continue program execution.
7: Internal Error: E_CLIPPING	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
8: Invalid ICA Protocol data received	This may indicate a network error.
9: Internal Error: E_TOO_MANY_CALLS	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
10: Cannot read file: "..."	There was a problem reading a connection database file.
11: Error in configuration file: "..." Cannot find section "..."	The configuration file has been edited directly or is corrupt.
12: Error in configuration file. Section "..." must contain an entry "..."	The configuration file has been edited directly or is corrupt.
13: Internal Error: E_DESTROY_WITHOUT_INIT	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
14: Cannot open visual: ...	The visual (ID = ...) cannot support the required number of colors.
15: The visual (ID = "...") cannot support the required number of colors	Cannot open visual.
16: Cannot allocate sufficient colors. Continuing in 16 color mode	A suitable visual has been found, but it can only support 16 colors.
17: Cannot find a suitable visual on this display	Unable to allocate a private color map on this display.

Error message	Description
18: Unable to allocate a private colormap for this display	Unable to get all the color cells needed for a private color map on this display.
19: Internal Error: E_BUFFER_OVERFLOW	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
20: X Server cannot allocate sufficient resource. Request "..."	The X Server was unable to allocate the resources required by Request ...
21: An error occurred in the graphics system	There is a problem with the display. Try exiting other applications, such as Netscape Navigator, to release the colors on your display.
22: Cannot find keyboard mapping file "..."	The keyboard mapping file specified in the Preferences page of the Settings dialog box is invalid or cannot be located.
23: A server must be entered	A server name must be entered in the Network page of the Properties dialog box.
24: Window size must be between 300x300 and 1280x1024	The Custom Width field in the Window page of the Properties and Settings dialog boxes can take values between 300 and 1280. The Custom Height field in the Window page of the Properties and Settings dialog boxes can take values between 300 and 1024.
25: Data has been changed. Are you sure you want to quit?	You are quitting from the ICA client without saving changes to the current connection entry.
26: Data has been changed. Are you sure you want to continue?	You are continuing to execute the ICA client without saving changes to the current connection entry.
27: Invalid serial number	Unable to obtain or generate a unique serial for this ICA client.
28: Cannot write file: "..."	There was a problem saving the connection database file, for example, no disk space.
29: Cannot create file: "..."	There was a problem creating a new connection database file.
30: The X Request "..." caused error: "..."	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
31: Invalid error: Cannot start NCS with this connection	The connection entry is invalid.
32: unused	
33: Internal Error: E_HH_INVALID_DISPLAY	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

Error message	Description
34: Internal Error: E_HH_UNSUPPORTED	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
35: Unable to start child program. Fork failed error: "..."	The ICA Remote Application Manager was unable to start the ICA client.
36: unused	
37: Cannot read file: "..."	Unable to open an ICA configuration file.
38: Cannot find specified connection	The configuration file is corrupt. Create a new configuration file.
39: Cannot find specified connection	The configuration file is corrupt. Create a new configuration file.
40: Error in configuration file: "..." Missing section: "..."	The configuration file is corrupt. Create a new configuration file.
41: Inconsistency in configuration file: "..." Missing section: "..."	The configuration file is corrupt. Create a new configuration file.
42: This description is already in use. The Description must be unique	The Description field in the Network page of the Properties dialog box must be unique.
43: This description is already in use. The Description must be unique	The Description field in the Network page of the Properties dialog box must be unique.
44: You must enter a serial number for Net Client to run	Enter serial number.
45: Invalid Demonstration License. Check that the Authorization Code and Expiry Date are correct.	Not used.
46: Cannot locate executable file "..." (...)	The executable file does not exist or the working directory or path is incorrect.
47: Cannot execute file "..." (...)	The ICA Remote Application Manager was unable to start the ICA client.
48: Cannot get address for server "..."	Unable to resolve the server name.
49: Cannot connect to server "..."	Unable to connect to server.
50: Your license does not allow you to connect to this server.	Not used.
51: A Master Browser cannot be located	The query server cannot locate the Master Browser or the query server cannot be located.
52: No servers were found	ICA servers were searched for, but none were found. You may have to set or reset Server Locations in the Settings dialog.
53: Invalid Citrix Server Browser command header received	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

