# Network Station Manager for S/390

*To view or print the update, go to:http://www.as400.ibm.com/networkstation/s390*

SC31-8546-00

# Network Station Manager for S/390

*To view or print the update, go to:http://www.as400.ibm.com/networkstation/s390*

SC31-8546-00

**Note:**

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

This book is also available in a softcopy form that can be viewed with the IBM BookManager READ program.


## First Edition (June 1997)

This edition applies to OS/390 (5645-001) and TCP/IP and to TCP/IP Version 2 Release 4 for VM/ESA (5735-FAL). See the “Summary of Changes” for a description of the changes made in this edition. Make sure you are using the correct edition for the level of the product.

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

IBM welcomes your comments. A form for readers' comments may be at the back of this publication. If the form has been removed, you may send your comments to the following address:

International Business Machines Corporation
Department CGMD
P.O. Box 12195
Research Triangle Park, North Carolina 27709
USA

If you prefer to send comments electronically, use one of the following methods:

| | |
|---|---|
| Fax (USA and Canada): | 1-800-227-5088 |
| Internet e-mail: | usib2hpd@vnet.ibm.com |
| World Wide Web: | http://www.s390.ibm.com/os390 |
| IBMLink: | CIBMORCF at RALVM13 |
| IBM Mail Exchange: | USIB2HPD at IBMMAIL |

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

# Contents

# Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them 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 that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter described 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:

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:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

## Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AS/400
IBM
OS/390
OpenEdition
Operating System/2

OS/2
RS/6000
S/390
System/390
VM/ESA

The following terms are trademarks of other companies:

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Java, JavaSoft, and HotJava are trademarks of Sun Microsystems, Inc.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

# About IBM Network Station Manager for S/390, SC31-8546-00

## Who Should use this Guide

This information is for the person who is installing and administering the IBM Network Station Manager for OS/390 and for VM. This guide refers to you as the IBM Network Station administrator.

## Information Available on the World Wide Web

More of our product information is available on the World Wide Web. You can access this information from our product home page, which is at the following uniform resource locator (URL) address:

`http://www.as400.ibm.com/networkstation/s390`

# Chapter 1. Introduction to the IBM Network Station Manager

The IBM Network Station Manager is a desktop network computer that provides:

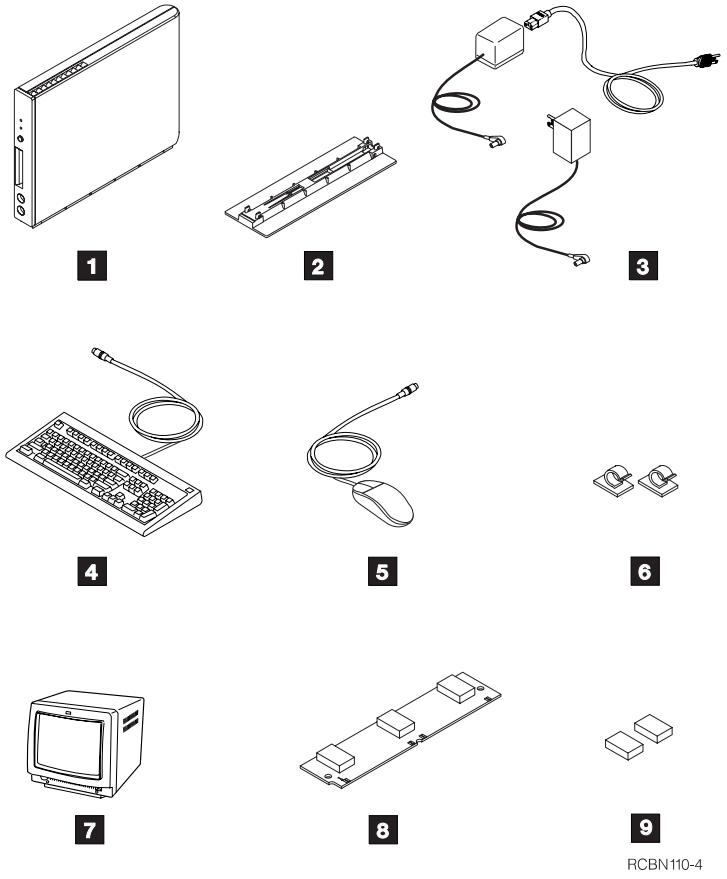
- Low cost of ownership
- Central management of software and data
- Access to the Internet and corporate intranets
- Simplicity in installation and administration
- Graphical interface with browser-based administration features

**About Names:** The name of this manual is the IBM Network Station Manager for S/390. This manual documents the licensed programs of IBM Network Station Manager for OS/390 and for VM/ESA.

Also discussed in this manual is a program used to administer IBM Network Stations. This program is the IBM Network Station Manager program. The name of the licensed program and the name of this administering program are very similar. When discussing the program that is used for administering IBM Network Stations, the text will read *IBM Network Station Manager program*. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for specific information.

## What Does an IBM Network Station Look Like?

The following diagram shows the components of the IBM Network Stations:




1 Logic unit
2 Logic unit base
3 Power module
4 Keyboard
5 Mouse
6 Cable clamps
7 Monitor
8 Memory SIMM
9 Video memory modules

## How Does the IBM Network Station Communicate with the Host?

The IBM Network Station for S/390 uses:

DHCP (Dynamic Host Configuration Protocol) for OS/390

BOOTP (Bootstrap Protocol) for VM

TFTP (Trivial File Transfer Protocol)

TIMED (Time Protocol) for OS/390

NSLD (Network Station Login Daemon)

## What is Dynamic Host Configuration Protocol (DHCP)?

DHCP is a TCP/IP protocol that enables you to centrally locate and dynamically distribute configuration information including IP addresses.

DHCP is based on the Bootstrap Protocol (BOOTP) and adds the capability of automatically allocating reusable network addresses and distributing additional host configuration options. DHCP clients and servers can use existing BOOTP relay agents. DHCP and BOOTP clients and servers can generally interoperate with one another.

See Chapter 5, “Configuring the Dynamic Host Configuration Protocol Server for OS/390” on page 5-1 for more information.

## What is Bootstrap Protocol (BOOTP)?

BOOTP is a TCP/IP protocol that is used to allow a diskless client (IBM Network Station) to request an IP address and the name of the load file.

When the BOOTP server receives a boot request, the server looks up the MAC address that is defined for the client. BOOTP then returns a reply with the IP address and the name and path of the load file that was requested. (The load file is the file that contains the operating system kernel for the client.) The client then initiates a TFTP request to the server for the load file.

The BOOTP server stores the IP address of the client and the name of the load file in a table. This table is called the BOOTP table.

See Chapter 6, “Configuring the Bootstrap Protocol Server for VM” on page 6-1 for more information.

## What is Trivial File Transfer Protocol (TFTP)?

TFTP is a TCP/IP protocol that is used to transfer files. TFTP can read or write files from or to a remote server. On the S/390 system, TFTP is a server that you can configure with the command line option during TFTP invocation. See Chapter 7, “Configuring the Trivial File Transfer Protocol Server” on page 7-1 for more information.

## What is Time Protocol Daemon (TIMED)?

TIMED is a TCP/IP daemon that is used to provide the time. TIMED gives the date and time.

## What is Network Station Login Daemon (NSLD)?

NSLD is a TCP/IP daemon that supports a Remote Authentication protocol to authenticate a user. NSLD provides the location of the user's preference files. See Chapter 8, “Configuring the Network Station Login Daemon Server” on page 8-1 for more information.

---

## How Do I Manage the IBM Network Stations?

There are several programs that are provided that allow you to manage the IBM Network Stations on a day-to-day basis. They are:

The IBM Network Station Manager program

The IBM Setup Utility

User Services

## What is the IBM Network Station Manager Program?

The IBM Network Station Manager program is a browser-based application that allows you to set and change settings for:

All or specific IBM Network Station users

All or specific IBM Network Station workstations

User settings can be for application programs (3270 emulation, 5250 emulation, browser sessions) or hardware settings such as mouse configuration or desktop background. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for a more detailed discussion.

## What is the IBM Setup Utility?

The IBM Setup Utility on the IBM Network Station allows you to **View** and then **Set** (change) configuration settings on a particular IBM Network Station. For example, you can view or set the MAC address or monitor resolution settings of any IBM Network Station.

The system administrator can access the IBM Network Station Setup Utility while the IBM Network Station is going through the boot-up process. See Chapter 12, “Working with the IBM Network Station Setup Utility” on page 12-1 for a more detailed discussion.

## What Are User Services?

User services are programs that provide users with tools to manage the IBM Network Station's operational environment.

Following are some of the user services:

Monitoring messages applicable to a specific IBM Network Station

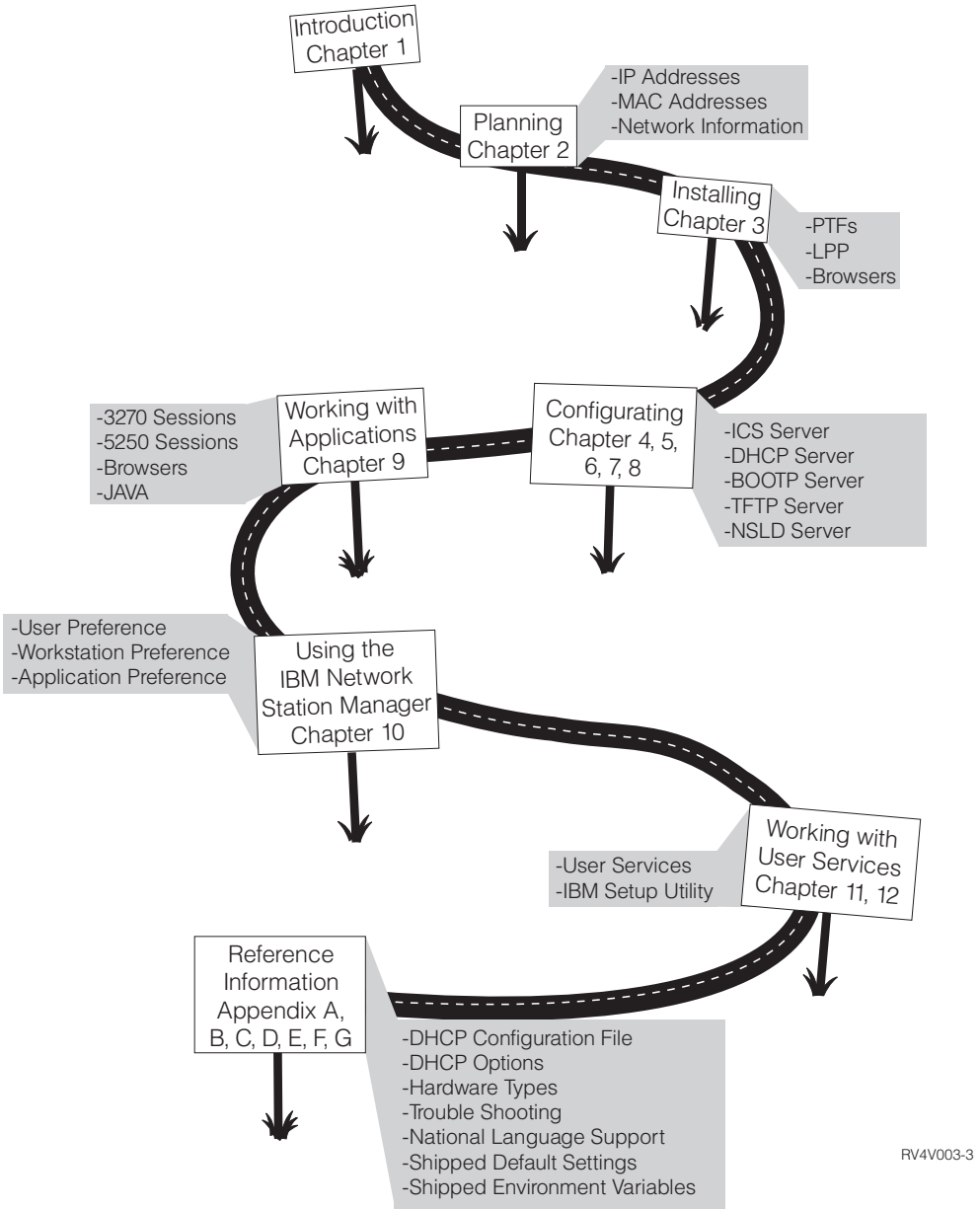
Locking your screen (with password control)

Monitoring statistics (for example, how much memory is available on a specific IBM Network Station)

See Chapter 11, “Working with User Services” on page 11-1 for a more detailed discussion.

## Using the IBM Network Station Roadmap

The following diagram represents a roadmap of the tasks you can perform while working with your IBM Network Stations. Follow the roadmap to facilitate smooth transition from planning, to installing, to configuring, to using.



# Chapter 2. Planning for the IBM Network Station Manager

As system administrator, you need to plan the integration of IBM Network Stations into your computing environment. A system administrator is a user that has root authority. A user ID with root authority (UID=0) installs and configures your system for Network Station use.

You must record some of the planning information that you gather on information charts. See Table 2-2 on page 2-13 to familiarize yourself with their contents. The following are the planning task divisions:

General planning

This section is not just for reading! These are tasks that you must complete before you move to the next planning section.

IBM Network Station planning

Use this information to define your IBM Network Stations.

Follow the configuration steps in the following chapters:

Chapter 4, “Configuring the Internet Connection Secure Server for OS/390” on page 4-1

Chapter 5, “Configuring the Dynamic Host Configuration Protocol Server for OS/390” on page 5-1 for OS/390

Chapter 6, “Configuring the Bootstrap Protocol Server for VM” on page 6-1 for VM

Chapter 7, “Configuring the Trivial File Transfer Protocol Server” on page 7-1

Chapter 8, “Configuring the Network Station Login Daemon Server” on page 8-1.

For additional VM configuration information, use the *TCP/IP for VM: Program Directory* to configure your servers and your *VM Web Server* documentation to configure your Web server.

## General Planning

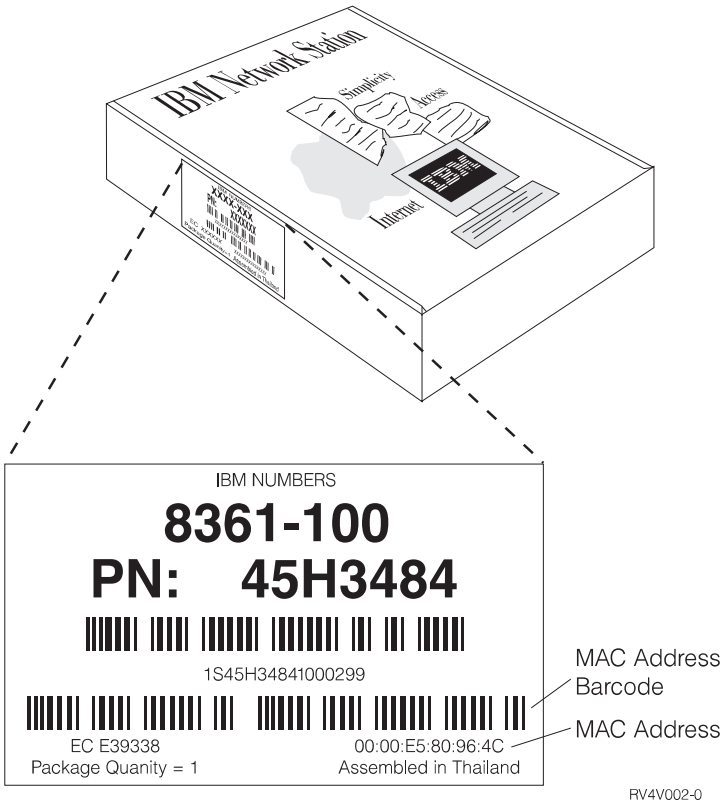
The general planning section contains mostly verification information to ensure that your host system and IBM Network Stations are ready to receive the software and hardware that is associated with IBM Network Stations.

__ 1. **Obtain the IBM Network Station Media Access Control (MAC) address (for VM).**

Use the MAC addresses to create BOOTP entries for assigning IP addresses.

You need to do this step for each IBM Network Station that you will be adding.

This address is on the box that the IBM Network Station system unit is packaged in. The following diagram shows the MAC address location on the box that contains the system unit:




**Note:** If you no longer have the box that the IBM Network Station system unit is packaged in, you may also find the MAC address through the Setup Utility:

a. Boot the Network Station.

b. Press the Escape key after the DRAM memory is tested during the boot.

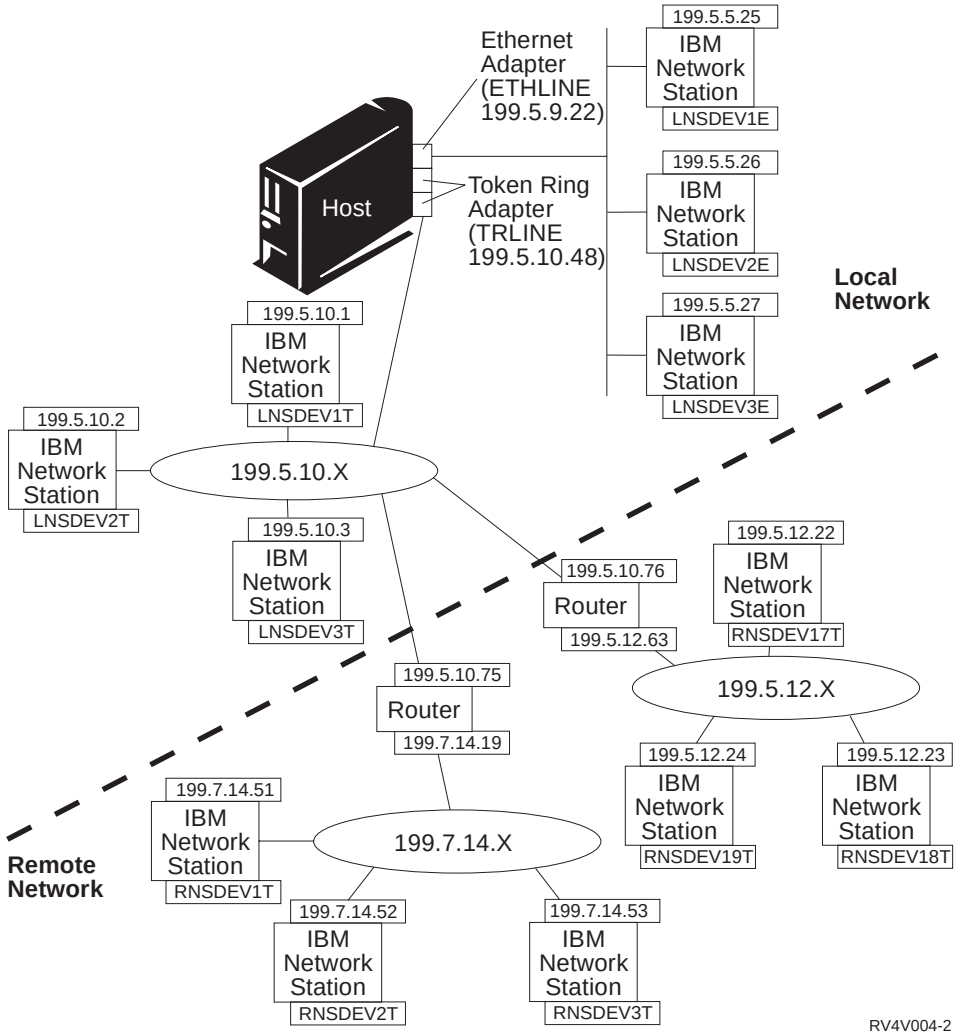
c. Press F4 to view the Hardware. You will find the MAC address here.

__ 2. **Familiarize yourself with your TCP/IP network.**

We recommend that you have a good working knowledge of your network. Having a topology map or diagram of your network will help you to more easily complete the planning tasks. Figure 2-1 on page 2-3 shows a physical rendering of a TCP/IP network with example addresses. Addresses from your network (similar to these) will be required on planning forms later in this section.

The following is information that relates to the network map that is presented in Figure 2-1.

```
System name:                HOSTTEST
Host Name:                  HOSTTEST
Domain Name:                MYCOMPANY.STATE.COM
Line Description:            ETHLINE  and TRLINE
ETHLINE Line IP Address:      199.5.9.22
TRLINE Line IP Address:       199.5.10.48
Device Naming:              L=Local, R=Remote, E=Ethernet, T=Token-Ri
      Local example name:    LNSDEV3E
      Remote example name:   RNSDEV2T
```




**Notes:**

1. The host can use the OS/390 or VM operating system. Other software contained in the the host includes the following:

   DHCP (for OS/390) or BOOTP (for VM)

   ICS (for OS/390)

   NSLD

   TFTP

   TIMED (for OS/390)

2. IBM Network Stations attached through any port other than the primary Home port and not attached through a relay agent must be configured using NVRAM settings.

*Figure 2-1. Sample TCP/IP Network Map*

__ 3. **Verify that you can configure your routers or gateways as DHCP or BOOTP relay agents.**

If your network uses routers or gateways, ensure that you can enable them to be DHCP or BOOTP relay agents. Enabling the routers or gateways for DHCP or BOOTP allows you to propagate (send) the DHCP or BOOTP packets across the network to other LAN segments.

If you can not configure routers to be DHCP or BOOTP relay agents, you could:

Use a UNIX system or RS/6000 system that has the necessary configuration support to receive limited DHCP or BOOTP broadcasts. Then forward those broadcasts to the appropriate host server.

Locate the host server on the same LAN segment as the IBM Network Stations. This would eliminate any need for routers or intermediate UNIX systems to pass on the broadcast requests of the IBM Network Stations.

__ 4. **Obtain IP Addresses and a Domain Name for your organization.**

Each node on a network is known as a host and has a unique address called an Internet Protocol (IP) address. This address is a 32-bit integer that is expressed in the form nnn.nnn.nnn.nnn.

For the networks within your organization, you can assign your own addresses. However, if you want to connect to the Internet, a central authority must officially assign the network addresses and domain names. The authority at the time of this writing is Network Solutions, Inc.. The address is:

```
Network Solutions
InterNIC Registration Services
505 Huntmar Park Drive
Herndon, VA 22070
1-703-742-4811
E-mail:  hostmaster@internic.net
WWW:  http://rs.internic.net/
```

**Note:** If your organization already has a range of IP addresses, you can use those instead of obtaining new IP addresses. For more information, see the *TCP/IP for MVS: Customization and Administration Guide*, SC31-7134 for OS/390 and the *TCP/IP for VM: Planning and Customization*, SC31-6082 for VM.

__ 5. **Verify that you have the correct PTF (Program Temporary Fix) media.**

As system administrator, you may need to install PTFs on your system. Check your program directory for the required PTFs.

__ 6. **Verify your Licensed Program Software and correct service for the IBM Network Station Manager.**

Verify that you have the correct licensed program software and correct service. You will install this software later.

**For OS/390**

Product Number is 5645-001. FMIDs are JTCP32G and JTCP32N.

**Notes:**

a. FMID JTCP32G contains the IBM Network Station software.

b. FMID JTCP32N contains the S/390 Host software.

**For VM**

TCP/IP 2.4.0 with PTFs UQ03096 and UQ03142.

**Notes:**

a. PTF UQ03096 contains the Server Support (BOOTPD, TFTPD).

b. PTF UQ03142 contains Release 1 of Client Code.

c. PTF which contains Release 2 of Client Code.

VM/ESA 2.1.0 with PTFs UM27709 and PTF UM28330 and APAR VM61222.

**Notes:**

a. PTF UM27709 and PTF UM28330 contain the CMS service.

b. APAR VM61222 contains the IBM Network Station Manager support.

VM/ESA 2.2.0 with PTF UM28331 and APAR VM61222.

**Notes:**

a. PTF UM28331 contains the CMS service.

b. APAR VM61222 contains the IBM Network Station Manager support.

__ 7. **Verify the IBM Browser Media.**

IBM offers a Web browser product for use on the IBM Network Station. This Web browser is the IBM Network Station Browser.

There are two versions of the IBM Browser licensed program. Licensed program 5648-B08 is a 40-bit RC4 encryption version and can be obtained free of charge. You can download it from an IBM Web page or order it from your IBM marketing representative.

The other version, 5648-B18, is a 128-bit RC4 encryption version. This version offers advanced encryption features for secure transactions on the Internet. You must purchase this version, and it is only available in the United States and Canada. To order, contact your IBM marketing representative.