Error message	Description
54: Invalid Citrix Server Browser command received	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
55: Invalid Citrix Server Browser command received on request	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
56: Invalid Citrix Server Browser command sequence received	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
57: Citrix Server Browser command contains an invalid parameter	An internal error occurred in the ICA client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.
58: Not enough memory	The client does not have enough memory to continue program execution.
59: I/O Error	One of the following problems occurred when attempting to contact a Citrix Master Browser: unable to bind socket, unable to get socket name, unable to set socket broadcast option, unable to set non-blocking option, connection refused, or unable to connect.
60: Read Timeout	Overdue response from a Citrix Master Browser after multiple attempts. In addition, this may cause a request for the election of a new Citrix Master Browser.
61: IPX protocol is not available	IPX protocol is not supported on the IBM Network Station.
62: TCP/IP protocol is not available	Network error. Contact your system administrator.
63: NETBIOS protocol is not available	NETBIOS protocol is not supported by the IBM Network Station.
64: The Citrix Server you have selected can not located	The Citrix Server name cannot be resolved.
65: The Citrix Server cluster you have selected can not located	Not used.
66: Unable to contact the Citrix Server Browser. Either your network is not functional, or you need to configure your an address under Server Browsing	Either your network is not functional, or you need to configure your an address under Server Browsing.
67: Error in configuration file: "..." Bad Key "..."	The configuration file has been edited directly or is corrupt.
68: Error in configuration file: "..." Bad Value "..."	The configuration file has been edited directly or is corrupt.

Error message	Description
69: Error in configuration file: "..." Bad Vendor Range "..."	The configuration file has been edited directly or is corrupt.
70: Unable to perform update: not running as super user	You must be running as a super user to perform a client update.
71: Unable to perform update: client is not on local file system	The client cannot update an installation on a non-local (for example, NFS mounted) file system.
72: Unable to perform update: not running $ICAROOT/wfica	The client cannot update an installation other than its own.
73: Error loading dynamic module: "..." ...	Not used.
74: Must specify proxy server address	Enter a proxy server address in the Firewall Settings under the Properties box.
75: The option "..." is required	Missing option "..." when using another option.
76: Cannot connect to the Citrix server. Your Citrix server does not support the encryption you required	Your Citrix server does not support the encryption you required. Please change the encryption.

Appendix L. Special notices

This publication introduces and describes the new features and functions available with IBM Network Station Manager Version 2 Release 1. The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM Network Station Manager product. See the PUBLICATIONS section of the IBM Programming Announcement for IBM Network Station Manager Version 2 Release 1 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

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

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

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

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
AT
CICS
Current
eSuite
Hummingbird
Lotus
Lotus Notes
Netfinity
Network Station
Nways
OS/2
OS/400
RS/6000
SecureWay
SP
System/38
Tivoli
VTAM
WebSphere
Word Pro
XT
AS/400
cc:Mail
CT
Domino
Home Director
IBM
Lotus eSuite
Lotus SmartSuite
NetView
Notes
OpenEdition
OS/390
PS/2
S/390
SmartSuite
SP1
System/390
VisualAge
Wave
Wizard
WorkPad
400

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Appendix M. Related publications

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

M.1 IBM Redbooks

For information on ordering these ITSO publications see “How to get IBM Redbooks” on page 677.

- *Lotus Domino R5 for IBM RS/6000*, SG24-5138
- *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147
- *AS/400 IBM Network Station - Techniques for Deployment*, SG24-5187
- *Lotus Domino for AS/400 R5: Implementation*, SG24-5592

The following redbooks are only available online in soft copy format at: `http://www.redbooks.ibm.com/` At the site, click **Redbooks Online!** in the left pane. Then, enter the book number (`SG24-XXXX`) in the search string field and click **Submit Search**.

- *IBM Network Station Guide for Windows NT,* SG24-2127
- *AS/400 IBM Network Station - Getting Started*, SG24-2153
- *IBM Network Station Printing Guide*, SG24-5212
- *IBM Network Station Release 3 Guide for Windows NT,* SG24-5221

M.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at `http://www.redbooks.ibm.com/` for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	**Collection Kit Number**
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr Format)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

M.3 Other resources

These publications are also relevant as further information sources:

- *IBM Network Station Manager Installation and Use*, SC41-0664
- *AS/400 Software Installation*, SC41-5120
- *AS/400 Client Access Express for Windows Setup*, SC41-5507

The following publications can be accessed at the IBM Network Station Library at: `http://www.pc.ibm.com/us/networkstation/tech_library.html` At the site, click **Technical Publications**. Then, click the appropriate topic heading.