__ 8. **Verify the Navio Browser Media.**

Another Web browser product for use on the IBM Network Station is the Navio NC Navigator Browser.

There are two versions of the Navio NC Browser licensed program. Licensed program 5648-B10 is a 40-bit RC4 encryption version and can be obtained free of charge. You can download it from an IBM Web page or order it from your IBM marketing representative.

The other version, 5648-B20, is a 128-bit RC4 encryption version. This version offers advanced encryption features for secure transactions on the Internet. You must purchase this version, and it is only available in the

United States and Canada. To order, contact your IBM marketing representative.

__ 9. **Verify IBM Network Station Memory Requirements.**

Verify that your IBM Network Stations have the amount of memory they will need to run the applications your users expect.

Each of the applications that are downloaded to the IBM Network Station requires memory. Use Table 2-1 on page 2-7 as a guide in determining how much memory each IBM Network Station should have.

**Notes:**

a. If some users require many different applications and if they will be using various IBM Network Stations, you will need to ensure each IBM Network Station has adequate memory to handle the projected applications.

b. Subsequent releases may have increased memory requirements.

*Table 2-1. Network Station Memory Requirements for Downloaded Software*

| **Software** | **Memory Requirement** |
|---|---|
| Base System, includes the following:<br>Motif Library<br>Window Manager<br>Fonts<br>IBM Login Utility | 5.35MB |
| 5250 Session (1st session)<br>Additional session<br>Help viewer<br>Keyboard remap<br>Color remap<br>Miscellaneous preferences | 1.4MB<br>0.3MB<br>0.3MB<br>0.55MB<br>0.45MB<br>0.35MB |
| 3270 Session (non-graphic)<br>Additional session (non-graphic) | 0.7MB<br>0.25MB |
| 3270 session (graphics)<br>Additional 3270 session (graphics) | 1.4MB<br>0.55MB |
| IBM Network Station Browser | 5.6MB |
| Navio NC Browser | 4.5MB |
| Java VM Session | 5.0MB default or 1.3MB in minimal configuration. Code size of each Java Applet must be added to either number.<br>**Note:** If you want to run large Java applications, you should calculate memory requirements from the default size of 4.2MB. |
| Video Memory Guidelines (Resolution)<br>800 x 600<br>1024 x 768<br>1280 x 1024<br>1360 x 1024<br>1600 x 1280 | 1MB<br>1MB<br>2MB<br>2MB<br>2MB |

# IBM Network Station Planning

This section will help you plan for DHCP for OS/390 and for BOOTP for VM.

# Planning for DHCP for OS/390

Before you implement DHCP in your network, there are some decisions that you need to make:

How many DHCP servers do you need?
Do you already have BOOTP servers in your network?
Do you have hosts with special requirements?
What is a reasonable lease time?

## How Many DHCP Servers Do You Need?

The number of servers that you need will depend largely on the number of subnets you have, the number of DHCP clients you plan to support, whether your routers are enabled with BOOTP Relay, and the lease time you choose. Keep in mind that the DHCP protocols do not currently define server-to-server communication. Thus, they cannot share information, nor can one DHCP server perform as a "hot backup" in case the other one fails.

DHCP clients send broadcast messages. By design, broadcast messages do not cross subnets. To allow the client's messages to be forwarded outside its subnet, your routers must be configured to forward DHCP requests using a BOOTP Relay agent. Otherwise, you will need to configure a DHCP server on each subnet.

***Using a Single DHCP Server:*** If you choose to use a single DHCP server to serve hosts on a subnet, consider the effects if the single server fails. Generally, the failure of a server will affect only DHCP clients that are attempting to join the network. Typically, DHCP clients already on the network will continue operating unaffected until their lease expires. However, clients with a short lease time may lose their network access before the server can be restarted.

***Using Multiple DHCP Servers:*** To avoid a single point of failure, you can configure two or more DHCP servers to serve the same subnet. If one server fails, the other can continue to serve the subnet. Each of the DHCP servers must be accessible either by direct attachment to the subnet or by using a BOOTP Relay agent.

Because two DHCP servers cannot serve the same addresses, address pools defined for a subnet must be unique across DHCP servers. Therefore, when using two or more DHCP servers to serve a particular subnet, the complete list of addresses for that subnet must be divided among the servers. For example, you could configure one server with an address pool consisting of 70% of the available addresses for the subnet and the other server with an address pool consisting of the remaining 30% of the available addresses.

Using multiple DHCP servers decreases the probability of having a DHCP-related network access failure, but it does not guarantee against it. If a DHCP server for a particular subnet fails, the other DHCP server may not be able to service all the requests from new clients which may, for example, exhaust the server's limited pool of available addresses.

However, you can bias which DHCP server exhausts its pool of addresses first. DHCP clients tend to select the DHCP server offering more options. To bias service toward the DHCP server with 70% of the available addresses, offer fewer DHCP options from the server holding 30% of the available addresses for the subnet.

## Do You Already Have BOOTP Servers in Your Network?

If you already have BOOTP clients and servers in your network, you may want to consider replacing your BOOTP servers with DHCP servers. DHCP servers can optionally serve BOOTP clients the same IP configuration information as current BOOTP servers.

If you cannot replace your BOOTP servers with DHCP servers and want to have both serve your network:

Turn off BOOTP support in your DHCP server
Make sure your BOOTP servers and DHCP servers do not give out the same addresses
Configure the BOOTP relay support in your routers to forward BOOTP broadcasts to both the appropriate BOOTP and DHCP servers

A DHCP server allocates a permanent IP address to a BOOTP client. In the event that subnets are renumbered in such a way that a BOOTP-assigned address is unusable, the BOOTP client must restart and obtain a new IP address.

## Do You Have Hosts with Special Requirements?

You may have hosts which have individual or special administrative needs, such as:

A permanent lease

You can assign permanent leases to designated hosts by specifying an infinite lease time. Also the DHCP server will allocate a permanent lease to BOOTP clients that explictly request it as long as support for BOOTP clients is enabled. The DHCP server will also allocate a permanent lease to DHCP hosts that explicitly request it.

A specific IP address

You can reserve a specific address and configuration parameters for a specific DHCP (or BOOTP) client host on a particular subnet.

Specific configuration parameters

You can allocate specific configuration information to a client regardless of its subnet.

Manually-defined workstations

You should explicitly exclude addresses from DHCP subnets for existing hosts that do not use DHCP or BOOTP for configuring their IP network access.

Although DHCP clients automatically check to see if an IP address is in use before allocating or using it, they will not be able to detect addresses of manually-defined hosts that are turned off or temporarily off the network. In that case, duplicate address problems may occur when a manually-defined host reaccesses the network, unless its IP address is explicitly excluded.

### What Is a Reasonable Lease Time?

The default lease time is 24 hours. The lease time you choose depends largely on your needs, including:

**The number of hosts to support compared to the number of available addresses.** If you have more hosts than addresses, you may want to choose a short lease time of one to two hours. This will help ensure that unused addresses are returned to the pool as soon as possible.

Keep in mind that the DHCP lease time you choose can affect your network operation and performance.

- Short lease times will increase the amount of network traffic due to DHCP lease renewal requests. For example, if you set a lease time of 5 minutes, each client sends a renewal request about every 2.5 minutes.
- Lease times that are too long, however, can limit your ability to reuse IP addresses. Very long lease times also delay configuration changes that occur when a client restarts or renews a lease.

**The time available to make network changes.** Hosts receive changes to configuration information when they are restarted or renew their lease. Be sure to allow a timely and adequate window to make these changes. For example, if you usually make changes overnight, you might assign a lease time of 12 hours.

**The number of DHCP servers that are available.** If you have only a few DHCP servers for a large network, you may want to choose a longer lease time to minimize the impact of server down-time.

For complex networks that need to support a combination of host leasing requirements, you can use DHCP classing. For more information, see Defining Classes.

Following is the specific information that is needed to identify each IBM Network Station to your network environment for OS/390. You should record this information. You need to provide the information once for each LAN:

__ 1. **Boot File Name**

The Boot File Name is the name of the file that the IBM Network Station will download and be used to boot the remote device. This is a constant and is prefilled on your form as *kernel*.

__ 2. **Boot File Path**

The Boot file path is the path name that is used to access the boot file on the host. This is a constant and has been prefilled on your form as */usr/lpp/tcpip/nstation/standard*.

## Planning for BOOTP for VM

This section will help you record the specific information that is needed to identify each IBM Network Station to your network environment for VM. You should record this information in Table 2-2 on page 2-13. Use this information to create a BOOTP entry for each IBM Network Station.

*The information that is contained on this form is LAN-specific*. You should fill out a separate form for each LAN to which you will be attaching IBM Network Stations. You need to provide the following information only once for each LAN:

__ 1. **Boot Type**

The Boot Type is already prefilled on your form as *IBMNSM*. This identifies this network device as an IBM Network Station.

__ 2. **Boot File Name**

The Boot File Name is the name of the file that the IBM Network Station will download and be used to boot the remote device. This is a constant and is prefilled on your form as *kernel*.

__ 3. **Boot File Path**

The Boot file path is the path name that is used to access the boot file on the host. This is a constant and has been prefilled on your form as */QIBM/ProdData/NetworkStation*.

__ 4. **Determine the Gateway IP address and Subnet Mask for Remote LANs**

If the LAN that you are attaching IBM Network Stations to is not directly attached to your host, it is referred to as a remote LAN. You will need to specify the IP Address of the IP Router/Gateway that your IBM Network Station will use to reach the host. You will also need to specify the subnet mask of this router. You should obtain this information from your network administrator.

__ 5. **Determine the Hardware Type of your IBM Network Stations**

Your IBM Network Stations can either attach to a token ring or ethernet LAN. If you will be attaching this IBM Network Station to a token ring network, then your IBM Network Station's hardware type is 6. If you will be attaching this IBM Network Station to a Version 2 (802.2) ethernet network, then your IBM Network Station's hardware type is 1. For IEEE (802.3) ethernet networks, the hardware type is 6, which is the same as a token ring network.

You will also need to complete the following tasks for each IBM Network Station that you will be adding to this LAN.

__ 1. **Assign a fully qualified host name to the IBM Network Station.**

The host name identifies the IBM Network Station as a unique destination within a TCP/IP environment. The fully qualified host name consists of two parts, the host name and the domain name. For example, ABCNSM.MYCOMPANY.STATE.COM is a qualifed host name, where ABCNSM is the host name and MYCOMPANY.STATE.COM is the domain name. The host name can be anything that is meaningful to you or the owner. You should obtain the domain name from your network administrator. For additional information, see the *TCP/IP for VM: Planning and Customization*, SC31-6082.

__ 2. **Record the Media Access Control (MAC) Address.**

The MAC address is a hardware-specific identifier that is unique to each IBM Network Station. You can find this address on the outside of the box that the IBM Network Station was shipped in. You should have captured this information in Step 1 of “General Planning” on page 2-1.

__ 3. **Assign an IP address to the IBM Network Station.**

Each IBM Network Station requires a unique IP address. You will need to assign a specific address to each IBM Network Station. You should ensure that the IP address is valid for your organization and that no other device in the network is using it.

## IBM Network Station Information for VM Chart

Use the information in Table 2-2 to install and configure your IBM Network Stations.

Complete one copy of Table 2-2 for each LAN adapter that has IBM Network Stations attached to it.

| *Table 2-2. IBM Network Station Information Chart* | | | |
|---|---|---|---|
| **IBM Network Stations** | | | |
| 1. Boot Type: IBMNSM | | | |
| 2. Boot File Name: kernel | | | |
| 3. Boot File Path: /QIBM/ProdData/NetworkStation | | | |
| 4. Gateway IP address (IBM Network Station side): | | | |
| 5. Router Subnet Mask (IBM Network Station side): | | | |
| 6. Hardware type (Token-Ring (6) or Ethernet (1)): | | | |
| IBM Network Station Unique Information | | | |
| 1. Host Name | 2. MAC Address | 3. IP Address | 4. Printer Type (MFRTYPMDL) |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Chapter 3. Installing the Network Station Manager

The IBM Network Station Manager uses several software products. You must install the software in the following order:

1. PTFs for S/390
2. IBM Network Station Manager software and corrective service

   **For OS/390**

   Product Number 5645-001 FMID JTCP32G and JTCP32N

   **Notes:**

   a. FMID JTCP32G contains the IBM Network Station software

   b. FMID JTCP32N contains the S/390 Host software

   **For VM**

   TCP/IP 2.4.0 with PTFs UQ03096 and UQ03142.

   **Notes:**

   a. PTF UQ03096 contains the Server Support (BOOTPD, TFTPD).

   b. PTF UQ03142 contains Release 1 of Client Code.

   c. PTF which contains Release 2 of Client Code.

   VM/ESA 2.1.0 with PTFs UM27709 and PTF UM28330 and APAR VM61222.

   **Notes:**

   a. PTF UM27709 and PTF UM28330 contain the CMS service.

   b. APAR VM61222 contains the IBM Network Station Manager support.

   VM/ESA 2.2.0 with PTF UM28331 and APAR VM61222.

   **Notes:**

   a. PTF UM28331 contains the CMS service.

   b. APAR VM61222 contains the IBM Network Station Manager support.

**Note:** If you delete the IBM Network Station Manager licensed program and then restore it, you will also have to restore the IBM Network Station Browser and the Navio NC Navigator Browser licensed programs. The browsers are separately orderable.

## Product Installation Methods

You can install the software products that are associated with the IBM Network Station Manager licensed program in the following ways:

Using media (tape) that you received from IBM

Go to “Installing from Tape” on page 3-2 to begin the process of software installation from media that you received from IBM.

Downloading the licensed program from an IBM Web site

Go to “Downloading and Installing IBM Network Station Products from an IBM Web Site” on page 3-2 to begin the process of software installation from an IBM Web site.

## Installing from Tape

To install the IBM Network Station Manager for OS/390, you must download the contents of the Network Station Manager tape. The *Network Station Manager Program Directory* that is shipped with the IBM Network Station Manager describes the procedure for installing the IBM Network Station Manager from the distribution tape. The *Network Station Manager Program Directory* contains the following information:

Basic and optional program materials and documentation

IBM support available

Program and service APARs and PTFs

Installation requirements and considerations

Installation instructions

**For OS/390**

Use the System Modification Program with Extended (SMP/E) to install the IBM Network Station Manager. For information on SMP/E, see *SMP/E Release 8.1 User's Guide*, SC28-1302.

**For VM**

For VM, use the Virtual Machine Serviceability Enhancements Staged with Extended (VMSES/E) to install the IBM Network Station Manager APAR. For information on VMSES/E, see *VMSES/E Introduction and Reference*, SC24-5747.

## Downloading and Installing IBM Network Station Products from an IBM Web Site

You can download IBM Network Station Manager from an IBM Web site. Following is important product information:

**For OS/390**

Product Number 5645-001 FMID JTCP32G and JTCP32N

**Notes:**

1. FMID JTCP32G contains the IBM Network Station software
2. FMID JTCP32N contains the S/390 Host software

**For VM**

TCP/IP 2.4.0 with PTFs UQ03096 and UQ03142.

**Notes:**

1. PTF UQ03096 contains the Server Support (BOOTPD, TFTPD).
2. PTF UQ03142 contains Release 1 of Client Code.
3. PTF which contains Release 2 of Client Code.

VM/ESA 2.1.0 with PTFs UM27709 and PTF UM28330 and APAR VM61222.

**Notes:**

1. PTF UM27709 and PTF UM28330 contain the CMS service.
2. APAR VM61222 contains the IBM Network Station Manager support.

VM/ESA 2.2.0 with PTF UM28331 and APAR VM61222.

**Notes:**

1. PTF UM28331 contains the CMS service.
2. APAR VM61222 contains the IBM Network Station Manager support.

Using any browser, go to URL:

**http://www.as400.ibm.com/networkstation/s390**

From the navigation bar at the bottom of the page, select ORDER for additional product information. From the selection list, select the version of software you want to order.

or

**http://www.ibm.com/nc**

From the navigation bar at the top of the page, select DOWNLOADS for additional product information. From the selection list, select the version of software you want to order.

Once you reach this Web page, first access the README file. The README file contains the necessary information for downloading PTFs, IBM Network Station programs, and other objects that are used to support downloading activities.

# Chapter 4. Configuring the Internet Connection Secure Server for OS/390

This chapter explains how to configure the Internet Connection Secure (ICS) server to support the IBM Network Station. To configure your IBM Network Stations, use the configuration information in this chapter. Refer to the *IBM Internet Connection Server Webmaster's Guide for OS/390*, GC31-8490 for additional details for the ICS server documentation.

Specifically, this chapter describes how to:

Set up the ICS server configuration file

Access the IBM Network Station Manager program

If you use the IBM Network Browser or the Navio NC Browser on the IBM Network Station Manager and your server has a port number other than the default (80), refer to “Changing the IBM Network Station Default Port Number” on page 10-18 for details for enabling the new port.

## Setting the ICS Server Configuration File

Before you can use the IBM Network Station Manager program, ensure that the following tasks have been completed:

1. The ICS server is installed.
2. The ICS server is started with root authority.
3. The URL maps to where the IBM Network Station Manager program has been installed.
4. The ICS server is configured to perform Basic Authentication before the IBM Network Station Manager program is invoked.

Refer to the ICS server program documentation for detailed instructions on how to update the ICS server configuration file (httpd.conf) and the syntax of the appropriate statements.

## Specifying the ICS Server User ID

To use the IBM Network Station Manager program, the Userid directive in the ICS server configuration file must specify a valid user ID that has root authority. The server must be invoked with root authority to validate users requesting services and to maintain a data base of user preferences (read/write) that can be accessed by all (read only).

## Mapping to the URL

Add the following sample request routing statements to the ICS server configuration file (httpd.conf):

```
Exec    /NetworkStation/Admin/*    /usr/lpp/tcpip/nsm/cgi-bin/QYTCMAIN
Exec    /NetworkStation/Dump/*     /usr/lpp/tcpip/nsm/cgi-bin/QYTCMDMP
Exec    /NetworkStation/cgi-bin/*.PGM  /usr/lpp/tcpip/nsm/cgi-bin/*
Pass    /NetworkStation/*         /usr/lpp/tcpip/nsm/*
```

*Figure 4-1. URL mapping*

**Notes:**

1. The /NetworkStation/Admin/ statement converts the URL which initially invokes the IBM Network Station Manager program into the specific program which will be invoked.

   The initial URL sets up the initial dialogue with the IBM Network Station Manager and is specified by users on their browsers as:

   ```
   http://yourservername:portnumber/NetworkStation/Admin
   ```

   where:

   *yourservername* is the host name or TCP/IP address of the ICS server

   *portnumber* is the port that is configured for use with the IBM Network Station program

   If you have not changed the default port number for the ICS server (80), you do not need to specify *portnumber*.

2. The /NetworkStation/Dump/ statement converts the URL which invokes the dump formatter.

3. The /NetworkStation/cgi-bin/ statement converts the call to the program contained in the HTML file to the library where the program is stored.

   The cgi-bin must be implemented with Basic Authentication which is used to verify that users are authorized to use the IBM Network Station Manager program.

4. The /NetworkStation/ statement enables the proper HTML and Image (GIFs) files to be displayed.

## Setting up Basic Authentication

Use Basic Authentication to protect the programs for the IBM Network Station Manager program. You can perform this authentication in one of the following ways:

Using ICS server function for authentication

Implementing an ICS server Internet Connection Application Programming Interface (ICAPI).

An ICAPI is a user-written exit that provides a program to verify that the user ID and password are authorized to use the system.

Refer to ICS server documentation for information on implementing an ICAPI.

### Using ICS Server function for authentication

Add the following protection setup directives to the ICS server configuration file.

```
Protection  PROT_NSM {
   Userid      %%SERVER%%
   PasswdFile   %%SAF%%
   PostMask    All@(*)
   PutMask     All@(*)
   GetMask     All@(*)
   Mask        All@(*)
   AuthType    Basic
   ServerId    NetworkStation_Manager
}

Protect /NetworkStation/cgi-bin/* PROT_NSM
```

*Figure 4-2. Protection with ICS Server interfacing to RACF (or equivalent system)*

With the protection directives shown in Figure 4-2, the server would activate protection as follows:

The Protect /NetworkStation/cgi-bin/ requests activate protection. The protection setup is defined on the Protection directive that has a label of PROT_NSM.

The server changes to the OpenEdition user defined on the Userid directive. This user ID must have root authority.

The text associated with ServerId is displayed by most Browsers on the screen and enables the user to verify that the user ID and password being entered are for the Network Station Manager program.

By specifying a unique ServerId for the Network Station Manager program, only IBM Network Station Manager program requests will be processed by the authenticated user. Because applications authenticated will be run as superusers , only IBM Network Station Manager program applications should be installed in the library specified by the URL mapping /NetworkStation/cgi-bin/*.

## Updating the NLSPATH variable

The NLSPATH variable for ICS server applications is defined in the file: /etc/httpd.envvars and may contain the following statements:

```
 NLSPATH=
/usr/lpp/internet/%N.cat:/usr/lib/nls/msg/%L/%N:/usr/lib/nls/msg/%L/%N.c
 LANG= en_US
 LIBPATH=/usr/lpp/internet/bin
```

*Figure 4-3. Sample /etc/httpd.envvars*

In the preceding example, the name associated with the Network Station Manager program catalog is:

```
/usr/lib/nls/msg/%L/%N.cat
```

The results returned for LANG= are substituted for the %L in the NLSPATH returned string and the %N is replaced with the file name of the file being

requested. This will result in the following file being opened for message catalog processing:

```
/usr/lib/nls/msg/en_US/nsmmsg.cat
```

**Note:** In the list of files defined for NLSPATH= do not code the real name of the IBM Network Station Manager program catalog (nsmmsg.cat). The file name should be represented by %N. Specifying the real file name for the IBM Network Station Manager message catalog (or any other catalog) may result in a failure by the application to access the catalog.

## Verifying the ICS Server NLSPATH setting

The ICS server may provide a script for displaying environment variables. This script is stored as

```
/usr/lpp/internet/ServerRoot/cgi-bin/environ.sh
```

With a properly configured server, this script can be invoked with the following URL:

```
http://yourservername:portnumber/cgi-bin/environ.sh
```

where:

*yourservername* is the host name or TCP/IP address of the ICS server

*portnumber* is the port that is configured for use with the IBM Network Station program

If you have not changed the default port number for the ICS server (80), you do not need to specify *portnumber*.

The ICS server provides a list of all environment variables and their current settings. Refer to the IBM Internet Connection Server product documentation for additional information.

If the environment variables script is not available, you can create an executable file and name it dispvar.scr. Figure 4-4 lists the information that should be placed in this file.

```
#! /usr/bin/sh
echo 'HTTP/1.0 200 OK'
echo 'Content-Type: Text/html'
echo ''
echo ''
echo '<HTML><BODY>'
echo 'NLSPATH='
echo $NLSPATH
echo 'LANG='
echo $LANG
echo '</BODY></HTML>'
```

*Figure 4-4. dispvar.scr*

**Note:** OpenEdition for MVS interprets the first line of this script to determine what script processor to use. This line may vary from installation to installation and may need to be changed accordingly.

After making the necessary change, store the script in an executable library accessible by the ICS server. Invoke this script interactively to verify that it works properly. It should echo back the HTML commands and the value of the NLSPATH should be substituted in place of the $NLSPATH.

If the script cannot be added to an existing library accessible by the ICS server, add a URL mapping record to the ICS server configuration file (httpd.conf) to enable the script to be found by the ICS server. A sample mapping record is listed below based on this file being created in a temporary directory in the /usr/lpp/tcpip directory structure.

```
Exec /dispvar/*    /usr/lpp/tcpip/tmp/dispvar.scr
```

After creating the preceding file, restart the ICS server to enable access to this script file.

To invoke the script from the browser, enter:

```
     http://yourservername:portnumber/dispvar
```

where:

*yourservername* is the host name or TCP/IP address of the ICS server

*portnumber* is the port that is configured for use with the IBM Network Station program

If you have not changed the default port number for the ICS server (80), you do not need to specify *portnumber*.

The results should be similar to the following:

```
 NLSPATH=
/usr/lib/nls/msg/%L/%N:/usr/lib/nls/msg/%L/%N.cat:
/usr/lib/nls/msg/en_US/%N
LANG= en_US
```

*Figure 4-5. Sample results of dispvar.scr execution*

## Accessing the IBM Network Station Server

After configuring the ICS server to support the IBM Network Station Manager program, restart the ICS server to activate the changes. You can take the following steps to validate that the IBM Network Station Manager program has been configured properly:

1. Display images of GIF files to verify accessibility to HTML and GIF files.
2. Start the IBM Network Station Manager program to verify Basic Authentication is active and programs can be executed.
3. Verify Message Catalog Accessible to verify that the IBM Network Station Manager program can access the message catalog.

## Displaying Images of GIF Files

Invoke the following URL listed to access the HTML directory and the directory where the GIF images are stored. A display of all application GIF files will be presented. No authentication should take place as the IBM Network Station Manager program does not require these directories to be protected.

```
http://yourservername:portnumber/NetworkStation/en_US/gifs.htm
```

where:

*yourservername* is the host name or TCP/IP address of the ICS server

*portnumber* is the port that is configured for use with the IBM Network Station program

If you have not changed the default port number for the ICS server (80), you do not need to specify *portnumber*.

## Starting the IBM Network Station Manager Program

From a frames-capable browser, start the IBM Network Station Manager program with the following URL:

```
http://yourservername:portnumber/NetworkStation/Admin
```

where:

*yourservername* is the host name or TCP/IP address of the ICS server

*portnumber* is the port that is configured for use with the IBM Network Station program

If you have not changed the default port number for the ICS server (80), you do not need to specify *portnumber*.

Log on with a user ID and password that have root authority. This ID will be treated as a system administrator. You must invoke authentication to ensure that the IBM Network Station Manager program functions properly.

### Possible Failure Conditions

Following are possible failure conditions which may occur if the IBM Network Station Manager program has not been configured properly:

Browser problems

Authentication error

Authentication error and catalog interface error

***Browser Problems:*** If a request for an executable is made to an object which cannot be executed, some browsers may hang or present a message, for example, "Document contains no data". Following are potential causes:

ICS Directive is not mapped to the proper executable.

Executable does not exist.

Executable is not readable by the ICS server.

Browser is not Java-script enabled.

Browser is not frames-capable.

Executable does not have the"sticky-bit" on.

For OpenEdition, executables which are to be executed from a partitioned data set must have the "sticky-bit" turned on.

All the executables in /usr/lpp/tcpip/nsm/cgi-bin/* for the Network Station Manager program must have this bit turned on. The contents of this file contains text similar to the following:

```
This file is not executable.
MVS loads the actual program from the partioned data set
because the stick bit is on.
```

The library containing the actual Network Station Manager program executables is not in the link list.

C++ DLL not in Link or LPA List

For systems that do not have the C++ Program Product installed, the C++ DLL Library is required for the Network Station Manager program to execute.

Correct the problem and retry the application.

***Authentication Error***

```
EZZ7354

(User:) Error during authentication for user.
```

*Figure 4-6. Authentication Error*

**Notes:**

1. Basic Authentication is not being performed by the IBM Internet Connection Server. IBM Network Station Manager program requires that Basic Authentication be performed before allowing any IBM Network Station Manager program functions to be performed.
2. This error is caused by the Internet Connection Server returning a null user ID and is usually caused by errors in the Internet Connection Server configuration file.

See “Setting up Basic Authentication” on page 4-2 for information on authentication.

***Authentication Error and Catalog Interface Error for OS/390***

```
Retrieval failed for the message

PSA_4_NSM_AUTHENTICATION_ERROR_MSG{1,5}(User:)
Error during authentication for user.
```

*Figure 4-7. Authentication Error and Network Station Manager Program Catalog Interface Error*

The preceding response is the result of two configuration errors.

1. Basic Authentication is not being performed by the IBM Internet Connection Server. IBM Network Station Manager requires that Basic Authentication be performed before allowing any IBM Network Station Manager functions to be performed. There are probably errors in the Internet Connection Server configuration files.

   See “Setting up Basic Authentication” on page 4-2 for information on authentication.

2. IBM Network Station Manager program could not access its catalog to properly display a message for the authentication failure.

   An internal representation of the message identifier is displayed beginning with PSA_. Sufficient information should be provided to enable the user to identify the error being reported.

   Verify that the IBM Network Station message catalog resides in a library specified by the NLSPATH variable of the ICS server and validate user preferences (read/write) that can be accessed by all (read only) for this file.

   See “Updating the NLSPATH variable” on page 4-3 for information on the NLSPATH= variable.

## Verifying Message Catalog Accessible for OS/390

From the Setup Tasks listed in the frame on the left, select the NSM Error Messages task at the bottom.

This task enables the Administrator to key in a message number and obtain a message description.

Key in a valid IBM Network Station Manager message number, such as 7350, and select the Submit key.

You will receive a response indicating if the message was successfully retrieved. Figure 4-8 shows a successful retrieval.

```
EZZ7350

(User: <User_name>) Unable to access HTML file <File_Name>
```

**Note:** Message has been successfully retrieved.

*Figure 4-8. Retrieval successful for the message*

## Message Failure

The message in Figure 4-9 indicates that the IBM Network Station Manager program could not access the message catalog.

```
Retrieval failed for the message
PSA_0_NSM_NO_TEMPLATE_MSG:{1,1} ...
```

**Note:** Message catalog is not properly configured.

*Figure 4-9. Retrieval failed for the message*

Verify that the message catalog has been placed in a directory which is accessible by the ICS server and contained in the NLSPATH variable and validate user preferences (read/write) that can be accessed by all (read only) for this file. See “Updating the NLSPATH variable” on page 4-3 information on setting the NLSPATH variable.

# Chapter 5. Configuring the Dynamic Host Configuration Protocol Server for OS/390

Dynamic Host Configuration Protocol (DHCP) allows clients to obtain IP network configuration information, including an IP address, from a central DHCP server. The DHCP serves controls whether the address they provide to clients are allocated permanently or are leased for a specific period. When a client is allocated a leased address, it must periodically request that the server revalidate the address and renew the lease.

The processes of address allocation, leasing, and lease renewal are all handled dynamically by the DHCP client and server programs and are transparent to you, the end user.

DHCP defines three IP address allocation policies:

**Dynamic** A DHCP server assigns a temporary, leased IP address to a DHCP client

**Static** A DHCP server administrator assigns a static, predefined address reserved for a specific DHCP client

**Permanent** A DHCP server administrator assigns a permanent IP address to a DHCP client. No process of lease renewal is required.

**Note:** If your network uses routers or gateways, you need to ensure that they can be enabled as DHCP relay agents. Enabling the routers or gateways for DHCP allows the DHCP packets to be sent across the network to other LAN segments.

If you do not have routers that you can configure to be used as DHCP relay agents, you could:

Use a UNIX system or RS/6000 system that has the necessary code to be configured to receive limited DHCP broadcasts. Then, forward those broadcast requests to the appropriate host server.

Use a host server that is located on the same LAN segment as the IBM Network Stations. This would eliminate any need for routers or intermediate UNIX systems to pass on the broadcast requests of the IBM Network Stations.

For dynamic address allocation, a DHCP client that does not have a permanent lease must periodically request the renewal of its lease on its current IP address in order to keep using it. The process of renewing leased IP addresses occurs dynamically as part of the DHCP and is transparent to the user.

## How Does DHCP Work?

DHCP allows clients to obtain IP network configuration information, including an IP address, from a central DHCP server. DHCP servers control whether the addresses they provide to clients are allocated permanently or are "leased" for a specific time period. When a client receives a leased address, it must periodically request that the server re-validate the address and renew the lease.

The DHCP client and server programs handle the processes of address allocation, leasing, and lease renewal.

To further explain how DHCP works, let's look at some frequently asked questions:

How is configuration information acquired?
How are leases renewed?
What happens when a client moves out of its subnet?
How are changes implemented in the network?

## Acquiring Configuration Information

DHCP allows DHCP clients to obtain an IP address and other configuration information through a request process to a DHCP server. DHCP clients use RFC-architected messages to accept and use the options served them by the DHCP server. For example:

1. The client broadcasts a message (containing its client ID) announcing its presence and requesting an IP address (DHCPDISCOVER message) and desired options such as subnet mask, domain name server, domain name, and static route.
2. Optionally, if routers on the network are configured to forward DHCP and BOOTP messages (using BOOTP Relay), the broadcast message is forwarded to DHCP servers on the attached networks.
3. Each DHCP server that receives the client's DHCPDISCOVER message sends a DHCPOFFER message to the client offering an IP address.

   The server checks the configuration file to see if it should assign a static or dynamic address to this client.

   In the case of a dynamic address, the server selects an address from the address pool, choosing the least recently used address. An address pool is a range of IP addresses to be leased to clients. In the case of a static address, the server uses a Client statement from the DHCP server configuration file to assign options to the client. Upon making the offer, the IBM DHCP server reserves the offered address.
4. The client receives the offer message(s) and selects the server it wants to use.
5. The client broadcasts a message indicating which server it selected and requesting use of the IP address offered by that server (DHCPREQUEST message).
6. If a server receives a DHCPREQUEST message indicating that the client has accepted the server's offer, the server marks the address as leased. If the server receives a DHCPREQUEST message indicating that the client has accepted an offer from a different server, the server returns the address to the available pool. If no message is received within a specified time, the server returns the address to the available pool. The selected server sends an acknowledgment which contains additional configuration information to the client (DHCPACK message).
7. The client determines whether the configuration information is valid. Upon receipt of a DHCPACK message, the IBM DHCP client sends an Address Resolution Protocol (ARP) request to the supplied IP address to see if it is already in use. If it receives a response to the ARP request, the client declines (DHCPDECLINE message) the offer and initiates the process again. Otherwise, the client accepts the configuration information.

8. Accepting a valid lease, the client enters a BINDING state with the DHCP server, and proceeds to use the IP address and options.

To DHCP clients that request options, the DHCP server typically provides options that include subnet mask, domain name server, domain name, static route, class-identifier (which indicates a particular vendor), user class, and the name and path of the load image.

However, a DHCP client can request its own, unique set of options. For example, Windows NT 3.5.1 DHCP clients are required to request options. The default set of client-requested DHCP options provided by IBM includes subnet mask, domain name server, domain name, and static route. For option descriptions, see Specifying DHCP Options.

## Renewing Leases

The DHCP client keeps track of how much time is remaining on the lease. At a specified time prior to the expiration of the lease, usually when half of the lease time has passed, the client sends a renewal request, containing its current IP address and configuration information, to the leasing server. If the server responds with a lease offer, the DHCP client's lease is renewed.

If the DHCP server explicitly refuses the request, the DHCP client may continue to use the IP address until the lease time expires and then initiate the address request process, including broadcasting the address request. If the server is unreachable, the client may continue to use the assigned address until the lease expires.

## Moving a Client Out of its Subnet?

One benefit of DHCP is the freedom it provides a client host to move from one subnet to another without having to know ahead of time what IP configuration information it needs on the new subnet. As long as the subnets to which a host relocates have access to a DHCP server, a DHCP client will automatically configure itself correctly to access those subnets.

For a DHCP client to reconfigure itself to access a new subnet, the client host must be rebooted. When a host restarts on a new subnet, the DHCP client may try to renew its old lease with the DHCP server which originally allocated the address. The server refuses to renew the request since the address is not valid on the new subnet. Receiving no server response or instructions from the DHCP server, the client initiates the IP address request process to obtain a new IP address and access the network.

## Implementing Changes in the Network?

With DHCP, you can make changes at the server, re-initialize the server, and distribute the changes to all the appropriate clients. A DHCP client retains DHCP option values assigned by the DHCP server for the duration of the lease. If you implement configuration changes at the server while a client is already up and running, those changes are not processed by the DHCP client until the client attempts to renew its lease or until it is restarted.

## Setting Up a DHCP Network

The following sections contain information to help you in setting up your DHCP system, see:

For planning recommendations, see “Planning for DHCP for OS/390” on page 2-8.
To create a scoped DHCP network, see “Creating a Scoped Network.”
To start the DHCP server, see “Starting the DHCP Server” on page 5-5.
For tips on maintaining a DHCP server, see “Maintaining the DHCP Server” on page 5-5.

The IBM DHCP server provides configuration information to clients based on statements contained in the server's configuration file and based on information provided by the client. The server's configuration file defines the policy for allocating IP addresses and other configuration parameters. The file is a "map" that the server uses to determine what information should be provided to the requesting client.

Before you start the DHCP server, create or modify the DHCP server configuration file.

Once the DHCP server is running, you can also make dynamic changes to the configuration by modifying the configuration file and using the DHCP Server Maintenance program to re-initialize the DHCP server. For more information on DHCP server initialization, see Re-initializing the Server.

## Creating a Scoped Network

You create a hierarchy of configuration parameters for a DHCP network by specifying some configuration values that are served globally to all clients, while other configuration values are served only to certain clients. Serving different configuration information to clients is often based on network location, equipment vendor, or user characteristics.

Depending on your configuration, you can specify subnets, classes, vendors, and clients to provide configuration information to different groups of clients:

When defined globally, client, vendor or class options are available to DHCP clients regardless of their network location.

Parameters specified for a subnet, class, or client are considered local to the subnet, class, or client. A client defined within a subnet inherits both the global options and the options defined for that subnet. If a parameter is specified in more than one level in the network hierarchy, the lowest level (which is the most specific) is used.

Use the Subnet statement to specify configuration parameters for one subnet for a specific location in your network or enterprise.

Use the Class statement to configure DHCP classes to provide unique configuration information from the server to clients that identify themselves as belonging to that class. For example, a group of clients can all use a shared printer or load image.

Use a Vendor statement to provide unique configuration information to clients that identify themselves as using a specific vendor's equipment or software. Specially-defined options may be served to these clients. For more information on defining vendors, see Defining Vendors.

Use a Client statement in the DHCP server configuration file to serve specified options to a specific client or to exclude that client from service. You can also use a Client statement to exclude IP addresses from service.

For more information on obtaining information for a DHCP client, see Maintaining the DHCP Server.

## Handling Errors in Configuration Files

Configuring the server incorrectly causes few, if any, warning messages. The DHCP server normally runs even when it encounters errors in the configuration file. The server may ignore the incorrect data and may optionally post a message to its log.

For more information on editing the server configuration file, see Appendix A, “Modifying the DHCP Server Configuration File” on page A-1.

## Starting the DHCP Server

When you are using Network Station Manager, DHCPSD is installed in the /usr/lpp/tcpip/nsm/sbin directory.

To start the DHCP server, use the following form of the **dhcpsd** command:

**dhcpsd [-q|-v] [-f configFile]**

**-q** Starts the server in **quiet** mode, which means that no banner is displayed when the server starts.

**-v** Starts the server in **verbose** mode. Causes messages dealing with client communication to print to screen.

**-f configFile**
Is the name of the DHCP server configuration file. By default, the server searches for a file called DHCPSD.CFG in the directory specified by the ETC environment variable.

or use a start procedure. When starting the DHCP server with a procedure (proc), the example start proc is found in the DHCP member of the install the partioned data set SEZAINST.

## Maintaining the DHCP Server

When you are using Network Station Manager, DADMIN is installed in the /usr/lpp/tcpip/nsm/sbin directory.

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

Re-initialize a DHCP server by causing the server to re-read its configuration file

Delete a lease

Control server tracing

Display client information

Display IP address information

Display server statistics

**Notes:**

1. This DHCP server release does not support earlier versions of dadmin clients. A new dadmin client that communicates with both previous and current releases of the DHCP server is provided with this release.
2. Verbose mode provides additional information for debugging purposes. Verbose mode is allowed on any of the following **dadmin** command instances. Verbose is shown as a parameter in those instances where additional, more detailed information is of particular value.

## Displaying dadmin Command Syntax

To display information about the command syntax, enter:

**dadmin -?**

## Re-initializing the Running Server

If you make changes to the configuration file, you will need to re-initialize the running server to implement the changes. To re-initialize the server, use the following form of the **dadmin** command:

**dadmin** [[**-h**]*host*] **-i** [**-v**]

**-h** Specifies the host

*host*
The IP address or host name of the DHCP server. If no server is specified, the local server is assumed.

**-i** Re-initializes the specified server.

**-v** Executes the command in verbose mode.

## Displaying Client Information

To display information for a client ID, use the following form of the **dadmin** command:

**dadmin -c***value* [**-v**]

**-c** Requests information for one or more clients that match this client ID.

*value*
The client ID is a MAC address. For example, enter 004ac77150fc. Information is returned for any matching hardware type.

**-v** Executes the command in verbose mode.

## Displaying IP Address Information

To display information for one IP address, use the following form of the **dadmin** command:

**dadmin -q***n.n.n.n* [**-v**]

**-q** Requests the IP address information.

*n.n.n.n*
The IP address of the client.

**-v** Executes the command in verbose mode.

## Querying an Address Pool

To display information for a pool of IP addresses, use the following form of the **dadmin** command:

**dadmin -p***n.n.n.n* [**-v**]

**-p** Requests the address pool information.

*n.n.n.n*
The IP address of the address pool.

**-v** Executes the command in verbose mode.

## Controlling Server Tracing

To start and stop tracing on the DHCP server, use the following form of the **dadmin** command:

**dadmin -t***value* [**-v**]

**-t** Specifies server tracing.

*value*
The value is ON to start tracing or OFF to stop tracing.

**-v** Executes the command in verbose mode.

## Displaying Server Statistics

To display statistics information about the pool of addresses administered by the server, use the following form of the **dadmin** command:

**dadmin** [[**-h**]*host* ] **-n***value* [**-v**]

**-h** Specifies the host

*host*
The IP address of the DHCP server. If no host is specified, the local server is assumed.

**-n** Requests statistics for the server specified as *host*.

*value*
The value is a decimal integer indicating the number of intervals from 0 to 100. For example, a value of three returns a summary record that includes totals information, the current interval record, and the 3 most recent history records. A value of 0 returns a summary record of activity since the last summary.

**-v** Executes the command in verbose mode.

Statistics include:

Discover packets processed

Discover packets with no response

Offers made

Leases granted

Negative acknowledgements (NAKs)

Informs processed, including informs plus acknowledgements (ACKs)

Renewals

Releases

BOOTP clients processed

proxyARec updates attempted

Unsupported packets

Monitor requests processed

For more information on defining statistics snapshots, see Defining Server and Lease Parameters.

### Deleting Leases

If you find that an assigned lease is not being used and you want to make the IP address available for allocation, you can delete the lease. You can only delete one lease at a time. You will be prompted to confirm deletion of the lease. To delete the lease, use the following form of the **dadmin** command:

**dadmin** [**-f**] [**-v**] [[**-h**]*host*]**-d***ip_address*

**-f** Forces deletion of the lease without prompting.

**-v** Executes the command in verbose mode.

**-h**

*host*
Specifies the IP address of the DHCP server. If no server is specified, the local server is assumed.

**-d** Deletes the lease for the specified IP address.

*ip_address*
The IP address for the lease to be deleted

## Configuring the DHCP Server for the IBM Network Station Client

You can configure the DHCP server to be used by an IBM Network Station. The DHCP server sets up the subnet and specifies the next bootstrap server. The IBM Network Station client can request information. The DHCP server should be configured to provide options that include subnet mask, router, domain name, and boot file name.

For option descriptions, see Appendix B, “Specifying DHCP Options” on page B-1.

## Multiple Local Subnet Restriction

The DHCP server allocates IP addresses from subnet pools based on information about the client's subnet determined from the incoming request packet. If no subnet information is found, the server defaults to allocating an IP address from the local subnet pool. The problem arises if the serving host machine supports multiple local subnets as shown in Figure 2-1 on page 2-3. Packets forwarded from a Relay Agent contain the remote subnet information. Packets arriving from clients on the

local LAN segments do not. In the current release of the DHCP server, the clients on the local Ethernet and token ring LAN segments receive the IP address from the same subnet pool. To avoid this problem, multiple local networks should be reconfigured to be remote with a router running the Relay Agent.

# Chapter 6. Configuring the Bootstrap Protocol Server for VM

Bootstrap Protocol (BOOTP) provides a dynamic method for associating workstations with servers and assigning workstation IP addresses and initial program load (IPL) sources. BOOTP and TFTP together provide support for the IBM Network Station for VM.

BOOTP is a TCP/IP protocol used to allow a *media-less* workstation (client) to request a file that contains initial code from a server on the network. The BOOTP server listens on the well-known BOOTP server port 67. When a client request is received, the server looks up the IP address defined for the client and returns a reply to the client with the client's IP address and the name of the load file. The client then initiates a TFTP request to the server for the load file.

You work with the BOOTP server to add or remove BOOTP entries for each IBM Network Station physically present in your network.

You work with the TCP/IP machine to specify the BOOTP startup parameters.

## Setting the BOOTP Server

The information necessary to run the BOOTP server is maintained in two files. The machine file contains the mapping between the client hardware address and IP address along with BOOTP data to be passed to the client. The configuration file contains information about which IP addresses to listen on and what BOOTP forwarding should occur, if any.

The files to be used are specified on the BOOTPD command. As part of the server initialization, it reads the machine and configuration files and maintains the information internally. You can change the data within the files and reload them while the server is running using the RELOAD subcommand.

For more information, see the *TCP/IP for VM Program Directory* and the *TCP/IP for VM Customization and Administration* manual.

# Chapter 7. Configuring the Trivial File Transfer Protocol Server

You will need to work with the Trivial File Transfer Protocol (TFTP) server to operate your IBM Network Stations.

The TFTP server enables the transferring of files to and from a remote server.

## Considerations for OS/390

When you are using IBM Network Station Manager, TFTP is installed in the /usr/lpp/tcpip/nsm/sbin/ directory.

**CAUTION:**
**The TFTP server uses well-known port 69. The TFTP server has no user authentication. Any client that can connect to port 69 on the server has access to TFTP. If the TFTP server is started without a directory, it allows access to the entire HFS. To restrict access to the HFS, start the TFTP server with a list of directories.**

You can start the TFTP server one of the following ways:

Using a shell script, nstftpd.

Issuing the tftpd command from the command line.

If you invoke the TFTP server outside the script, be sure to include:

```
tftpd -a /usr/lpp/tcpip/nstation/standard [/usr/lpp/tcpip/nstation/standard]
```

where the directory name in brackets ensures that the client code is accessible. Only specify the directory without the brackets if you are using the tftpd's command-line directory access control.

To start the TFTP server from the command line, type the tftpd command.

```
tftpd [-l] [-p port] [-t timeout] [-r maxretries] [-c concurrency_limit]
  [-s maxsegsize] [-f file] [-a archive directory [-a ...]]
  [directory ...]
```

Following are the parameters used for the tftpd command:

**-l** Logs all the incoming read and write requests and associated information to the system log. Logged information includes the IP address of the requestor, the file requested, whether the request was successful.

**-p port** Uses the specified port. The TFTP server usually receives requests on well-known port 69. You can specify the port in which requests are to be received.

**-t timeout** Sets the packet timeout. The TFTP server usually waits 5 seconds before presuming that a transmitted packet has been lost. You can specify a different timeout period in seconds.

**-r maxretries** Sets the retry limit. The TFTP server usually limits the number of retransmissions it performs because of lost packet to 5. You can specify a different retry limit.

**-c concurrency_limit** Sets the concurrency limit. The TFTP server spawns both threads and processes to handle incoming requests. You can specify the limit for the number of threads that may be concurrently processing requests under a single process. When the limit is exceeded, a new process is spawned to handle requests. The default is 200 threads.

**-s maxsegsize** Sets the maximum block size that can be negotiated by the TFTP block size option. The default is 8192.

**-f file** Specifies a cache file. You can specify a file containing information on files to be pre-loaded and cached for transmission. A cache file consists of one or more entries. For clarity, place each entry on a separate line. An entry has the form:

**a | b** <**pathname>**

where:

*a* indicates that the specified file is cached in ASCII form. The file is preconverted to netascii format.

*b* indicates that the specified file is cached in binary form, with no conversion.

Following are examples of cache file entries,

```
a  /usr/local/textfile
b  local/binaryfile
```

If a relative pathname to the file is specified, the TFTP server searches the specified directories for the file.

The cached version of a file is only used for requests requiring the specified format. For example, the binary cached version of a file is not used in satisfying a request for the file in netascii format. If a file is to be retrieved in both binary and ASCII formats, the user must specify that two copies of the file be cached with one in binary format, and the other in netascii format.