- *Installing IBM Network Station Manager for AS/400*, SC41-0684
- *Installing IBM Network Station Manager for RS/6000*, SC41-0685
- *Installing IBM Network Station Manager for Windows NT*, SC41-0688
- *Using IBM Network Station Manager V2R1*, SC41-0690
- *IBM Network Station Advanced Information V2R1*

M.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- Effective September 9, 1999, Lotus discontinued marketing the eSuite product line. For details on this and other important information regarding the Lotus eSuite product, visit the Lotus We site at: `http://www.lotus.com/home.nsf/welcome/esuite1`
- For information about the Whistle InterJet, see the Whistle Communications Web site at: `http://www.whistle.com`
- Touch-screen monitors that are supported with V2R1 of NSM include the ELO TouchSystems' IntelliTouch Ultra. For more information, visit the ELO Web site at: `http://www.elotouch.com`
- Memory requirement tables are available on the Web at: `http://www.pc.ibm.com`

  At the site, select your country. Once inside the IBM Network Station home page, select **Support**. Then, select **Online Publications** to find the document entitled *NSM V2R1 - Memory requirements and performance recommendations*. Download and view or print this document.
- For information about AS/400 Client Access and integrating the AS/400 with your PC environment, visit the Web site at: `http://www.as400.ibm.com/clientaccess`
- The AS/400 Information Center can be used to find task and in-depth reference information on using AS/400 functions. The site can be accessed at: `http://www.as400.ibm.com/infocenter`
- For in-depth information about the AS/400 Setup Assistant in Version 1 Release 3, access related publications available at: `http://as400bks.rochester.ibm.com`
- XFree86 is a freely redistributable implementation of the X Window System that runs on UNIX and UNIX-like operating systems (and OS/2). More information on XFree86 can be found on the Web at: `http://www.xfree86.org`
- Windows NT product information can be accessed on the Web at: `http://techsupport.services.ibm.com/nc/`
- If you want to look at and modify certain UNIX files, use the free Programmer's Facility Editor (PFE). PFE can be downloaded from its author's site at: `http://www.lancs.ac.uk/people/cpaap/pfe`

- For information on the Java Communications Extensions, visit Sun Microsystems' Java Communications Extensions page at: http://java.sun.com/products/javacomm
- For information on the Java Plug-In and a complete description of how to modify the HTML code, visit Sun Microsystems' Java Plug-In page at: http://java.sun.com/products/plugin
- For more information on the Java Media Framework, visit Sun Microsystems' Java Media Framework page at: http://java.sun.com/products/java-media/jmf
- For more information on the Java Foundation Classes, visit Sun Microsystems' Java Foundation Classes page at: http://java.sun.com/products/jfc
- For information regarding Java security, refer to the Sun Microsystems' Java security FAQ at: http://java.sun.com/sfaq/index.html
- Download JDK 1.1.8 and JFC 1.1/Swing 1.0.3 from Sun's Web page at: http://www.sun.com
- For a comprehensive listing of the new functions in Netscape Communicator 4.5, visit the site at: http://home.netscape.com/eng/mozilla/4.5/relnotes/windows-4.5.html
- The Netscape Communicator 4.5 browser supports several hundred different preferences that can be used in the overrides.js file to customize the browser. A full list of the supported parameters can be found at the Netscape Web site at: http://developer.netscape.com/docs/manuals/deploymt/index.htm
- The Client Customization Kit can be downloaded free-of-charge from Netscape at: http://www.netscape.com/download/cck.html
- For a complete description of how to create an autoproxy configuration file, see the Netscape Web site at: http://home.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html
- Xpdf, a PDF viewer for X, can be downloaded from: http://www.foolabs.com/xpdf
- Information about the XAnim player for UNIX systems can be accessed at: http://xanim.va.pubnix.com
- Complete Host On-Demand product information can be accessed at: http://www.ibm.com/software/network/hostondemand
- Visit the Microsoft home page at: http://www.microsoft.com
- Citrix and MetaFrame information can be accessed at the Citrix home page at: http://www.citrix.com
- For information about Thin Client computing, visit the NCD Web site at: http://www.ncd.com
- Access update information and downloads of the third-party SNMP software kit called MIB Browser Professional Edition with MIB Compiler Version 5B (Evaluation edition) produced by MG-SOFT Corporation at: http://www.mg-soft.com/download.html
- For general help about assorted UNIX commands, refer to the NetBSD manual pages found via the NetBSD home page at: http://www.netbsd.org
- For Remote Control of Unix Netscape support documentation, visit the site at: http://home.netscape.com/newsref/std/x-remote.html

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** http://www.redbooks.ibm.com/

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  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.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the "How to Order" section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

IBM Redbooks fax 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

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at http://www.redbooks.ibm.com/
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-5844-00 IBM Network Station Manager V2R1
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	 O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. http://www.ibm.com/privacy/yourprivacy/

SG24-5844-00

Printed in the U.S.A.

IBM Network Station Manager V2R1

SG24-5844-00