Caching is not dynamic. The cache files are read in when the TFTP server is started and are not updated, even if the file on disk is updated. To update or refresh the cache, the TFTP server must be recycled.

**-a archive directory** Specifies an archive directory. The files in this directory and its subdirectories are treated as binary files for uploading and downloading. This option is useful on EBCDIC machines that act as file servers for ASCII clients. Multiple -a options can be specified; one directory per -a option. Directories must be specified as absolute pathnames.

**Note:** For Network Station Manager, the root of the client code hierarchy (for example, /usr/lpp/tcpip/nstation/standard) should be specified as an archive directory.

**directory** Specifies an absolute path name for a directory. You may specify no more than 20 directories on the tftpd command line.

If the TFTP server is started without a list of directories, all mounted directories are considered active.

If a list of directories is specified, only those specified directories are active. That list is used as a search path for incoming requests that specify a relative path name for a file.

Activating a directory activates all of its subdirectories.

For a file to be readable by the TFTP server, the file must be in an active directory and have world ("other") read access enabled. For a file to be writable by the TFTP server, the file must already exist in an active directory and have world ("other") write access.

The TFTP server for OS/390 or MVS OpenEdition pre-forks a child process to handle incoming requests when the concurrency limit is exceeded. Consequently, immediately after starting the TFTP server, two TFTP processes exist.

In case of a flood of concurrent TFTP requests, the TFTP server may fork additional processes. When the number of concurrent requests being processed drops below the concurrency limit, the number of TFTP processes is decreased back to two.

To terminate the TFTP server, send a SIGTERM signal to the oldest existing TFTP process. This is the process that has a parent process ID of 1. Termination of this process will cause all of its children to terminate.

## Considerations for VM

The TFTP server transfers files between the Byte File System (BFS) and the TFTP clients. TFTP supports access to files maintained in a BFS directory structure that is mounted during initialization.

To configure the TFTP server, you must perform the following steps:

Update the TCPIP server configuration file.

Update the TFTPD profile exit.

Review and address additional configuration considerations.

Create the TFTPD PERMLIST data file.

Create the TFTPF USERLISR data file.

For details for configuring the TFTP server and using the TFTPD command and associated subcommands, see the *TCP/IP for VM Program Directory.*

# Chapter 8. Configuring the Network Station Login Daemon Server

You will need to work with the Network Station Login Daemon (NSLD) server to operate your IBM Network Stations in the OS/390 and VM environments.

The NSLD server performs user authentication and provides data for user configuration.

## NSLD for OS/390

The NSLD server responds to Network Station Login client requests for login information about the user ID logging into an IBM Network Station. The NSLD server first determines if the user ID and password combination passed is valid on this system. If it is not valid, an error response in sent to the client. If it is valid, the information passed back to the IBM Network Station includes the user's user ID and group ID, home directory, and Network Station Manager preference directory.

**Note:** The nsld code must be installed in an authorized library to determine user ID and password validity.

When you are using IBM Network Station Manager, NSLD is installed in the /usr/lpp/tcpip/nsm/sbin/ directory.

To start the NSLD server, type the nsld command from the command line.

```
nsld [-l] [-p port] [-t timeout] [-c concurrency_limit]
```

Following are the parameters used for the nsld command:

**-l** Logs the requests and replies. Information on each logon request and reply is logged to the system log. Logged information includes the type of the request or reply, the success or failure of requests, and the destination of replies. Errors and important events always are logged, even when this option is not specified.

**-p port** Uses the specified port. The NSLD server usually receives requests on well-known port 256. You can specify the port on which requests are to be received.

**-t timeout** Sets the packet timeout. The NSLD server usually waits 5 seconds before presuming that a transmitted packet has been lost. You can specify a different timeout period in seconds.

**-c concurrency_limit** Sets the concurrency limit. The NSLD server spawns both threads and processes to handle incoming requests. You can specify the limit for the number of threads that may be concurrently processing requests under a single process. When the limit is exceeded, a new process is spawned to handle requests. The default is 200 threads.

The NSLD server for OS/390 or MVS OpenEdition pre-forks a child process to handle incoming requests when the concurrency limit is exceeded. Consequently, immediately after starting the NSLD server, two NSLD processes exist.

In case of a flood of concurrent NSLD requests, the NSLD server may fork additional processes. When the number of concurrent requests being processed drops below the concurrency limit, the number of NSLD processes is decreased back to two.

To terminate the NSLD server, send a SIGTERM signal to the oldest existing NSLD process. This is the process that has a parent process ID of 1. Termination of this process causes all of its children to terminate.

## NSLD for VM

The NSLD server for VM responds to client requests for login information about a user ID on the system.

## Update the NSLD Profile EXEC

To invoke the NSLD server, add the nsld command to the PROFILE EXEC.

```
nsld [port] [([STAYUP|TRACE]
```

Following are the parameters used for the nsld command.

**port** Uses the specified port. The NSLD server usually receives requests on well-known port 256. You can specify the port on which requests are to be received.

**STAYUP** Indicates that the NSLD server should continue to operate if subsequent VM TCP/IP failures occur.

**TRACE** Indicates that the NSLD server should display trace information as requests are processed.

The NSLD server responds to Network Station Login client requests for login information about the user ID logging into an IBM Network Station. The NSLD server first determines if the user ID and password combination passed is valid on this system. If it is not valid, an error response in sent to the client. If it is valid, the information passed back to the IBM Network Station includes the user's user ID and group ID, home directory, and Network Station Manager preference directory.

**Note:** The NSLD user ID should have class B privilege class for determining user ID and password validity.

## NSLD Subcommands

You must be logged on to the NSLD server to use the NSLD subcommands. The NSLD subcommands are listed in Table 8-1 on page 8-3. Table 8-1 on page 8-3 provides the shortest abbreviation, and a description for each NSLD subcommand.

| *Table 8-1. NSLD Subcommands* | | |
|---|---|---|
| **Subcommand** | **Minimum Abbreviations** | **Description** |
| CMS | CMS | Passes a command to CMS for execution. |
| EXIT | EXIT | Stop the NSLD server and its processing. EXIT is equivalent to QUIT and STOP. |
| HELP | HELP | Displays a summary of NSLD subcommands. |
| QUIT | QUIT | Stops the NSLD server and its processing . QUIT is equivalent to EXIT and STOP. |
| STAYUP | STAYUP | Toggles the STAYUP mode of the NSLD server. |
| STOP | STOP | Stops the NSLD Server and its processing. Stop is equivalent to EXIT and QUIT. |

## Usage Notes

1. Do not issue any CMS command that would take considerable time to execute, for example, XEDIT. While the CMS command executes, the server does not respond to requests.
2. The CMS keyword is usually not required because the server will pass any command string that is not recognized as a NSLD subcommand to CMS. The CMS keyword is used to identify commands which would normally be interpreted as a subcommand, for example TRACE.

After completion of any command, the following ready prompt is displayed: `NSLD Ready;`

# Chapter 9. Logging on and Working with IBM Network Station Manager Applications

This chapter discusses how to log on to the IBM Network Station and work with various applications that are supported by the IBM Network Station. Topics are:

Logging on to the IBM Network Station

Working with applications such as:

- 3270 Emulation sessions
- 5250 Emulation sessions
- Browser sessions
- Java applications
- Java applets

## Login

After you power-on your IBM Network Station, the following login screen appears:

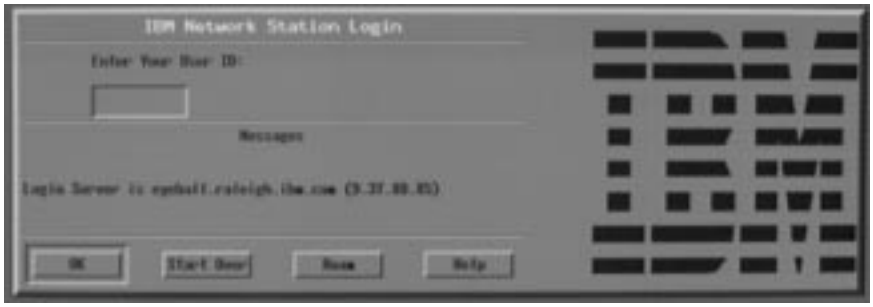



*Figure 9-1. IBM Network Station Login Screen*

Figure 9-1 shows the initial IBM Network Station login screen. Type your user profile name and press Enter. Type your password and press Enter.

The buttons within the menu bar are:

Ok

Clicking Ok sends request to server for processing.

Start Over

Clicking Start Over prompts for userid and password.

Roam

Clicking Roam allows you to specify the network server to log into.

Help

Clicking Help allows you to access Help for the IBM Network Station Manager program.

**Note:** The mouse must be inside the window to make the window active.

Figure 9-2 on page 9-2 shows the IBM Network Station menu bar, which contains the available applications to select. If any applications were specified to autostart by the IBM Network Station Manager (see Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for more information), they will appear on your screen. If no applications were set to autostart, select any applications that appear in your menu bar. Additional available application buttons are: 5250, the IBM Browser, and the Navio NC Browser.


*Figure 9-2. IBM Network Station Menu Bar*

The buttons within the menu bar are:

Log Out

Clicking Logout logs you off the IBM Network Station.

Hide

Clicking Hide makes the menu bar float out of view when you move the mouse pointer off the menu bar. To retrieve the menu bar, move your mouse pointer to the very bottom of your screen (If you clicked the Move to Top button, go to the very top of the screen instead) . This is useful if the menu bar covers part of an application window. Clicking the Hide button changes the button to Show and keeps the menu bar displayed on the screen.

Move to Top

Clicking Move to Top moves the menu bar to the top of the screen. The button will read Move to Bottom after the menu bar moves to the top. Clicking the Move to Bottom button, once the menu bar is located at the top, moves the menu bar back to the bottom.

Other buttons

Other buttons on the menu bar will be applications available to select and use.

Lock Screen

The Lock Screen button allows you to lock the screen when you leave the workstation. You will be prompted for a lock screen password.

## Working with the 3270 Application

The 3270 application provides access to a System/390. How a 3270 session is presented on the IBM Network Station depends on how you configured the session using the IBM Network Station Manager program.

If you used the Menu feature of the Startup function (within the IBM Network Station Manager program) and you added a New 3270 session labeled MY3270, that Menu button (labeled MY3270) will appear within the menu bar as shown in Figure 9-3 on page 9-3.

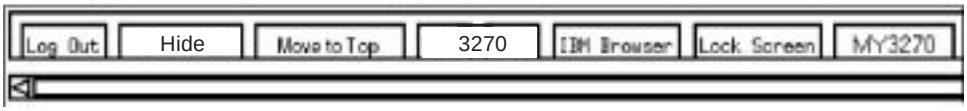



*Figure 9-3. IBM Network Station Menu Bar with NEW3270 Button*

If the 3270 session was set to autostart, a 3270 session will appear on the screen of your IBM Network Station as shown in Figure 9-4.


*Figure 9-4. 3270 Session Display*

If autostart was not specified, and you click the 3270 button within the IBM Network Station menu bar, a New 3270 Session window appears as shown in Figure 9-5 on page 9-4.


*Figure 9-5. New 3270 Session Dialog Box*

**Note:** You can use the name of the system or the IP address of the system to log on. To use a system name, you must set up name translation information in your TCP/IP configuration.

Depending on the volume of network traffic, you can expect it to take from several seconds up to a minute to see the Host Login Session screen appear.

## Learning About the 3270 Emulation Function

3270 emulation provides system users with greater function than they normally receive if they just use a 3270 nonprogrammable work station(NWS) to access a System/390. This additional function is available by clicking various pulldown options from the 3270 menu bar as shown in Figure 9-6 on page 9-5:

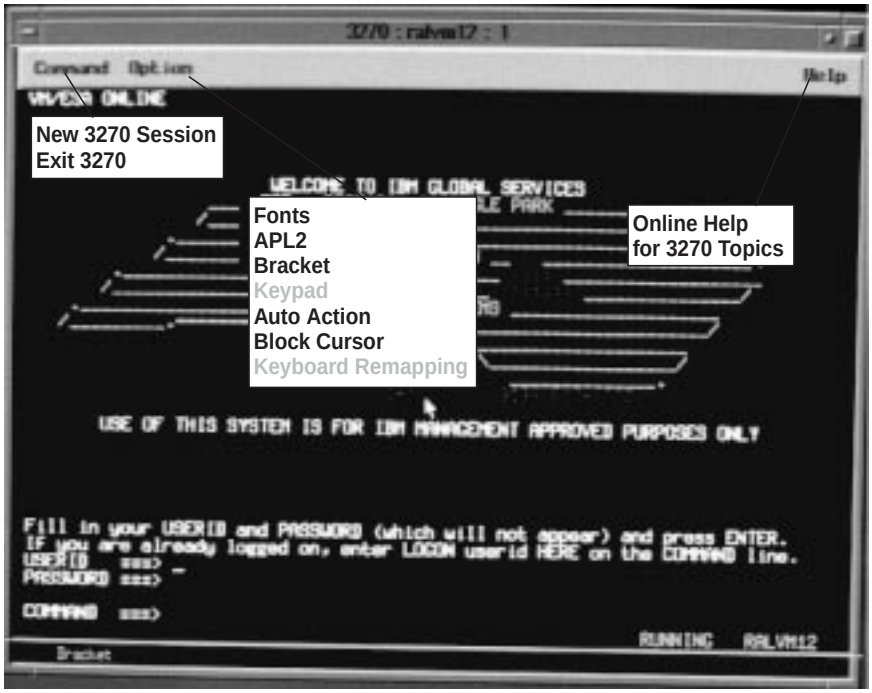



*Figure 9-6. 3270 Emulation Session with Expanded Pulldowns*

As shown in Figure 9-6, pulldowns are available to allow you to quickly access 3270 emulation functions such as font selection by session (Option pulldown) and online help (Help).

The following list contains some of the 3270 emulation support:

- Keyboard remapping[1]
- Graphics support[1]
- Choosing an Enter key location[1]
- Screen size support (for example: 24 x 80, 32 x 80, 43 x 80, and 27 x 132)[1]
- APL character mode support
- Pop-up keypad support[1]
- Copy and paste functions
- Auto action[1]
- Cursor style options (for example: underscore, block)
- Customizable window title[1]

All the 3270 emulation functions have shipped defaults. Those functions that are managed by the IBM Network Station Manager program also have IBM-supplied defaults. See Appendix F, “IBM Network Station Manager Program Shipped Default Settings” on page F-1 for a listing of all 3270 emulation defaults controlled by the IBM Network Station Manager program.

Accessing the 3270 emulation Help (clicking the Help button) will provide more information on how to make each of these 3270 emulation functions work.

---

[1] The IBM Network Station Manager program controls these 3270 emulation functions. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for more information. Also, the online help in the IBM Network Station Manager program provides more information along with all 3270 emulation default settings.

## Accessing Help

You can access help for the 3270 Emulator or your Host session.

For the 3270 emulator, place your mouse pointer in the emulator's menu bar and click Help. In general, to access help for the 3270 application, place your mouse pointer inside the Host session window and press F1.

## Working with the 5250 Emulation Application

The 5250 application provides access to a host system. How each 5250 session is presented on the IBM Network Station depends on how you configured the session using the IBM Network Station Manager program.

If you used the Menu feature of the Startup function (within the IBM Network Station Manager program), and you added a new 5250 session labeled MY5250, that menu button (labeled MY5250) will appear within the menu bar as shown in Figure 9-7.

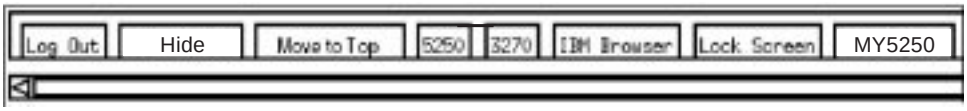



*Figure 9-7. Menu Bar with New 5250 Button - menu5250*

If, in the IBM Network Station Manager program, the 5250 session was set to autostart, a 5250 session will appear running on the screen of your IBM Network Station as shown in Figure 9-8.

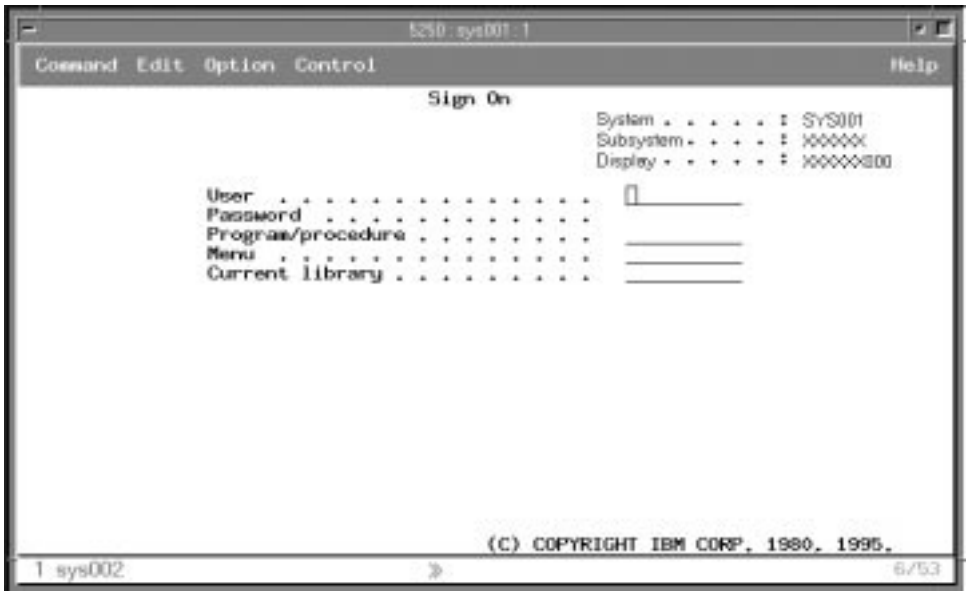



*Figure 9-8. 5250 Session Display*

If you click the 5250 button within the IBM Network Station menu bar, a New 5250 Session window appears as shown in Figure 9-9 on page 9-7.

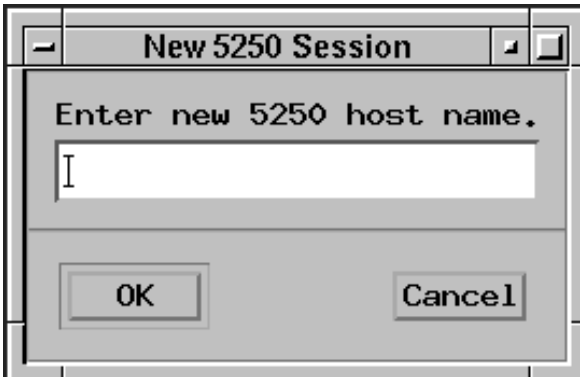



*Figure 9-9. New 5250 Session Dialog Box*

**Note:** You can use the name of the system or the IP address of the system to connect to or start a session. To use a system name, you must set up name translation information in your TCP/IP configuration.

Depending on the volume of network traffic, you can expect it to take from several seconds up to a minute to see the host sign-on display appear.

## Learning About the 5250 Emulation Function

5250 emulation provides system users with greater function than they normally receive if they just use a nonprogrammable work station (NWS) to access the system. This additional function is available by clicking various pulldown options from the 5250 menu bar as shown in Figure 9-10:

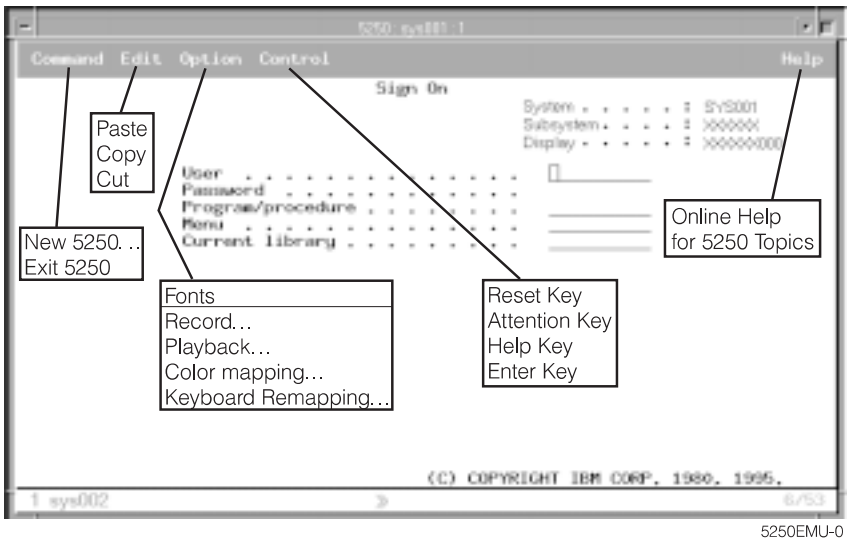



*Figure 9-10. 5250 Emulation Session with Expanded Pulldowns*

As shown in Figure 9-10, pulldowns are available to allow you to quickly access 5250 emulation functions such as multi-session support (Command pulldown), font selection by session (Option pulldown), and online help (Help).

The following list contains additional 5250 emulation support:

Keyboard remapping[2]
Color mapping (basic and advanced)[2]
Record/playback capability[2]
Autostart of playback file (from the Record/playback function)[2]
Auto-logon
Enter key location (you can specify your choice of key to be used for the Enter key)
Multiple screen size support (for example: 24 X 80, 27 X 132)
OV/400 controller text assist
Cut, copy, paste function[2]
Hotspot support
Cursor style options (for example, block or underscore)
Rule line support
Row and column indicator
Customizable window title[2]
Column separator function

All the 5250 emulation functions have shipped defaults. Those functions that are managed by the IBM Network Station Manager program also have IBM-supplied defaults. See Appendix F, “IBM Network Station Manager Program Shipped Default Settings” on page F-1 for a listing of all 5250 emulation defaults controlled by the IBM Network Station Manager program.

Accessing the online 5250 Emulation Help (by clicking the Help button) will provide more information on how to make each of these 5250 Emulation functions work.

## Accessing Help

You can access help for the 5250 Emulator or your host session.

For the 5250 emulator, place your mouse pointer in the emulator's Menu bar and click Help. To access help for S/390, sign on to the S/390, place your mouse pointer in the host session window and press F1.

## Working with the IBM Browser

The IBM Browser can provide access to the Internet. It is also used to access the IBM Network Station Manager program, which is used to manage IBM Network Station users and workstations. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for more information.

If you used the Menu feature of the Startup function (within the IBM Network Station Manager program) and you added an IBM Network Station Browser session labeled IBM Browser, that Menu button (labeled IBM Browser) will appear within the menu bar as shown in Figure 9-11 on page 9-9.

[2] The IBM Network Station Manager program controls these 5250 Emulation functions. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for more information. Also, the online help in the IBM Network Station Manager program provides more information along with all 5250 emulation default settings.


*Figure 9-11. IBM Network Station Menu Bar with IBM Browser Button*

If the IBM Browser session was set to autostart, an IBM Browser session will appear on the screen of your IBM Network Station as shown in Figure 9-12.


*Figure 9-12. IBM Browser Session Display*

If autostart was not specified, and you click the IBM Browser button within the menu bar, an instance of the IBM Browser appears.

Depending on the volume of network traffic, you can expect it to take from several seconds up to a minute to see the new IBM Browser screen appear.

## IBM Browser News - What is the Latest?

To find out the latest information about IBM Browser features and what is new with this level of the IBM Browser product, click Help on the IBM Browser main page.

Select the HELP Page option from the Help pulldown.

In the Contents frame, scroll to Frequently Asked Questions (FAQ) or the README items. Either of these items provide late-breaking information about the IBM Browser.

## IBM Browser Capabilities

Key IBM Browser features that are available in the first release of the browser include the following:

Ability to display Web pages that contain text, HTML, GIF images (including animated GIFs), and JPEG images

Javascript 1.1 or compatible

HTML 3.2

Frames

SSL 2 at 128 or 40 bit levels (in separate versions of the product, for US and Canada, or for export, respectively)

Java applets can be run by the IBM Network Station Java VM

## IBM Browser MIME Types:

*Table 9-1. IBM Browser MIME Types*

| TYPE/SUBTYPE | USAGE |
|---|---|
| **Text/plain** | Plain text with no HTML tags |
| **Text/HTML** | Text with HTML markup tags |
| **Image/gif** | GIF images, including animated GIFs |
| **Image/jpeg** | JPEG images |
| **Note:** No other MIME types are supported (because they require plug-ins or helper applications). | |

## IBM Browser URL Types Supported

The IBM Browser can handle the following URL types:

*Table 9-2. IBM Browser URL Types Supported*

| URL TYPE | USAGE |
|---|---|
| **HTTP** | Display content using HTTP protocol, such as any web page with HTML, and so forth |
| **HTTPS** | Same as HTTP, but using SSL security |
| **MAILTO** | Start the e-mail editor to create and send an e-mail message |
| **ABOUT** | Display copyright information about the browser |
| **FTP** | Open an FTP session |
| **JAVASCRIPT** | Run JavaScript |
| **VIEW SOURCE** | Display source file |

## Learning About IBM Network Station Browser Functions

The IBM Network Station Browser licensed program has many capabilities to help you manage Internet access and quick connection the IBM Network Station Manager program.

These functions, and others, are available by clicking various pulldown options from the IBM Browser menu bar as shown in Figure 9-13:

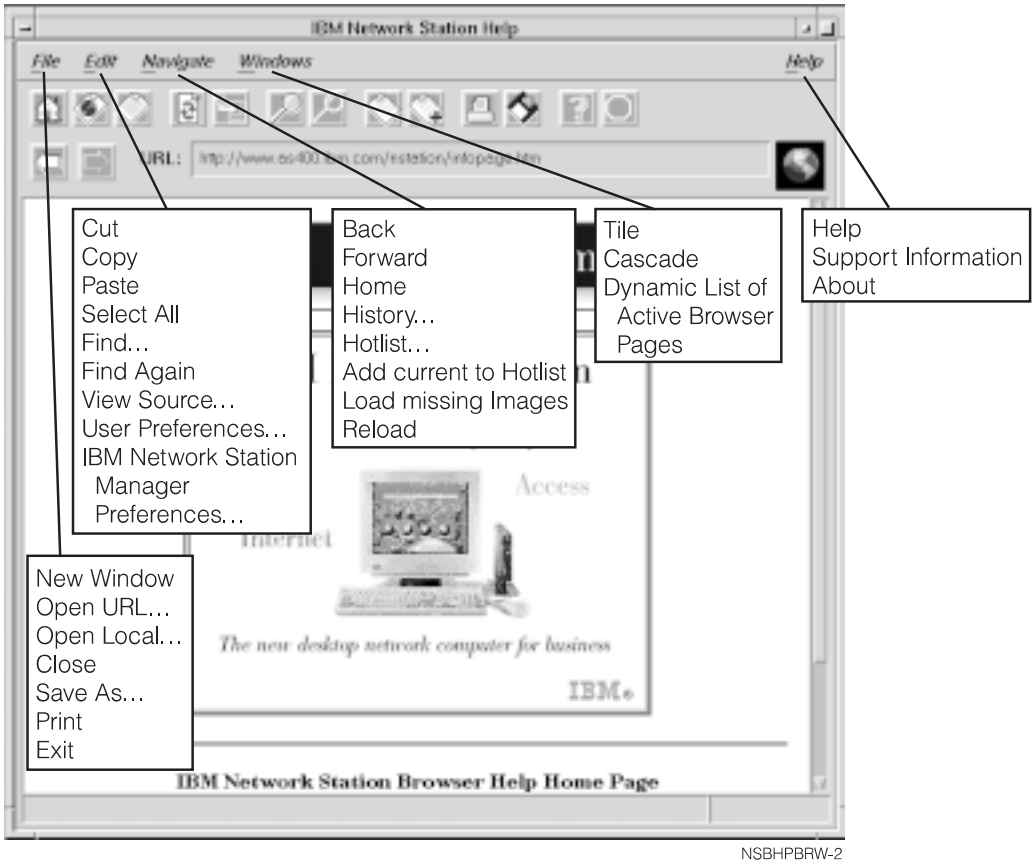



*Figure 9-13. IBM Network Station Browser with Extended Pulldowns*

As shown in Figure 9-13, pulldowns are available to allow you to quickly access IBM Browser functions such as multiple IBM Browser session support (New Window in the File pulldown), font selection by user (User Preferences in the Edit pulldown), and online help (Help).

The following list contains some of the IBM Network Station Browser support:

Open URL. . .

Open Local. . .

Opens an ASCII or HTML file.

Close

Save As. . .

Saves a file with user-specified name and file extension.

Print[3]

View Source. . .

Views the program source for the file in the current IBM Browser session.

User Preferences[3]

Allows configuration of fonts, colors, printing, caching and so on.

IBM Network Station Manager program preferences. . .

Provides a direct link to the IBM Network Station Manager program.

History. . .

Provides a list of web pages that were visited during the current IBM Browser session.

Hotlist

A list of frequently visited web pages. Access the web page by clicking the Hotlist entry.

Tile

Tile allows you to manage how multiple IBM Browser sessions will be presented on the display screen. For example, assume that you want four sessions. You can use the Tile function to specify two side-by-side sessions at the top of the display followed by two side-by-side sessions at the bottom of the display.

Cascade

Cascade allows you to manage multiple IBM Browser sessions on the display screen by layering one over the other. Each new session is slightly lower that the previous session, thus allowing a user to work with all active IBM Browser sessions.

Help Page

Allows a user to access Help for the IBM Browser through a Contents listing on this page. Key topics are the README and the Frequently Asked Questions (FAQ).

Support Information

Allows a user to view and save IBM Browser support information to a file.

Many of the IBM Browser functions have shipped defaults. Those functions that are managed by the IBM Network Station Manager program also have IBM-supplied defaults. See Appendix F, “IBM Network Station Manager Program Shipped Default Settings” on page F-1 for a listing of all IBM Browser defaults controlled by the IBM Network Station Manager program.

[3] The IBM Network Station Manager program controls these IBM Browser functions. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for more information. Also, the online help in the IBM Network Station Manager program provides more information along with all IBM Browser default settings.

## Accessing Help

You can access help for the IBM Browser via the Help menu option. The help includes a Frequently Asked Questions (FAQ) section, and an addendum for last-minute changes.

For IBM Browser help, place your mouse pointer in the IBM Browser Menu bar and click Help.

## Changing the IBM Browser Encryption Level for Improved Transaction Security

To change the IBM Browser encryption capability, use the IBM Network Station Manager program. You will need to work with the Internet Setup Task and select Network. Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 provides information on using the IBM Network Station Manager program.

---

## Working with the Navio NC Navigator Browser

Navio NC Navigator Browser can provide access to the Internet. It is also used to access the IBM Network Station Manager program, which is used to manage IBM Network Station users and workstations. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for more information.

If you used the Menu feature of the Startup function (within the IBM Network Station Manager program) and you added a new Navio NC Navigator Browser session labeled Navio Browser, that Menu button (labeled Navio Browser) will appear within the Menu bar as shown in Figure 9-14.


*Figure 9-14. IBM Network Station Menu Bar with Navio Button*

If the Navio NC Navigator browser session was set to autostart, an Navio NC Navigator browser session will appear on the screen of your IBM Network Station as shown in Figure 9-15 on page 9-14.

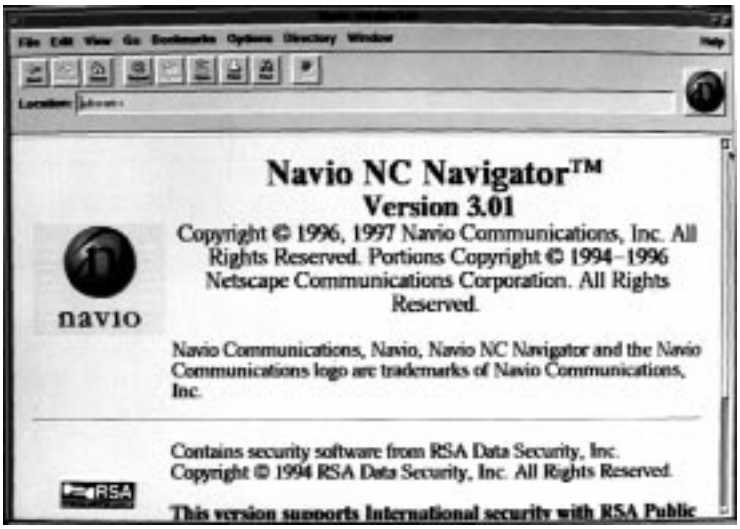



*Figure 9-15. Navio NC Navigator Browser Session Display*

If autostart was not specified, and you click the Navio button within the Menu bar, an instance of the Navio NC Navigator browser appears.

Depending on the volume of network traffic, you can expect it to take from several seconds up to a minute to see the new Navio NC Navigator browser screen appear.

## Navio NC Navigator Browser News - What is the Latest?

To find out the latest information about Navio NC Navigator browser features and what is new with this level of the Navio NC Navigator browser product, click Help on the Navio NC Navigator main page.

Select the HELP for Navio NC Navigator option from the Help pulldown.

In the Contents frame, scroll to Frequently Asked Questions (FAQ) or the README items. Either of these items provide late-breaking information about the Navio NC Navigator browser.

## Navio NC Navigator Browser Capabilities

In general, Navio NC Navigator is a compatible subset of the popular Netscape Navigator 3.01 browser (UNIX version). Key features that are available include the following:

Ability to display Web pages that contain text, HTML, GIF images (including animated GIFs), and JPEG images

Javascript 3

HTML Compatible with Navigator 3.01

Frames

SSL 2 and 3 at 128 or 40 bit levels (in separate versions of the product, for US and Canada, or for export, respectively) with server and client certificates

Java applets can be run by the IBM Network Station Java VM

## Navio NC Navigator MIME Types:

| *Table 9-3. Navio NC Navigator MIME Types* | |
|---|---|
| **TYPE/SUBTYPE** | **USAGE** |
| **Text/plain** | Plain text with no HTML tags |
| **Text/HTML** | Text with HTML markup tags |
| **Image/gif** | GIF images, including animated GIFs |
| **Image/jpeg** | JPEG images |
| **Note:** No other MIME types are supported (because they require plug-ins or helper applications). | |

## Navio NC Navigator URL Types Supported

The Navio NC Navigator Browser can handle the following URL types:

| *Table 9-4. Navio NC Navigator URL Types Supported* | |
|---|---|
| **URL TYPE** | **USAGE** |
| **HTTP** | Display content using HTTP protocol, such as any web page with HTML, and so forth |
| **HTTPS** | Same as HTTP, but using SSL security |
| **MAILTO** | Start the e-mail editor to create and send an e-mail message |
| **ABOUT** | Display copyright information about the browser |
| **FTP** | Open an FTP session |
| **JAVASCRIPT** | Run JavaScript |
| **VIEW SOURCE** | Display source file |

## Learning About Navio NC Navigator Browser Functions

The Navio NC Navigator browser licensed program has many capabilities to help you manage Internet access and quick connection to the IBM Network Station Manager program.

These functions, and others, are available by clicking various pulldown options from the Navio NC Navigator browser Menu bar as shown in Figure 9-16 on page 9-16:

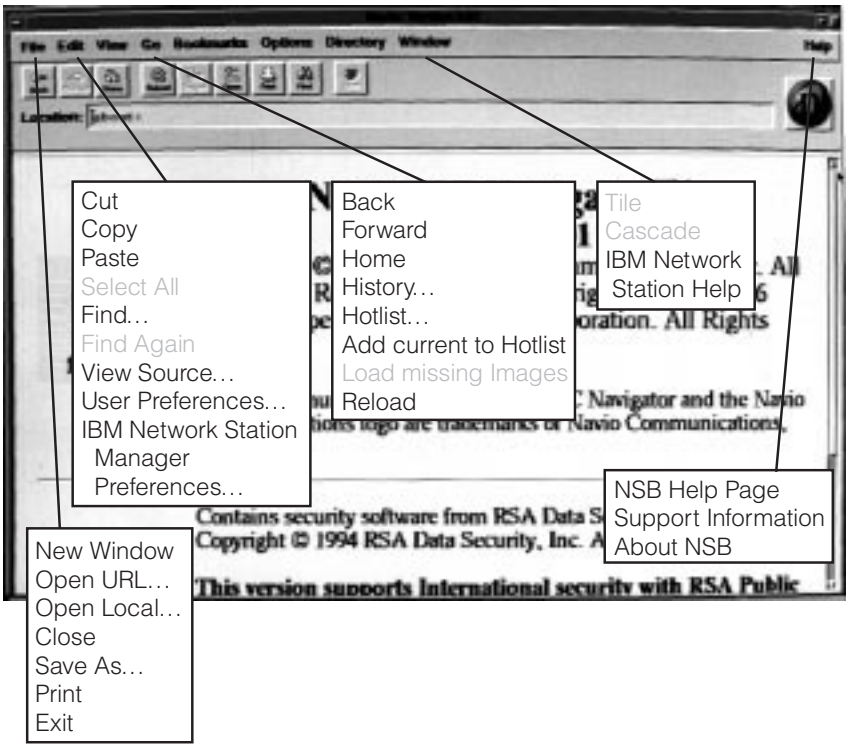



*Figure 9-16. Navio NC Navigator Browser with Extended Pulldowns*

As shown in Figure 9-14 on page 9-13, pulldowns are available to allow you to quickly access Navio NC Navigator functions such as multiple Navio NC Navigator browser session support (New Web Browser in the File pulldown), font selection by user (General Preferences in the Option pulldown), and online help (Help).

The following information presents and describes some of the Navio NC Navigator browser support.

## File Pulldown

The following Navio NC Navigator functions are available from the File pulldown:

**New Web Browser**
Provides another session of the Navio NC Navigator browser to appear on your screen.

**New Mail Message**
Provides the capability to address and send E-mail to another person. To use New Mail Message, you must have the Identity tab, located in the Options pulldown under Mail & News Preferences, completed.

**Mail Document**
Provides the capability to address and send documents to another person. To use Mail Document, you must have the Identity tab, located in the Options pulldown under Mail & News Preferences, completed.

**Open Location**
Provides the capability to specify a URL address that, when requested, is displayed in the browser window.

**Open File**
Provides the capability to specify a file that, when requested, is displayed in the browser window.

**Save as. . .**
Provides the capability to save (with a different name and file type) a document or file currently displayed in the browser.

**Print**
Provides the capability to specify how (paper size, print orientation, font, which pages, and so on) a document currently displayed in the browser will be printed.

**Close**
Provides the capability to close the current browser window. Any other browser windows remain open.

**Exit**
Provides the capability to close all browser sessions at once.

## Edit Pulldown

The following Navio NC Navigator functions are available from the Edit pulldown:

**Undo**
Provides the capability to undo or cancel the previous operation. For example, if you deleted a word and decided you did not want to, you could click undo and the word would return.

**Cut**
Provides the capability to delete specified pieces of a document.

**Copy**
Provides the capability to copy specified pieces of a document so that it can be pasted elsewhere.

**Paste**
Provides the capability to paste (or insert) specified pieces of a document that had been marked for either copying or cutting (deleting).

**Find**
Provides the capability to search a document for a specified word or text string.

**Find Again**
Provides the capability to search a document for multiple occurrences of a word or text string.

## View Pulldown

The following Navio NC Navigator functions are available from the View pulldown:

**Reload**
Provides the capability to reload (retrieve) the currently displayed page. You also have a Reload button in the Tool bar.

**Reload Frame**
Provides the capability to reload the active frame of a document currently displayed in the browser.

**Load Images**
Provides the capability to retrieve the images for the document currently displayed in the browser. Load Images only works if the Auto Load Images function (located in the Options pulldown) is off.

**Refresh**
Provides the capability to retrieve a new copy of the currently displayed document. The new copy is retrieved from cache, not from a server.

**Document Source**
Provides the capability to view the HTML source of the currently displayed document.

**Document Info**
Provides the capability to retrieve basic information about the currently displayed document. For example, creation date, date last modified, size, number of URL links on the page.

**Frame Source**
Provides the capability to view the HTML source for the active frame currently displayed in the browser.

**Frame Info**
Provides the capability to retrieve basic information about the active frame currently displayed in the browser. For example, creation date, date last modified, size, number of URL links on the page.

## Go Pulldown

The following Navio NC Navigator functions are available from the Go pulldown:

**Back**
Provides the capability to navigate backwards to previously accessed documents. Back is only active if you have been to one or more documents. A Back button is also available on the Tool bar.

**Forward**
Provides the capability to navigate forward to previously visited documents. Forward is only active if you have been to a document and then navigated (or moved) backwards. A Forward button is also available on the Tool bar.

**Stop**
Provides the capability to stop or end the activity of loading a new document to be displayed in the browser. A Stop button is also available on the Tool bar.

**Remainder of Go Pulldown**
Entries in the remainder of the Go pulldown represent URL locations that you have been to in the current browser session. You can access these locations by clicking on them or by pressing the listed combination of keys (usually Alt + a number).

## Bookmarks Pulldown

The following Navio NC Navigator functions are available from the Bookmarks pulldown:

**Add Bookmark**
Provides the capability of adding the URL of the currently displayed document to your list of bookmarks. Bookmarks is a list of URLs that a user frequently

visits. Placing the URL in the Bookmark list gives a user quick access to those URLs.

**Remainder of Bookmarks Pulldown**
Entries in the remainder of the Bookmarks pulldown represent URL locations that can be accessed by clicking them. To change or delete items that you have added to this list, use the Bookmarks item on the Window pulldown.

## Options Pulldown

The following Navio NC Navigator functions are available from the Options pulldown:

**General Preferences...**
Provides the capability to customize browser appearance, browser fonts, and how images are handled by the browser.

**Mail and News Preferences...**
Mail and News Preferences consists of the following tabs:

Compose

Provides the capability to specify how E-mail is handled when it is mailed.

Servers

Provides the capability to view the name of the SMTP server.

Identity

Provides the capability of identifying yourself and your organization for the purpose of using E-mail and the sending of documents.

**Network Preferences**
Network Preferences consists of the following tabs:

Cache

Provides the capability to clear memory caches and specify how often cached documents are verified.

Connections

Provides the capability to specify the number of connections to an internet server and to determine the size of the network buffer (amount of data Navio NC Navigator can receive in a transmission).

Proxies

Provides the capability to view your proxy configurations. You have to work with the network administrator to understand or change any proxy configurations.

Protocols

Provides the ability for you to be notified before accepting a cookie from a remote server. A cookie is a mechanism that allows a server to remember information about you that the server can use in subsequent sessions.

Languages

Provides the capability to view how Java and JavaScript are configured. Java and JavaScript are controlled by the IBM Network Station Manager program. Work with your system administrator if changes need to be made to the configuration of Java or JavaScript.

**Security Preferences**

Security preferences consist of the following tabs:

General

Provides the capability to set an alert when entering, leaving, viewing, or submitting a document insecurely. These alerts can also remind you of when you change levels of security.

Passwords

Provides the capability to specify that a password be required from people who want to access your computer.

Personal Certificates

Provides validation of who you say you are when attempting to access a secure server. Personal certificates are password protected (from the password tab). To obtain personal certificates you have to contact companies that issue personal certificates. If a personal certificate is issued, it is typically downloaded to your computer and accessible through the browser. You can view or delete personal certificates. However, you can not edit or modify personal certificates.

Site Certificates

Provides validation that this user, on this machine (the site), is who they say they are while attempting to access a secure server. Site certificates can be issued by secure servers. They are typically downloaded to your computer and accessible through the browser. You can view or delete site certificates. However, you can not edit or modify site certificates.

**Show Menubar**

Provides the capability to have the Menu bar displayed or not displayed during a browser session. The Menu bar contains the File, Edit, View, Go, Bookmarks, Options, Directory, Window, and Help pulldowns. If you deselect Show Menubar, the Menu bar immediately disappears from the browser. To retrieve the Menu bar, press the right mouse button and select Show Menubar.

**Show Toolbar**

Provides the capability to have the Toolbar displayed or not displayed during a browser session. The Toolbar provides buttons for Back, Forward, Home, Reload, Images, Open, Print, Find, and Stop buttons. If you deselect Show Toolbar, the Toolbar immediately disappears from the browser. To retrieve the Toolbar, select the Options pulldown and select Show Toolbar.

**Show Location**

Provides the capability to enter a URL directly from the keyboard and show the URL for the current document.

**Show Directory Buttons**

Provides the capability to display or not display directory buttons. Directory buttons provide users with quick access to specified URLs. Directory buttons are best used to provide access to certain URLs for all users. Directory buttons are similar to Bookmarks; however, Bookmarks are generally used for personal preference rather than for a whole organization. Directory buttons, when specified, appear below the Location field in the browser. Directory buttons are managed through the IBM Network Station Manager program. No Directory buttons will be shown unless they have been defined by your installation.

**Auto Load Images**

Provides the capability to have images loaded automatically or not at all when a document is requested. You may want to select this option if you are browsing documents on remote servers. Auto Load Images works in conjunction with the Load Images item in the View pulldown. If Auto Load Images is disabled, images can be loaded for a particular document by using the Load Images function under the View pulldown.

**Save Options**

Provides the capability to immediately save any changes made to any Options.

## Directory Pulldown

The following Navio NC Navigator functions are available from the Directory pulldown:

**Navio's Home**

This Directory entry provides a link to Navio's home page.

You must be able to access the Internet to use this item.

**IBM Network Computing**

This Directory entry provides a link to IBM's Network Computing home page.

You must be able to access the Internet to use this item.

**IBM Home Page**

This Directory entry provides a link to IBM's corporate home page.

You must be able to access the Internet to use this item.

**IBM Network Station Manager for (your system name appears here)**

This Directory entry provides a link to the IBM Network Station Manager program for the server system that your IBM Network Station was loaded from. This program is used to manage all IBM Network Stations and their users. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1 for more information.

## Window Pulldown

The following Navio NC Navigator functions are available from the Window pulldown:

**Address Book**

Provides the capability to compile a book of names and addresses of individuals or groups you correspond with on a regular basis. This item is used for sending mail.

Search, editing, and filing capabilities are also provided in the Address Book function.

**Bookmarks**

Provides the capability to file, edit, and manage your personal lists of bookmarks.

The Bookmark function activities you perform are reflected in the list of bookmarks that you can view using the Bookmarks pulldown in the Tool bar. For example, if you have two bookmarks whose names are very similar, you could edit one of them and add a text string that more readily identifies the bookmark when you access the Bookmarks pulldown.

**History**
Provides the capability to view a list of documents you have accessed during this session.

From this list you can create bookmarks for documents previously accessed or go directly to any selected document.

**Remainder of Window Pulldown**
The remainder of the Window pulldown contains a list of documents you have accessed during this session. You can access the document by pressing the push button next to it.

### Help Pulldown

The following Navio NC Navigator functions are available from the Help pulldown:

**About Navio NC Navigator**
Provides the version level and trademarking information about Navio NC Navigator.

**Help for Navio NC Navigator**
Provides help information and Frequently Asked Questions (FAQs).

**Navio NC Navigator Handbook**
Provides additional information about using the browser.

Many of the Navio NC Navigator browser functions have shipped defaults. Those functions that are managed by the IBM Network Station Manager program also have IBM-supplied defaults. See Appendix F, “IBM Network Station Manager Program Shipped Default Settings” on page F-1 for a listing of all Navio NC Navigator defaults controlled by the IBM Network Station Manager program.

## Accessing Help

You can access help for the Navio NC Navigator browser using the Help menu option. The help includes a Frequently Asked Questions (FAQ) section, and an addendum for last-minute changes.

For Navio NC Navigator browser help, place your mouse pointer in the Navio NC Navigator browser Menu bar and click Help.

---

## JAVA VM

You can set up Java applets and applications by using the IBM Network Station Manager. The applets and applications can be set to either autostart (they appear running on your workstation when you login) or set as menu items (they appear as buttons in the menu bar).

**Note:** Only a single Java application can run within the IBM Network Station and, if running, also precludes applets from running in both the desktop and in the browser.

The Java Virtual Machine (JVM) and the supporting class packages that were installed with the product together provide an environment for programs that were written and compiled in the Java programming language. The current level of Java that is supported by the IBM Network Station is equivalent to the 1.0.2 level distribution of the Java Development Kit (JDK) from JavaSoft. You can start and configure Java programs through the IBM Network Station Manager program.

## What Is Java?

Java is an object-oriented programming language. Java is compiled into a byte code stream which JVM interprets at runtime. Java programs are portable and, in general, may be run on any computer that supports a JVM. This is one of the primary attractions of the Java language.

## What do I do with Java?

In order to use Java, you must first obtain a program that was written in Java. This may be a program that you have purchased, downloaded from the Internet, or written and compiled by yourself. In general, the IBM Network Station is not geared towards being a development platform; therefore any significant program should be developed on another platform before loading it on the IBM Network Station.

## What are Java Applications and Applets?

There are two kinds of Java programs: those which are intended to be transferred and run across the Internet (applets), and those which run as programs from the local file system (applications). The first variety, applets, are designed so that they utilize a browser to provide windows and graphical layout for the applet. In general, these applets are not trusted by the browser since they are downloaded across the Internet and there is no way of knowing the intent of the author. Therefore, the browser has the ability to restrict applets from reading or writing to local files and from connecting to machines other than the machine from which they are downloaded. These restrictions are intended to protect the user from malicious programs and provide a safe environment to examine programs on the Internet.

## Starting an Application

An application must be installed on the file system of the server - Hierarchical File System in the case of the S/390.

**Notes:**

1. Only a single Java application can run within the IBM Network Station and, if running, also precludes applets from running in both the desktop and in the browser.
2. In order to run a Java application, the IBM Network Station Manager program must be used to either autostart the application or create a button on the IBM Network Station menu bar.

## Starting an Applet

Applets can be installed on the file system of the server that is your boot host, or downloaded from a remote system by using a Uniform Resource Locator (URL). The applet to load is specified through tags on an HTML page.

Applets can be run three different ways:

By creating a button on the IBM Network Station menu bar for an applet

By creating a button for a browser URL

By starting a browser then loading an HTML page which contains an applet

Configuration of the applet is managed through parameter tags within the HTML file (the specific parameter names are determined by the applet vendor). Applets that

load from the file system of your boot host should be well-known and trusted applets (the source of the applets is reliable). There are no security restrictions placed on applets that run from the local file system, so the applet may write to files and communicate with other machines (which may be desirable if you are saving your spreadsheet, but it would be a problem if a malicious applet decided to erase your files).

## Where do I find Additional Information on Java?

You can find additional information at the following web sites.

JavaSoft home page:

```
http://www.javasoft.com
```

IBM Java home page:

```
http://www.ibm.com/java
```

# Chapter 10. Using the IBM Network Station Manager Program

The IBM Network Station Manager program is a browser-based application program. This application program allows you to perform the setup and management tasks that are associated with one or all of your IBM Network Stations and IBM Network Station users. Setup Tasks are:

Hardware configuration:

Examples of configurable Hardware settings are: specifying primary mouse buttons (left or right-handed), mouse pointer speeds, screen savers, desktop background, and more.

Startup application and program selection

- Programs and menus

  Examples of configurable Startup settings are 5250 sessions, 3270 sessions, remote program sessions, Java application or applets, and IBM Network Station Browser sessions.

- Environment variables

  Environment variable settings are also configured under Startup. Environment variables can be used with Startup programs, menus, or any applications that are running on the IBM Network Station.

Desktop Management

Examples of configurable Desktop settings are screen colors for window frames, Icon placement, Font selection, and specifying how windows on the workstation are made active.

3270 Session configuration

Examples of configurable settings for 3270 sessions are screen size, key remapping capability, color customization, and 3270 sessions with graphics support.

5250 Session configuration

Examples of configurable settings for 5250 sessions are screen size, key remapping capability, color customization (basic and advanced), record/playback, and edit/copy/paste functions.

Internet configuration

- Network

  Examples of configurable Network settings are E-Mail address, default home page, proxy settings, and encrypted or non-encrypted version of the IBM Network Station Browser.

- IBM Browser

  Examples of configurable IBM Browser settings are disk caching, auto loading of images, print headers and footers, and print margins.

- Navio NC Browser

  Examples of configurable Navio NC Browser settings are caching, auto loading of images, and network buffer size.

- Java Applet Viewer

Examples of configurable Java applet viewer settings are message style, heap and stack size settings, and defining properties.

This application also allows you to view the error messages generated by the Network Station Manager program. This facility is limited to the Network Station Manager administrator only.

This chapter discusses the following IBM Network Station Manager program topics:

IBM Network Station Manager program overview

- Who can use the IBM Network Station Manager program
- Working with IBM Network Station Manager defaults
- Working with settings

Starting the IBM Network Station Manager program. This section discusses:

- Starting the IBM Network Station Manager program from a web browser
- Signing onto the IBM Network Station Manager program

Working with the IBM Network Station Manager program - Examples

Viewing Network Station Manager Error Messages

## IBM Network Station Manager Program - an Overview

Figure 10-1 on page 10-3 provides a graphical view of how the IBM Network Station Manager program flows. Take a moment to study Figure 10-1 on page 10-3; it highlights the differences between the defaults and setup tasks that a system administrator and end user can work with.

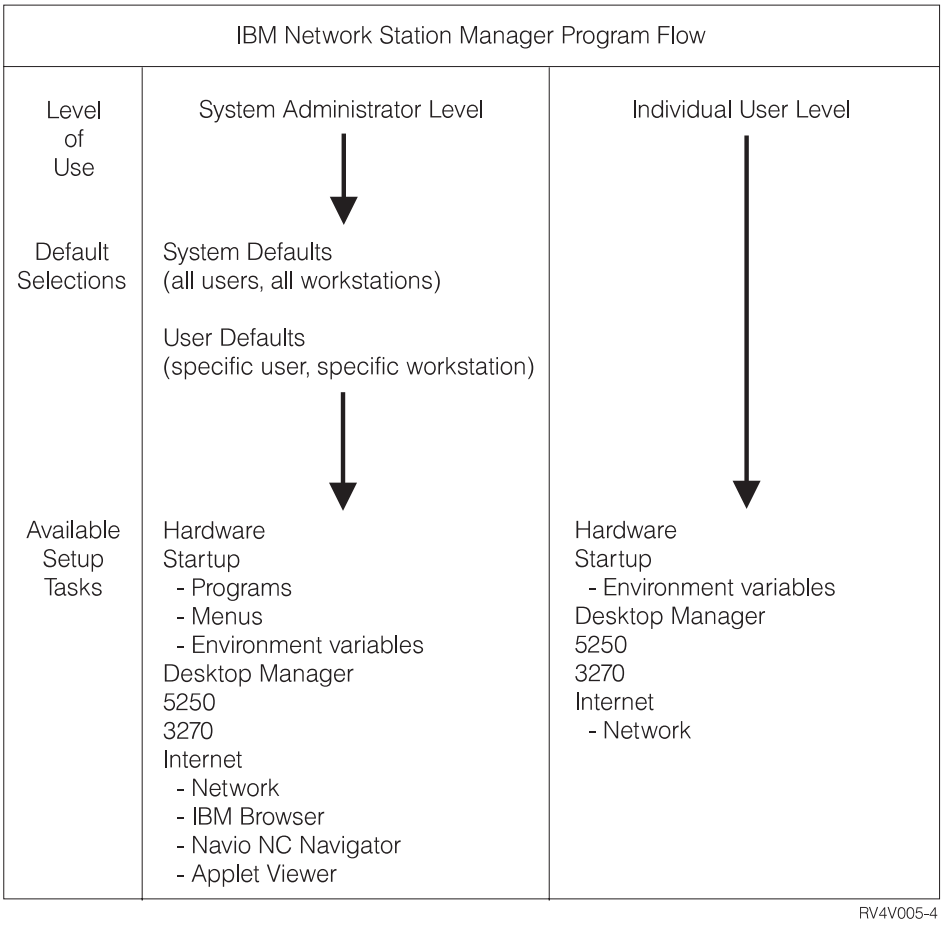



*Figure 10-1. IBM Network Station Manager Program Flow*

## Who can use the IBM Network Station Manager Program?

As shown in Figure 10-1, both system administrators and individual end users can access and use the program.

### System Administrators

System administrators are users having root authority and can work at a level that is either system-wide or specifically for one user or one workstation. For example, an administrator could specify that all IBM Network Station users will have one 3270 emulation session available and that one particular user could have an additional 3270 emulation session.

For information on how to sign on to the IBM Network Station Manager program, see “Starting the IBM Network Station Manager Program using a Browser” on page 10-8.

Figure 10-2 on page 10-4 shows the screen a system administrator sees after signing onto the IBM Network Station Manager program. Notice the range of functions presented in the Setup Tasks frame.

**Note:** This screen can vary in how it appears depending on the web browser you are using.

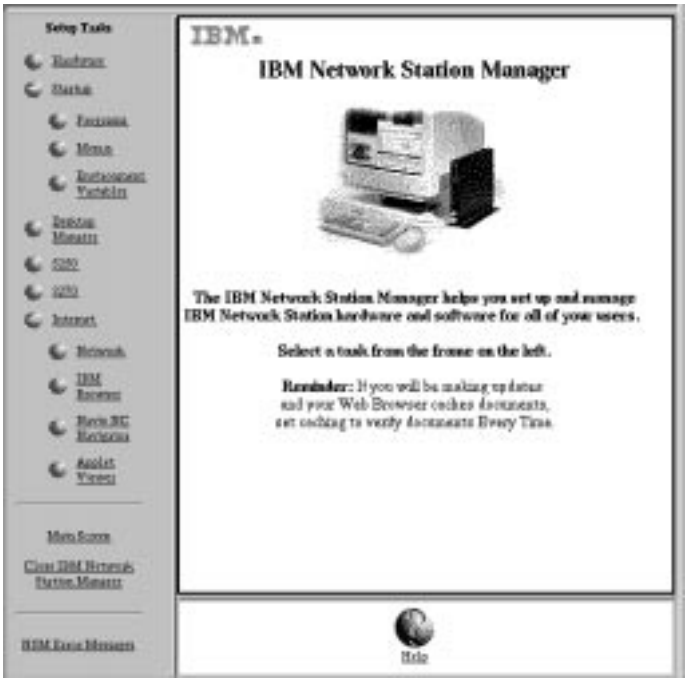



*Figure 10-2. System Administrator Level*

Compare these functions to the range of functions that are available to individual end users as shown in Figure 10-3 on page 10-5.

## Individual End Users

End users also have access to the IBM Network Station Manager program. However, the functions that an end user can work with are limited to settings that pertain only to themselves.

The following diagram shows the screen that an end user would see after signing onto the IBM Network Station Manager program. Notice the range of functions presented in the Setup Tasks frame.

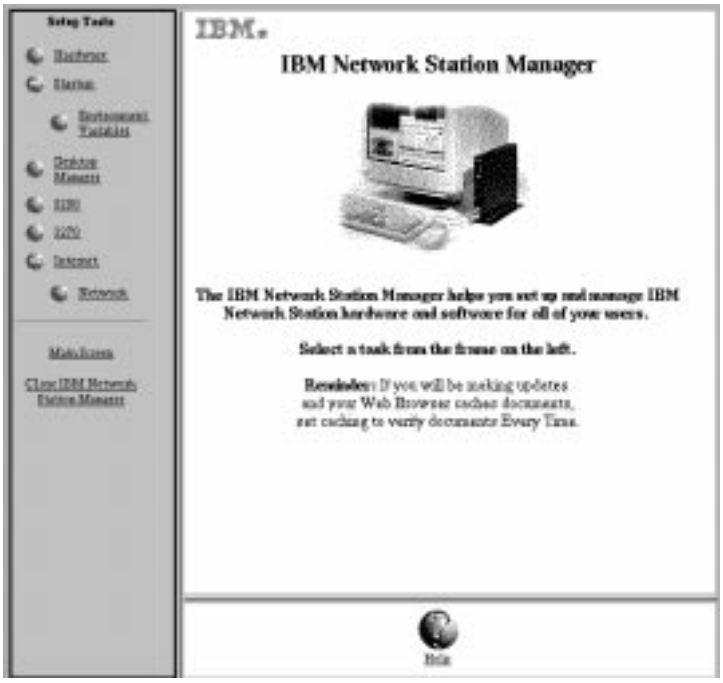



*Figure 10-3. End-user Level*

As you can see, the program's flexibility allows broad system-wide settings management by the administrator and individual settings management by the end user.

## Working with IBM Network Station Manager Program Defaults

There are three levels of defaults. They are:

IBM-supplied defaults

IBM-supplied defaults are provided for all settings that are supported by the IBM Network Station Manager program.

The IBM-supplied defaults can not be changed. They can be overridden using the IBM Network Station Manager program feature of System defaults or User level defaults.

See Appendix F, “IBM Network Station Manager Program Shipped Default Settings” on page F-1 for a complete list of all IBM-supplied default values for the IBM Network Station Manager program.

System defaults

System defaults are used to change settings for all users or all workstations.

System defaults take precedence over IBM-supplied defaults.

User defaults

User defaults are used to change settings for an individual user or individual workstation.

User defaults take precedence over IBM-supplied defaults and system defaults.

**Note:** Settings work differently in the Startup function of Setup Tasks. For Programs, Menus, and Environment Variables, the IBM-supplied, System-specified, and User-specified, are additive. However, for the same environment variable, the value set at the user level takes precedence over

the value set at the system or IBM-supplied levels. (That is, the values for a given environment variable are not additive.) Any settings that are specified at the system or user level are added to those that are specified in the IBM-supplied default settings.

## IBM Network Station Manager Program Defaults - Example

This example uses the Desktop background setting that is in the Hardware function of Setup Tasks.

The IBM-supplied setting for Desktop background is the IBM bitmap.

At this point, the administrator determines that all Desktop backgrounds will be set to dark red. Using the IBM Network Station Manager program, the administrator applies the change by working through the System Defaults level. This change, to the color dark red, overrides the IBM-supplied value of the IBM bitmap for Desktop background.

After viewing the new desktop background color of dark red, a user determines it is too difficult to look at for long periods of time and requests his Desktop background color be changed to green. The user can either change the Desktop background color or request the administrator to do it.

The administrator can make the change by selecting the Hardware Setup Task, User defaults and specify the user name of the person who is requesting the change. Scroll to the Desktop background field and specify green. Click Finish to apply the change. This change, to a User default setting, overrides the IBM-supplied default and the administrator-set System Default value of dark red.

**Notes:**

1. If the user changed the Desktop setting, they would go directly to the Hardware settings panel, bypassing the Default selection panel.
2. To view this change in Desktop settings you would have to log off and then log on to the workstation.

## Working with System-Wide Defaults

Figure 10-4 on page 10-7 is representative of the panel that appears when a selection is made from the Setup Tasks frame. In this example, the Hardware Defaults panel is used.

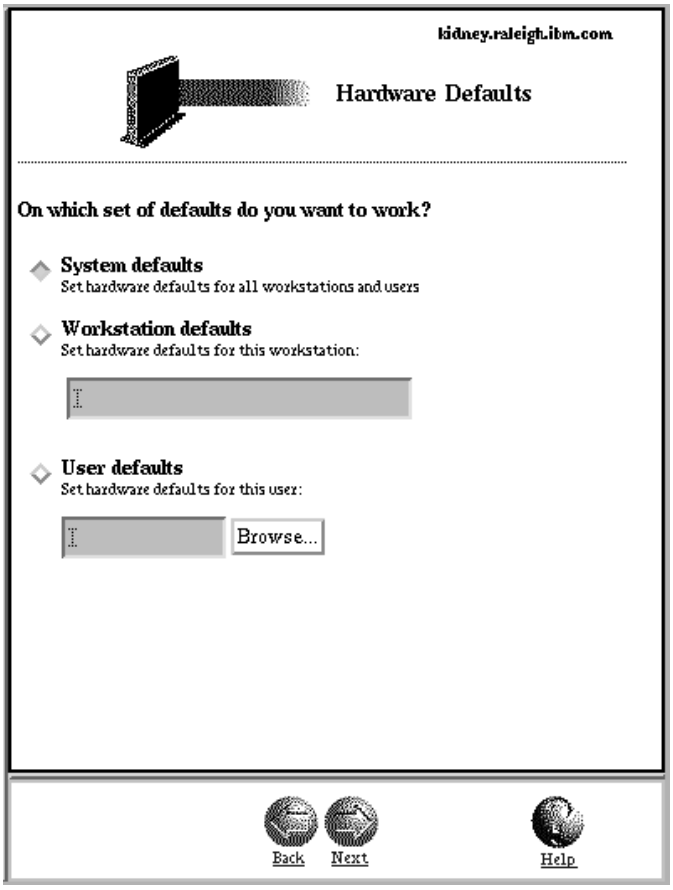



*Figure 10-4. Hardware Defaults*

As you can see, the Hardware Defaults panel allows you to work with System defaults for all workstations and users, Workstation defaults for a particular workstation, or User defaults for a particular user. The Hardware Defaults panel is unique in that it allows you to specify settings for workstations in addition to specific users. If you want to specify defaults for a particular user, you can click the Browse button and get a list of users on the system.

System defaults have settings that are not available when working with an individual user or workstation.

## Working with Individual User Defaults

User defaults are designed to change settings on a user-by-user basis, one user at a time. This gives you flexibility in custom tailoring individual sessions.

From any of the Default panels, select User defaults, enter the user name, and press the Next button.

## Working with Settings

Settings are fields that you see after you have selected which defaults (System or User) you want to work with. For example, Figure 10-5 on page 10-8 shows the Desktop Manager Settings fields for Screen colors, Icon preferences, Fonts, and Window focus.


*Figure 10-5. Desktop Manager Settings Fields*

In this example, Figure 10-5 represents Desktop settings that are being worked with from the System Defaults level. That means that any changes to the settings would be applied to **ALL** users.

**Note:** Settings in the Startup function of Setup Tasks work differently than the settings in other Setup Tasks. The difference is that any changes that are made at the system default level and user default level are added to the settings that are shipped with the IBM-supplied default settings.

For example, the IBM-supplied default is that all users have one 5250 session. Then, in Setup Tasks, the administrator selects Startup, Menus, System defaults, 5250 and applies this setting. The result is that all users would now have two 5250 sessions available to them.

## Starting the IBM Network Station Manager Program using a Browser

To best understand and learn how the IBM Network Station Manager program works, we recommend that you now sign on and follow the examples in this chapter.

To start working with the IBM Network Station Manager program, power-on your IBM Network Station, login, and click **IBM Browser** from the Menu bar on your IBM Network Station as shown in Figure 10-6.


*Figure 10-6. IBM Network Station Menu Bar*

**Note:** If you do not have, or have not installed, the IBM Network Station Browser licensed program, you can use the following web browsers to sign on to the IBM Network Station Manager program from your workstation:

Netscape** 3.01

Microsoft Internet Explorer** 3.01

The IBM Network Station Browser appears as shown in Figure 10-7:


*Figure 10-7. IBM Network Station Browser Sign on Screen*

Click the Edit pulldown and select IBM Network Station Manager Preferences as shown in Figure 10-8 on page 10-10:

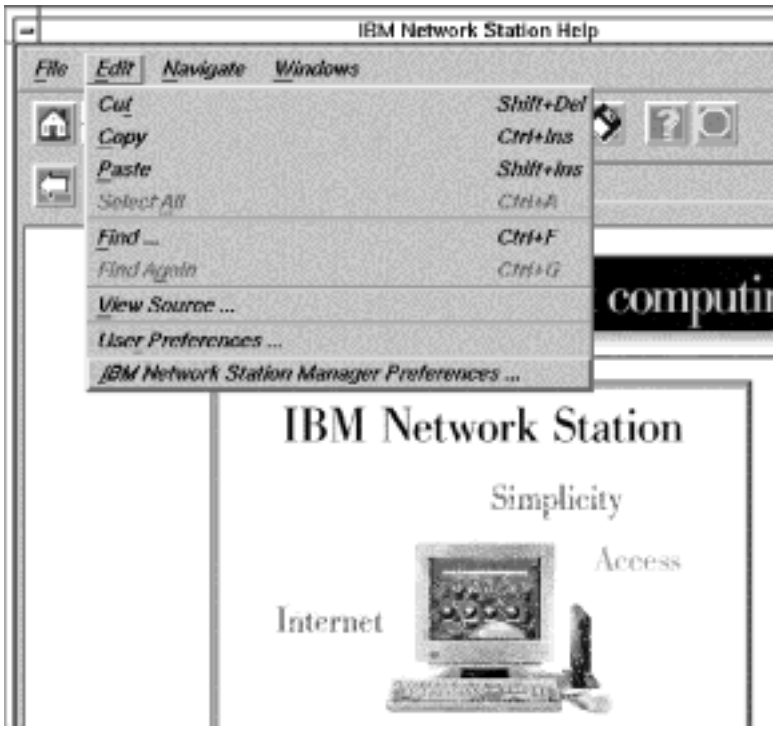



*Figure 10-8. IBM Network Station Browser Sign on Screen with Edit Pulldown*

The IBM Network Station Manager program sign-on screen appears:

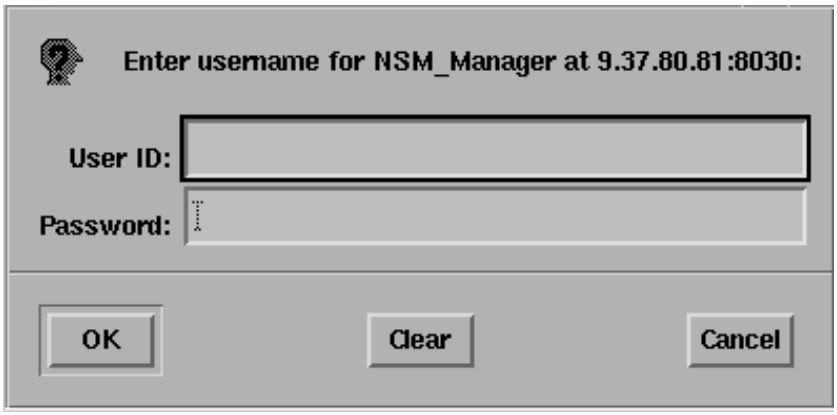



*Figure 10-9. Sign on Screen*

**Note:** An alternative way to reach the IBM Network Station Manager program sign-on screen is to enter the following case-sensitive URL in the IBM Browser's URL field:

***http://yourservername:portnumber/NetworkStation/Admin***

where:

***yourservername*** is the host name or TCP/IP address.

***portnumber*** is the port that is configured for use with the IBM Network Station program.

If you have not changed the default port number for the ICS server (80), you do not need to specify *portnumber*.

Type your username and password, then click **Ok**.

The Main Screen of the IBM Network Station Manager appears:


*Figure 10-10. System Administrator Level*

## Working with the IBM Network Station Manager Program Setup Tasks - Examples

**Note:** You must be a system administrator to work with these examples.

As shown in Figure 10-10, setup tasks are represented by icons in the left-most frame of the screen.

Clicking on any icon presents a panel where you select which set of Defaults you want to work with.

When working with these examples, select User defaults and use your own user name. Then, when you are done going through the examples, you will be able to see the results on your workstation.

In order to see the changes you make using the IBM Network Station Manager program, you will have to log off and then log on to your workstation. Do not do this until we have gone through all of the examples that are presented here.

**Notes:**

1. When going through the examples, the Main panel and the Default selection panel will not be presented in this document every time.
2. See “Additional IBM Network Station Manager Program Examples” on page 10-21 for information on working with remote programs such as AIX sessions and WinCenter Pro for PC applications.

## Hardware Settings - User Example

From the Setup Tasks frame, click Hardware.

Select User defaults, and type in your user name (USER001 in this example) as shown in Figure 10-11.

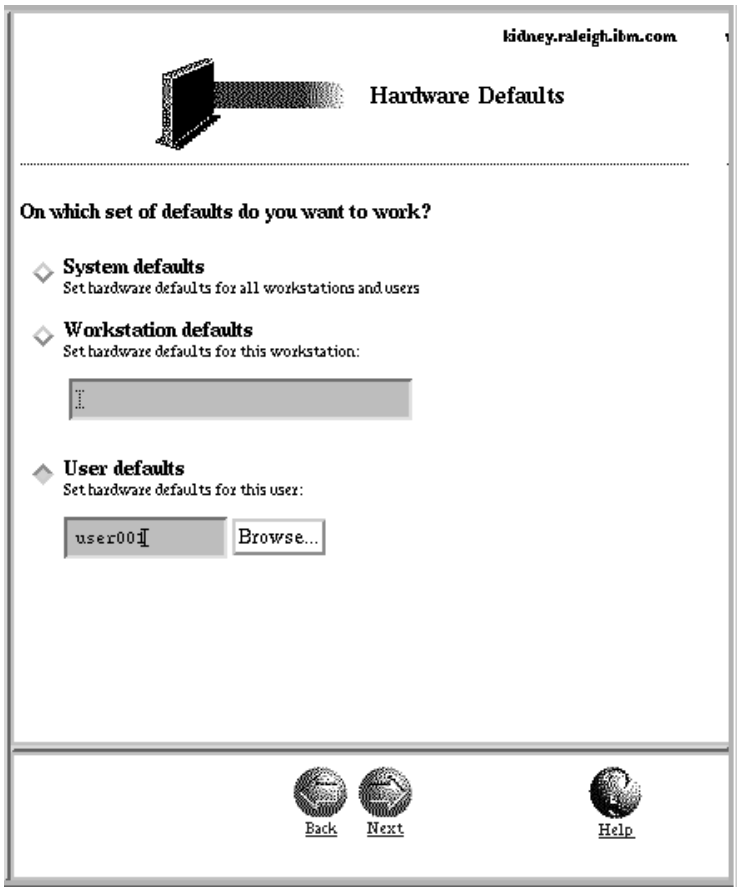



*Figure 10-11. Hardware Defaults Panel with User Defaults Specified*

In the bottom frame, click Next to continue.

The Hardware Settings frame appears as shown (scrolled-down) in Figure 10-12 on page 10-13.

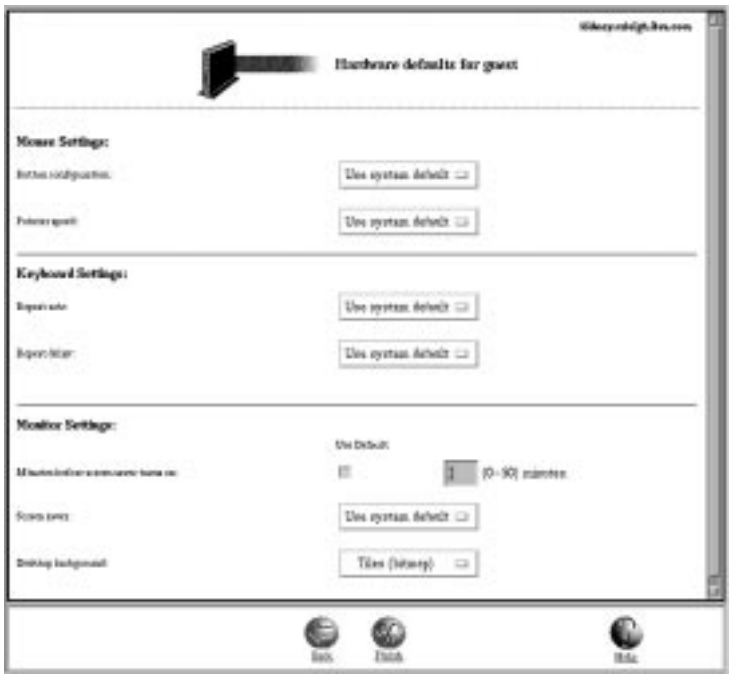



*Figure 10-12. Hardware Settings User Example*

Scroll to Desktop background and select the Tiles bitmap.

Click Finish to apply the change. Go to the next example.

## Hardware Settings - System Defaults Example

From the Setup Tasks frame, click Hardware.

Select System defaults. In the bottom frame, click Next to continue. The Hardware Settings - System Defaults panel is displayed.

Scroll forward to the box labeled Update host table and DNS configuration from server as shown in Figure 10-13 on page 10-14.

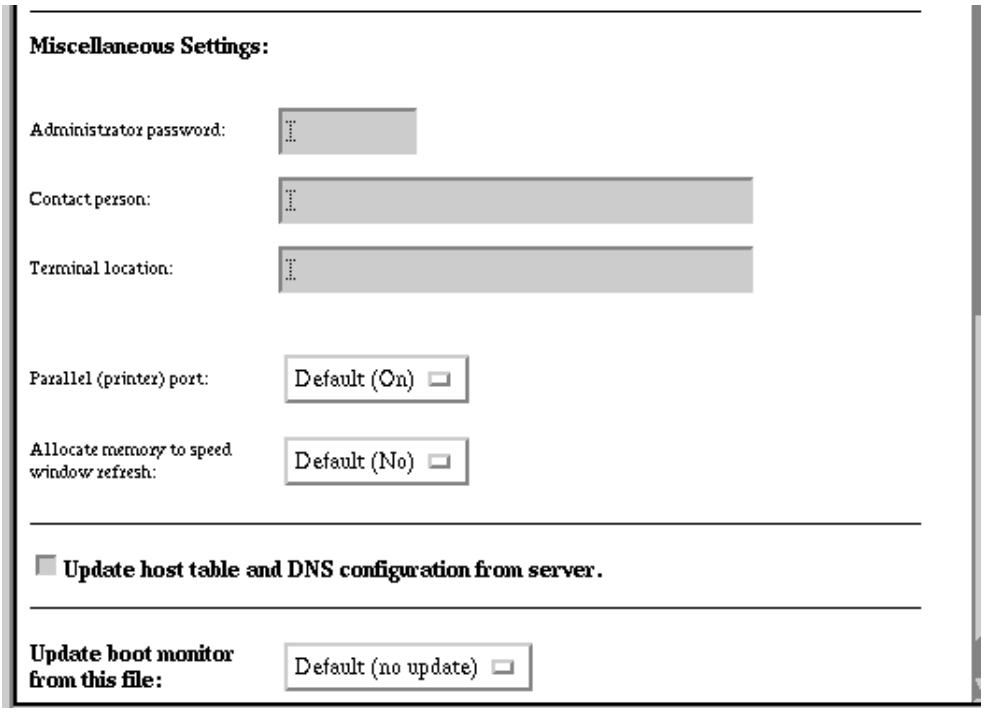



*Figure 10-13. Hardware Defaults Panel with System Defaults Specified*

The IBM Network Stations take their TCP/IP configuration information (domain name, name servers, and host table) from the DHCP or BOOTP server. The configuration file, /etc/resolv.conf, contains this information.

Click the IBM Network Station configuration button to change the configuration information. Any existing name server or domain name configuration data provided by DHCP or BOOTP server is overridden.

Click the Finish button.

## Startup Settings Example

From the Setup Tasks frame, click Startup, click Programs, and select User defaults. In the bottom frame, click Next to continue.

The Programs Settings frame appears as shown in Figure 10-14 on page 10-15.

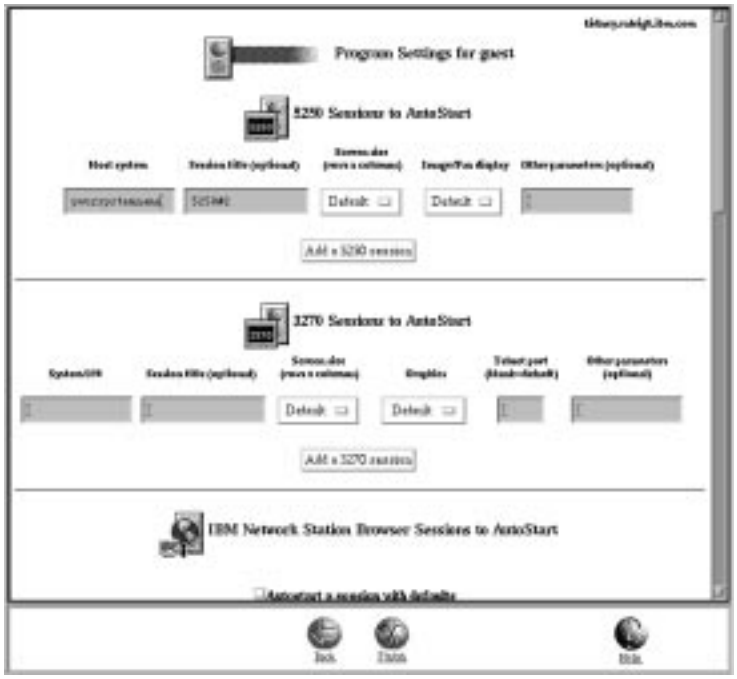



*Figure 10-14. Startup Settings Example*

Scroll to 3270 Sessions to Autostart. This setting, when completed, will automatically start a 3270 session for you when you sign on to your workstation. Complete the following fields:

S/390 system - Type the name or TCP/IP address of the S/390 your workstation boots from.

Session title - Type in a text string that represents your 3270 session. For example, 3270#2. This text string will appear in the Title bar of your 3270 session. This field is optional and you do not need a value. However, in this example you might want to try a name (3270#2) so you can see it when we verify the examples.

For the other settings fields, use the defaults.

Click Finish to apply the change. Go to the next example.

## Desktop Manager Example

From the Setup Tasks frame, click Desktop Manager and select User defaults. In the bottom frame, click Next to continue.

The Desktop Manager Settings frame appears as shown in Figure 10-15 on page 10-16.

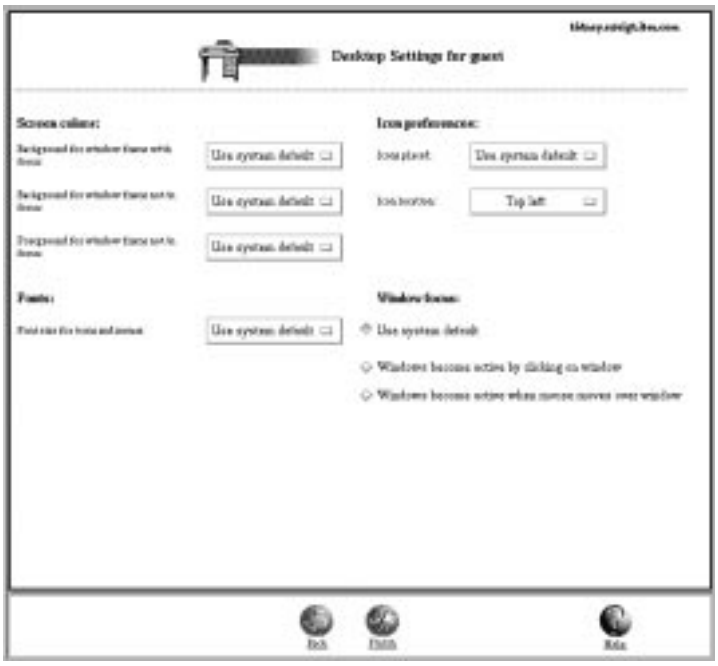



*Figure 10-15. Desktop Manager Settings Example*

Scroll to Icon preferences. In the Icon location field, select Top left.

Click Finish to apply the change. Go to the next example.

## 5250 Example

From the Setup Tasks frame, click 5250 and select User defaults. In the bottom frame, click Next to continue.

The 5250 Settings appear as shown in Figure 10-16 on page 10-17.

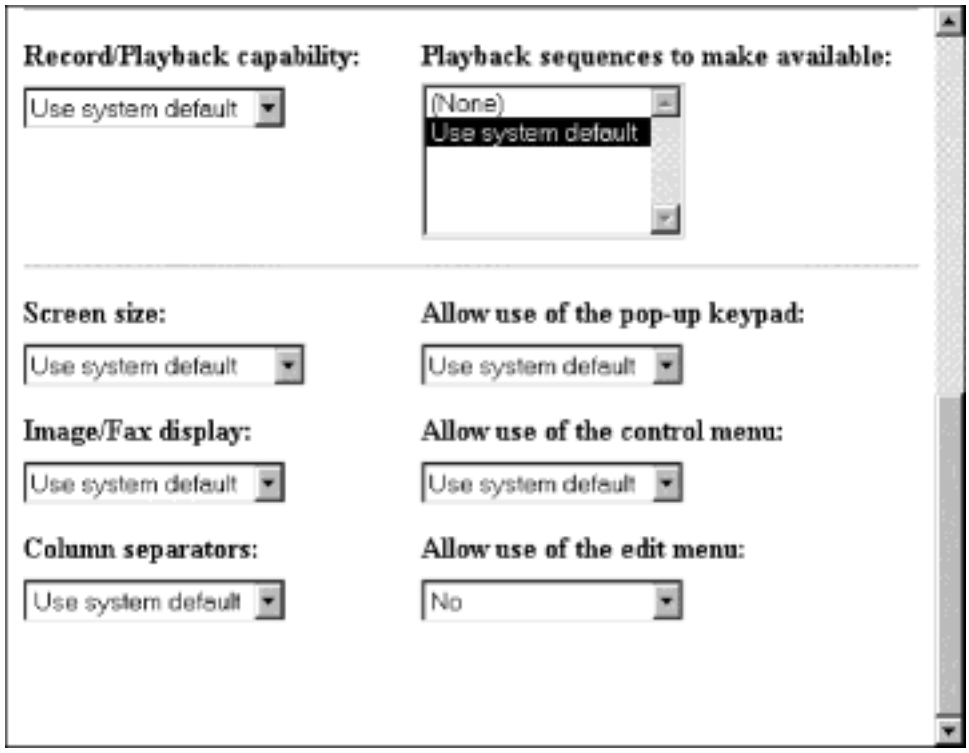



*Figure 10-16. 5250 Setting Example*

Scroll to the Allow use of the edit menu field and select No to disable the edit menu. (The default is Yes, meaning that you can use the edit menu).

By disabling Allow use of the edit menu, your 5250 sessions will not have the Edit pulldown displayed for use.

Click Finish to apply the change. Go to the next example.

## 3270 Example

From the Setup Tasks frame, click 3270 and select User defaults. In the bottom frame, click Next to continue.

The 3270 Settings panel appears as shown in Figure 10-17 on page 10-18.

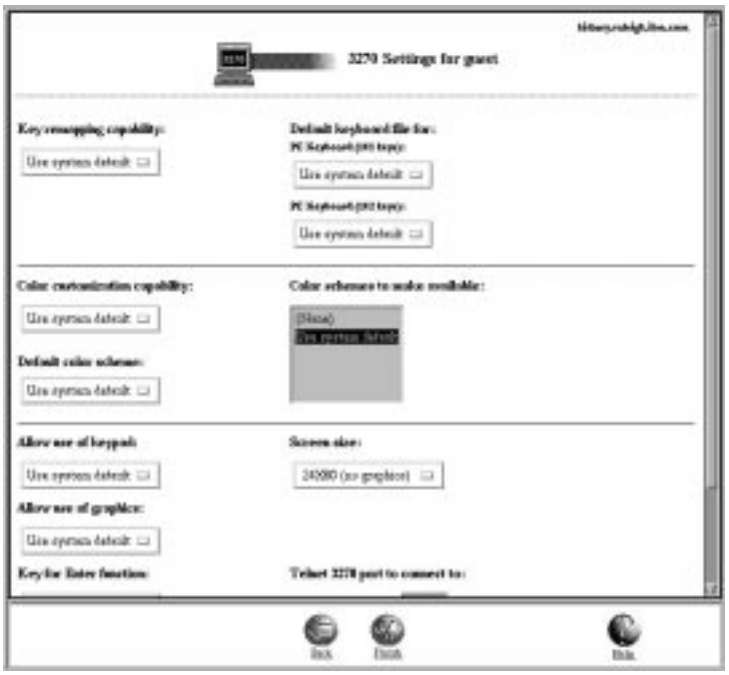



*Figure 10-17. 3270 Settings Example*

Scroll to the Screen size field. Select 24 x 80.

This will change your 3270 session screen size from 32 x 80 (the default) to 24 x 80.

Click Finish to apply the change. Go to the next example.

# Internet

## Changing the IBM Network Station Default Port Number

The default IBM Internet Connection Secure (ICS) server number is port 80. This port number is also the default port number used by the IBM Network Station browsers to access the IBM Network Station Manager program. If the ICS server configured for use with IBM Network Station Manager program does not use the default port 80, do the following steps to configure the IBM Network Station browsers to select the appropriate port.

1. Invoke the IBM Network Station Manager program

```
http://yourservername:portnumber/NetworkStation/Admin
```

where:

*yourservername* is the host name or TCP/IP address of the ICS server

*portnumber* is the port that is configured for use with the IBM Network Station Manager program

If you have not changed the default port number for the ICS server (80), you do not need to specify *portnumber*.

Enter the URL and log as a system administrator.

2. Access the Internet Network System default panel. The Internet Network System panel appears as shown in Figure 10-18.

   From the 'Setup Tasks' frame on the left, click Internet, click Network, and select System defaults. In the bottom frame, click Next to continue.

3. Update the port number.

   Scroll to the 'Proxy Section'. At the end of this section, see the following:

   Web server port on the boot host:

   To the right is a box that indicates 'Use default' or key in the new port number.

   Enter the new port number (for example 8080).

   Select Finish.

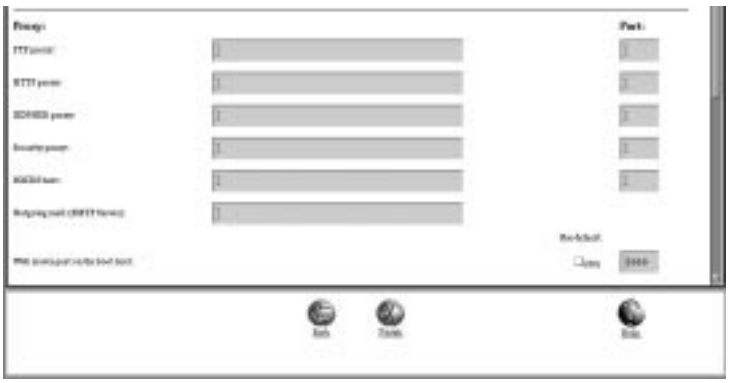


*Figure 10-18. IBM Network Station Manager program Internet Network System Defaults*

Reboot the IBM Network Station. Do the following to verify the change.

1. Select Edit
2. Select Network Station Manager Program Preferences.

The updated port number appears in the URL.

## Changing Other Internet Settings

From the Setup Tasks frame on the left , click Internet, click Network, and select System defaults. In the bottom frame, click Next to continue.

The IBM Network Station Browser Settings frame appears as shown in Figure 10-19 on page 10-20.

*Figure 10-19. IBM Network Station Browser Settings Example*

Scroll to the Proxy Section heading and select No in the Auto load images field.

**Note:** Remember that if you apply this change, no images will display when you are using a browser. After a page loads the text, you can use the browser's Navigate pulldown menu to load the images. Select the Navigate pulldown, and then select Load Missing Images.

Click Finish to apply the change. Click Main Screen in the Setup Tasks frame.

### Verifying your Setting Changes

After completing the examples, you can verify the settings you specified.You will need to log off and then log on for the settings to be applied.

**Do not forget:** If you do not want any of the settings specified in the example exercises to remain, you will have to use the IBM Network Station Manager program to return them to the original settings or some other settings of your choice.

## IBM Network Station Manager Program Education

It is recommended that you provide some hands-on education, similar to what you just experienced going through the above examples, for your users of the IBM Network Stations.

Practice choosing and applying settings within the various Setup Tasks to build skills among your users.

## Additional IBM Network Station Manager Program Examples

Following is a list of additional examples that use the IBM Network Station Manager program:

Setting up an AIX session on your IBM Network Station by using Remote Program support

Setting up a Windows NT session on your IBM Network Station by using Remote Program support

## Setting up an AIX Session using the IBM Network Station Manager Program

Complete the following steps to setup an AIX session by using the IBM Network Station Manager program:

1. Verify that the user name and password on the host system match the user name and password on the AIX server.
2. You must create a .rhosts file on the AIX server. This file must contain the IBM Network Station's name and the name that the user logs into AIX with. This file resides on the AIX server under the user's directory. An example for a userid of user001:

   ```
                Contents of File

   Directory Structure:          /home/user001
   File name:                   .rhosts
   IBM Network Station name       MYNWS.mycompany.ABC.com
   Name user signs on with:       user001
   ```

   This file can contain multiple lines. Each line should have one IBM Network Station name and one user name on it. If a user will be working from more than one IBM Network Station, create an entry for each IBM Network Station.
3. Sign on to the IBM Network Station Manager program.
4. From Setup Tasks, click Startup.
5. Under Startup, click Menu.
6. From Program Defaults, click User defaults.

   If you are setting this up for someone else, type their user name or click Browse to select their user name if you do not know it.
7. Click Next to continue.
8. Scroll ahead to Remote Programs. Type in the information as shown in Figure 10-20.

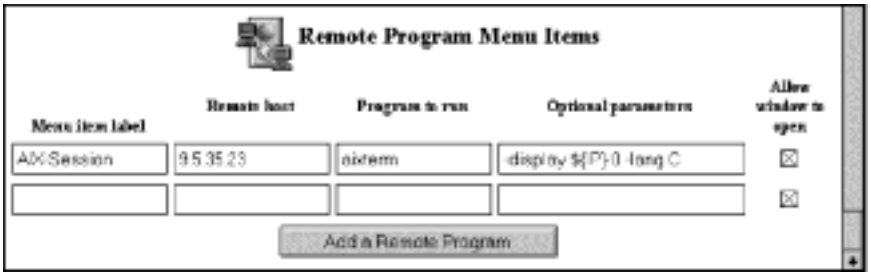



*Figure 10-20. Remote Program Example for AIX*

Where:

**Menu item label**
This text string will appear in the Menu bar on the IBM Network Station.

**Remote host**
The name or IP address of the AIX server.

**Program to run**
This identifies the program to run on the AIX server.

**Optional parameters**
-display is an AIX requirement that causes the program to display on the IBM Network Station rather than on the remote host. ${IP} is an IBM-supplied environment variable that gets replaced with the IP address of the IBM Network Station. -lang C is an AIX requirement that is used by programs such as Netscape on AIX.

The required parameters for AIX-Session are: -display and ${IP}:0.

9. Click Finish to apply the AIX remote program setting.
10. Log off and then log on your IBM Network Station. In the Menu bar there will be a button that is labeled AIX-Session, as shown in Figure 10-21.


*Figure 10-21. Menu Button for Remote Program Example for AIX*

11. Click AIX-Session and a window will open with your X-station session.

    From the Aixterm window, you can run additional programs.

## Setting up a Windows NT Session using the IBM Network Station Manager Program

Complete the following steps to setup a Windows NT session by using the IBM Network Station Manager program:

1. Verify that you have a Windows NT machine in your network that has the WinCenter Pro** application loaded on it.
2. Verify that the user has a valid user name and password on the Windows NT server. When the session from the Windows NT server is requested on the IBM Network Station, the user will have to sign on.
3. Sign on to the IBM Network Station Manager program.
4. From Setup Tasks, click Startup.
5. Under Startup, click Menu.
6. From Program Defaults, click User defaults.

   If you are setting this up for someone else, type their user name or click Browse to select their user name if you do not know it.
7. Click Next to continue.
8. Scroll ahead to Remote Programs. Type in the information as shown in Figure 10-22 on page 10-23.


*Figure 10-22. Remote Program Example for Windows NT*

Where:

**Menu item label**
This text string will appear in the Menu bar on the IBM Network Station.

**Remote host**
The name or IP address of the Windows NT server.

**Program to run**
This identifies the program to run on the Windows NT server.

**Optional parameters**
-display is a WinCenter Pro requirement that causes the program to display on the IBM Network Station rather than on the remote host. ${IP} is an IBM-supplied environment variable that gets replaced with the IP address of the IBM Network Station.

The required parameters for WinCenter Pro are: -display and ${IP}:0.

9. Click Finish to apply the WinCenter Pro remote program setting.
10. Log off and then log on your IBM Network Station. In the Menu bar there will be a button that is labeled WinCenter Pro, as shown in Figure 10-23.


*Figure 10-23. Menu Button for Remote Program Example for NT - EDBAR*

11. Click WinCenter Pro and a window will open with your WinCenter session.

## Viewing Network Station Manager Error Messages

Only system administrators can view network station manager error message descriptions online. From the Setup Task frame, click NSM Error Messages. This will open the window as shown in Figure 10-24 on page 10-24.

Enter the error message number you want to view and click on Submit. You can enter an error number with or without message prefix.

The corresponding error message will be displayed as shown in Figure 10-25 on page 10-24. Variable tokens, which are substituted in the messages, are high-lighted within brackets ([]).

Use the back button to go to the previous screen if you want to see another error message. The Close button will close this new window.


*Figure 10-24. Network Station Manager's Error Messages*


*Figure 10-25. Network Station Manager's Error Message Displayed*

# Chapter 11. Working with User Services

User services are programs that provide users with tools to manage the IBM Network Station's environment. You can work with User Services whenever you want, including when an application is running. Following are a list of User Services (not all User Services are enabled):

Console

Login (not enabled)

Terminals

WindowMgr

Utilities

Setup (not enabled)

Statistics

## Accessing User Services

Access User Services by pressing the Ctrl and Pause keys all at the same time.

Figure 11-1 shows the User Services window with all the service programs that are displayed within the menu bar:

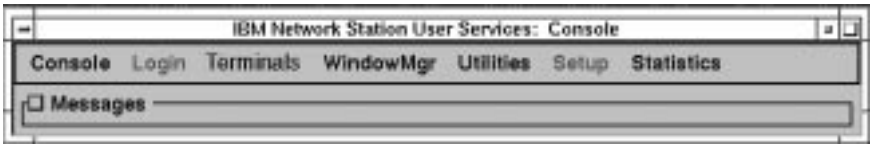



*Figure 11-1. User Services Window*

## Console

This function provides a menu bar option (Console) for handling messages. Click the button by Messages to display messages that record IBM Network Station activity. Figure 11-2 shows the tools available through the Console services option:


*Figure 11-2. User Services: Console View*

Click Console to change the information displayed on the console.

The list below contains the name of the tool and a description of its function:

**Clear Messages**
Selecting this option clears all the current messages from the console display.

**Rescan Messages**
Selecting this option refreshes the console display with any current messages that are not presently being displayed.

**Close**
Selecting this option closes the console function of User Services.

## Login

The Login services option is disabled. The IBM Network Station Manager licensed program provides a login capability.

## Terminals

Figure 11-3 shows the tools available through the Terminals services option:

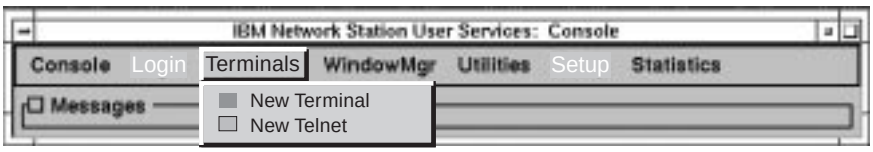



*Figure 11-3. User Services: Terminals View*

The list below contains the name of the tool and a description of its function:

**New Terminal**
Selecting this option starts terminal management.

The New Terminal function provides you with the ability to select from a list of hosts, which allows terminals on the hosts to communicate with each other.

**New Telnet**
Selecting this option starts the Telnet manager.

The New Telnet function provides similar capability as the New Terminal function.

## WindowMgr

Figure 11-4 on page 11-3 shows the tools available through the WindowMgr services option:


*Figure 11-4. User Services: Window Manager View*

The list below contains the name of the tool and a description of its function:

**Builtin Window Manager**
Selecting this option starts the Builtin Window Manager (an OSF or Motif-style). Deselecting this option ends the Builtin Window Manager.

The Builtin Window Manager function provides you with the ability to size, move, and make active (clicking) all the windows open on your monitor.

## Utilities

Figure 11-5 shows the tools available through the Utilities services option:

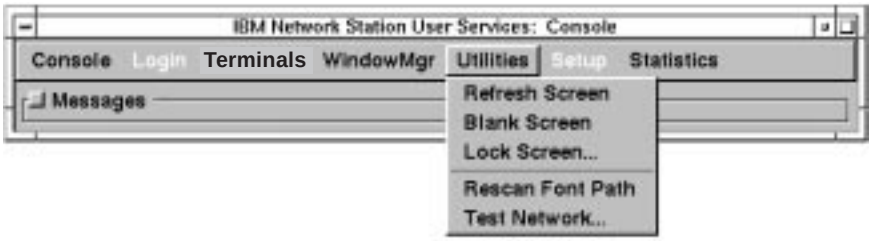



*Figure 11-5. User Services: Utilities View*

The list below contains the name of the tool and a description of its function:

**Refresh Screen**
Selecting this option refreshes the active window.

**Blank Screen**
Selecting this option starts the screen-saver program.

**Lock Screen**
Selecting this option locks the screen after prompting for a password. The Lock Screen function keeps anyone without the password from using the workstation.

**Rescan Font Path**
Selecting this option refreshes any font changes that are provided by the system administrator.

For example, if the font currently being used is so large you can't display an entire 5250 session, you might have the administrator make available a smaller font. When this is done, you can then select the font by clicking on the Option pull-down within the tool bar and selecting fonts.

Another use of fonts would be to make your windows smaller, therefore enabling several full windows to be displayed at the same time.

**Test Network**

Selecting this option runs the network test. This would be similar to the TCP/IP command "PING".

## Setup

The Setup services option is disabled.

## Statistics

Figure 11-6 shows the tools available through the Statistics services option:

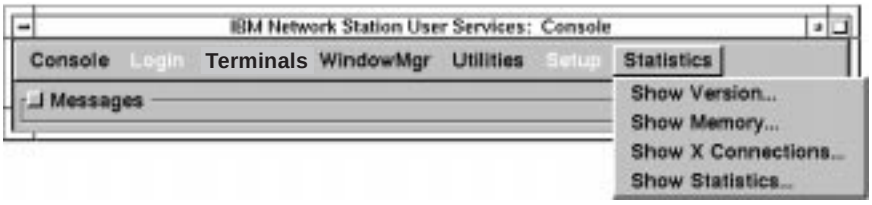



*Figure 11-6. User Services: Statistics View*

The list below contains the name of the tool and a description of its function within the statistics services function:

**Show version**

Selecting this option displays version numbers and other information about the current state of the IBM Network Station.

**Show Memory**

Selecting this option displays information about free and installed memory in the IBM Network Station.

**Show X Connections**

Selecting this option displays information about all the current X clients that are connected to the IBM Network Station.

**Show Statistics**

Selecting this option displays statistics that pertain to the IBM Network Station.

# Chapter 12. Working with the IBM Network Station Setup Utility

The system administrator can access the IBM Network Station Setup Utility while the IBM Network Station is going through the boot-up process.

The primary purpose of the Setup Utility is to allow you to **View** and then **Set** (change) configuration settings on a particular IBM Network Station. Following is a list that contains the names of configuration settings that can be viewed or set (changed):

View:

- Network Parameters
- Boot Parameters
- Hardware Configuration

Set (change):

- Network Parameters
- Boot Parameters
- Monitor Parameters
- Language Parameters
- Verbose Diagnostic Messages (Enabled or Disabled)

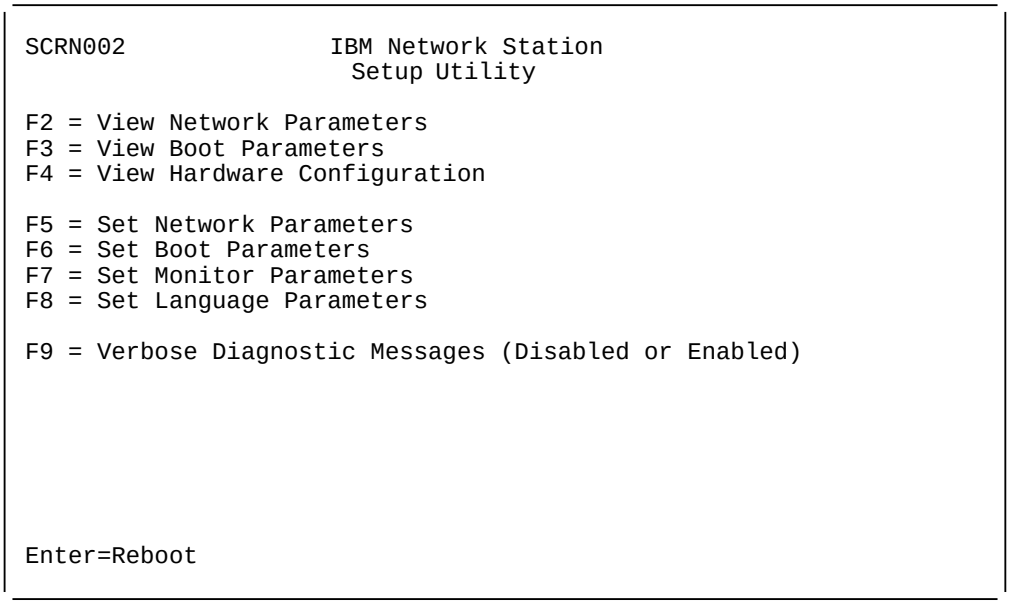
## Accessing the IBM Network Station Setup Utility

While the IBM Network Station is booting (downloading the file from the boot Host), press the Escape key.

Then, type in the Administrator password if password control is active. (The password is case-sensitive). The administrator password is specified through the IBM Network Station Manager program in the Hardware setup tasks. Once the password is accepted, the following display appears:

**Notes:**

1. If the password has not been set using the IBM Network Station Manager program, any user can use the configuration settings in the IBM Setup Utility.
2. If you attempt the password three times without success, only the viewing capability of the IBM Network Station Setup Utility is available to you.
3. If you changed the Administrator password using the IBM Network Station Manager program, you will have to boot the IBM Network Station system unit up to the Login window in order for the new Administrator password to be enabled at the system unit.




## F2 = View Network Parameters

This option lets you view the following Network Parameters for an IBM Network Station.

IP Addressed from

Whether the IBM Network Station is booted from the Network setting (DHCP for OS/390 and BOOTP for VM is normal operation for the IBM Network Station), or if the IBM Network Station is booted from specific parameters stored on the IBM Network Station (NVRAM setting)
Network Station IP Address
First Boot Host IP Address
Second Boot Host IP Address
Third Boot Host IP Address
Gateway IP Address
Subnet Mask
Broadcast IP Address

## F3 = View Boot Parameters

This option lets you view the following Boot Parameters for an IBM Network Station:

Boot File
TFTP Boot Directory
NFS Boot Directory
Configuration File
Configuration Directory
TFTP Order
NFS Order
MOP Order
LOCAL Order

## F4 = View Hardware Configuration

This option lets you view the following Hardware Configuration parameters for an IBM Network Station:

Video Memory
DRAM Memory Total

- Slot 1
- Slot 2

Boot Monitor Version

Specifies the level of initial program that runs when the IBM Network Station is powered on.
Keyboard Controller
Keyboard ID
Keyboard Language
Startup Language
Processor Version
Boot Resolution

This indicates the monitor resolution when the IBM Network Station is powered on.
Server Resolution

This indicates the monitor resolution when applications are loaded on the IBM Network Station.
Monitor ID
Token Ring/Ethernet

- MAC Address

  This indicates the address of the communication adapter.
- Manufacturer
- Product
- Microcode Version
- Information

PCMCIA Card

- Manufacturer
- Product
- Microcode Version
- Information

## F5 = Set Network Parameters

This option lets you **Set or Change** how this IBM Network Station will determine its network parameters as specified by IP Addressed from:

Network - IBM Network Station boots from the network
NVRAM - IBM Network Station boots from the parameters stored in this IBM Network Station.

If the IBM Network Station is booting from the Network setting, the following Network Parameters are available:

| Using a Token Ring Connection | Using an Ethernet Connection |
|---|---|
| IP Addressed from | IP Addressed from |
| DHCP IP Address order | DHCP IP Address order |
| BOOTP IP Address order | BOOTP IP Address order |
| RARP IP Address order | RARP IP Address order |
| | Version 2 IEEE 802.3 |

If the IBM Network Station is booting from the NVRAM setting, the following Network Parameters are available:

Network Station IP Address
First Boot Host IP Address
Second Boot Host IP Address
Third Boot Host IP Address
Gateway IP Address
Subnet Mask
Broadcast IP Address

The main use of the Set Network Parameters function is to allow you to select specific TCP/IP parameters for connection to boot hosts to isolate network connection problems.

## F6 = Set Boot Parameters

The main use of this function is to monitor or change the files and location of files that are used for booting this IBM Network Station.

This parameter lets you **Set or Change** the following Boot Parameters for an IBM Network Station:

Boot File

TFTP Boot Directory (path on the boot server to the Boot File)

When using TFTP (see below on this screen), this is the path name the server uses to locate and download the operating system.

NFS Boot Directory

When using NFS (see below on this screen), this is the path name the server uses to locate and download the operating system.

Configuration File

This is the name of the configuration file. The configuration file contains the settings that are used by this IBM Network Station. You can configure these settings by using the Hardware function of Setup Tasks through the IBM Network Station Manager. See Chapter 10, “Using the IBM Network Station Manager Program” on page 10-1, for a high-level description of the Hardware Setup Tasks. The online help of the IBM Network Station Manager provides the details about using the Hardware function of Setup Tasks.

Configuration Directory

This is the name the boot server uses to locate the configuration file.

Protocol Order

You can use the following protocols (that are located near the bottom of the screen) to perform the software download to the IBM Network Station. You can assign an order (first, second, and so on) that the system follows when performing the software download.

- TFTP Order

  Trivial File Transfer Protocol (TFTP).

- NFS Order

  Network File System (NFS).

- MOP Order

  This protocol order is not supported.

- LOCAL Order

  This indicates that you have installed, in the IBM Network Station system unit, a flash card with the operating system on it.

## F7 = Set Monitor Parameters

**F2 = Set Monitor Resolution** The main use of this function is to select a resolution to use with the monitor that is attached to this IBM Network Station.

We recommended that you test the resolution (pressing Enter allows you to test the resolution) before selecting and exiting this screen to ensure the resolution is supported by this monitor. If the grid size fits your display screen, and the font resolution is acceptable, the resolution that is selected will work.

**CAUTION:**
**Setting a resolution that is not supported by your monitor can cause permanent damage to the monitor.**

**F3 = Monitor Power Management Disabled** The main use of this function is to enable or disable the power management function of the monitor that is attached to this IBM Network Station system unit.

**CAUTION:**
**Enabling power management for a monitor that does not support this feature can cause permanent damage to the monitor.**

## F8 = Set Language Parameters

**F2 = Select Keyboard Language** The main use of this function is to select a keyboard language to use with this IBM Network Station. Selecting a different language will change the mapping of keys. For example, if the current mapping results in a $ sign being put on the display when the $ sign key is pressed, changing the keyboard language may result in a different character being put on the display.

**Note:** If you change your keyboard language by using the IBM Network Station Setup Utility, you could have a different keyboard language than what is specified in the IBM Network Station Manager program. We recommended that you use the IBM Network Station Manager program to change keyboard languages.

**F3 = Select Startup Language** The main use of this function is to select your language type.

**Note:** For release 1, English is the only supported language type.

## F9 = Verbose Diagnostic Messages (Enabled or Disabled)

The main use of this function is to monitor boot activity from the boot Host. As the files are loaded, messages are written to a message log or displayed on the monitor. The default is Verbose disabled. When the boot process is in progress, a series of periods appears on the monitor.

If Verbose is enabled, all the file loading activity and any error messages are displayed.

# Appendix A. Modifying the DHCP Server Configuration File

You configure the DHCP server by manually editing the DHCP server configuration file.

**Attention:** Configuring the server incorrectly causes few, if any, warning messages. The DHCP server normally runs even when it encounters errors in the configuration file and typically ignores incorrect data and may optionally post a message to its log.

The DHCP server defaults to locating the configuration file in \ETC\DHCPSD.CFG. A sample server configuration file called DHCPSD.CFG is located in the \usr\lpp\tcpip\nsm\samples\dhcpsd directory.

You can create a hierarchy of configuration parameters by nesting statements within the DHCP server configuration file. This allows you to specify the scope of some configuration values that are served to all clients, while other configuration values are served only to certain clients. The statement used and its position in the file determines what information is supplied to the clients.

When editing the DHCP server configuration file:

Comments must begin with a pound sign (#).

Class and vendor names that include spaces must be surrounded by quotes (").

Parameters to the right of a left parenthesis are used only by the DHCP Server Configuration program graphical interface. A space must precede the left parenthesis. For example, `(alias=mysubnet` is used only by the DHCP Server Configuration program in the following:

```
subnet 9.67.48.0 255.255.240.0 9.67.48.1-9.67.48.15 (alias=mysubnet
```

Statement parameters are positionally dependent. If you omit a required parameter and enter a subsequent required parameter in a statement, the server ignores the missing parameter, writes an error message to a log file, and continues to read the configuration file.

A continuation character \ indicates the information is continued on the next line. When used within a comment, the character is treated as part of the comment and is ignored as a continuation character.

Braces are used to specify statements that are scoped within other statements.

If a parameter is specified in more than one place, the lowest level statement (which is the most specific) is used:

- Statements specified outside braces are considered global and are used for all addresses served by this server unless the statement is overridden at a lower-scoped level.
- Parameters specified within braces under a statement such as a Subnet statement, are considered local and apply only to clients within the subnet.
- Definition of a parameter in a class takes precedence over definition of the parameter in a subnet.

Vendor statements always have a global scope.

Class statements are not allowed inside Client statements.

Client statements are not allowed inside Option, Vendor, or Class statements.

Subnet statements are not allowed inside Class or Client statements.

Keywords are not case sensitive. Capitalization patterns used in this documentation are not required in the configuration file. This program uses the convention that keywords start with a lower case letter and subsequent "word" subparts start with a capital letter. For example, a keyword is proxyARec.

## Defining Global Values

Assign global values such as Class, Subnet, Option, Client, or Vendor statements by placing the statement outside any braces.

## Defining Vendors

To provide vendor configuration information to the DHCP clients in your network:

At the global level, define a vendor and assign the appropriate configuration values. Unlike the Class statement, the scope of the Vendor statement cannot be controlled by its placement in the file. Vendor statements within Subnet, Class, or Client statements are ignored. Options can be redefined in the vendor class.

Using the DHCP-BOOTP protocol, the DHCP client identifies itself to the DHCP server as belonging to a vendor class by sending option 60, Class Identifier, with a specific vendor name.

The DHCP server recognizes the client has a specific vendor and returns encapsulated option 43, Vendor-specific Information, containing vendor-specific DHCP options and option values.

The format of the Vendor statement is:

**vendor** *vendor_name* [**hex** *value*]

*vendor_name*
The user-defined label that identifies the vendor. The vendor name is an ASCII string of up to 255 characters (for example, "IBM"). If the vendor name contains spaces, it must be surrounded by quotes (").

**[hex** *value***]**
The value for each option must be specified either as an ASCII string, or as hexadecimal in the hexadecimal ASCII string construct. For example:

```
hex"01 02 03"
```

For more information, see descriptions of option 60, Class-Identifier, in Specifying DHCP Options.

The vendor statement can also be specified in the DHCP server configuration file as a vendor statement followed by a pair of braces containing the options particular to this vendor. Within these braces, the usual option value encoding and decoding rules do not apply:

```
vendor vendor_name
{
option x hex "01 02"
option y hex "05 07"
}
```

## Defining Subnets

The Subnet statement specifies configuration parameters for an address pool administrated by a server. An address pool is a range of IP addresses to be leased to clients. The task of configuring subnets also allows you to set lease time and other options for clients using the address pool. Lease time and other options can be inherited from a global level.

The Subnet statement can be used to define a subnet or a subnet group. The format of the Subnet statement used to define a subnet is:

**subnet** *subnet_address* [*subnet_mask*] *range* [(**alias=***name* ]

**Note:** Parameters to the right of a left parenthesis are used by the DHCP Server Configuration program. The DHCP server parses statements to the right of a left parenthesis as comments.

*subnet_address*
The address of this subnet, specified in dotted-decimal notation (for example, 9.67.48.0).

*subnet_mask*
The mask for the subnet in dotted decimal notation or in integer format. A subnet mask divides the subnet address into a subnet portion and a host portion. If no value is entered for the subnet mask, the default is the class mask appropriate for an A, B, or C class network.

A subnet mask can be expressed either in dotted-decimal notation, or as an integer between 8 and 31. For example, enter a subnet mask as a dotted decimal notation of 255.255.240.0 or an integer format of 20. In subnet 9.67.48.0, a mask of 255.255.240.0 implies an address range from 9.67.48.001 to 9.67.63.254. The value 20 is the total number of 1s in a mask expressed in binary as 11111111.11111111.11110000.00000000.

Although not required, in most configurations the DHCP server should sned option 1, subnet mask, to DHCP clients. Client operation may be unpredicatable if the client receives no subnet maske from the DHCO server and assumes a subnet mask that is not appropraite for the subnet.

If not specified, the client uses the following default subnet masks:

Class A network - 255.0.0.0

Class B network - 255.255.0.0

Class C network - 255.255.255.0

*range*
All addresses to be administered to this subnet. Enter the addresses in dotted-decimal notation, beginning with the lower end of the range, followed by a hyphen, then the upper end of the range, with no spaces in between; for example, 9.67.48.1-9.67.48.128. Ranges should not overlap.

**Notes:**

1. In the range of addresses, do not include the address of the subnet and the address used for broadcast messages. For example, if the subnet address is 9.67.96.0 and the subnet mask is 255.255.240.0, do not include 9.67.96.0 and 9.67.111.255 in the range of addresses.
2. Use the Client statement to exclude an IP address in the range that the server should not administer. For example, exclude an address that has been permanently assigned to a host. For more information on client statements, see Defining Clients.

**(alias=***name*

A symbolic name for ease in identifying a subnet.

The parameter **alias=***name* immediately after a left parenthesis contains the symbolic name, which appears in the DHCP Server Configuration program graphic display of the server configuration. If no name is entered, the subnet IP address is used to identify the subnet in the DHCP Server Configuration program display.

## Defining Subnet Groups

To define a subnet group, use **label:***value[/priority]* in the Subnet statement:

**subnet** *subnet_address* [*subnet_mask*] *range* [**label:***value[/priority]*]

The *subnet_address*, *subnet_mask*, and *range* parameters are described in Defining Subnets. The parameters that define subnet groups include:

**label:**

Identifies subnets grouped together on the same wire.

*value[/priority]*

A string of 1 to 64 alphanumeric characters that identifies the subnet, followed by the priority in which this subnet's address pool is used. No spaces are allowed in labels. More than one subnet can have the same identifier. Priority is a positive integer, where 1 is a higher priority than 2. If no priority is specified, the highest priority is assigned. If two subnets have identical priority, the subnets within a label are processed based on the physical position in the configuration file.

For example, the following two subnets are on the same wire:

```
inOrder
subnet 9.67.49.0 255.255.240.0 9.67.49.1-9.67.49.100 label:WIRE1/2
subnet 9.67.48.0 255.255.240.0 9.67.48.1-9.67.48.50 label:WIRE1/1
```

### Using Subnet Group Processing Statements

To specify the policy by which IP addresses are served from multiple subnets, an inOrder or balance statement is required. Enter the following additional statements at a global level:

**inOrder:** *labelslist*

The *labelslist* is a list of labels in which each label identifies a subnet group. Each listed group is processed in order within that group. The subnet address pool with the highest priority within that group is completely exhausted before the subnet address pool with the next highest priority is used.

**balance:** *labelslist*

The *labelslist* is a list of labels in which each label identifies a subnet group. The server provides the first IP address from the subnet that is first in the priority list, and subsequent IP addresses from each lesser-priority subnet, repeating the cycle until addresses are exhausted equally from all subnets.

The following is an example of inOrder processing of two subnet groups. Requests for subnet group WIRE1 exhaust addresses in subnet 9.67.48.0 (WIRE1/1) first, followed by subnet 9.67.49.0 (WIRE1/2). WIRE1 and WIRE3 are not related. Requests for subnet group WIRE3 exhaust addresses in subnet 9.67.50.0 (WIRE3/1) first, followed by subnet 9.67.51.0 (WIRE3/2) and then 9.67.50.0 (WIRE3/3), which has the same subnet address as WIRE3/1, but specifies a higher address range:

```
inOrder: WIRE3 WIRE1
subnet 9.67.49.0 255.255.240.0 9.67.49.1-9.67.49.100 label:WIRE1/2
subnet 9.67.48.0 255.255.240.0 9.67.48.1-9.67.48.50 label:WIRE1/1
subnet 9.67.51.0 255.255.240.0 9.67.51.1-9.67.51.50 label:WIRE3/2
subnet 9.67.50.0 255.255.240.0 9.67.50.1-9.67.50.50 label:WIRE3/1
subnet 9.67.50.0 255.255.240.0 9.67.50.51-9.67.50.100 label:WIRE3/3
```

The following balance statement exhausts IP addresses equally in WIRE1/3 and WIRE1/4:

```
balance: WIRE1
subnet 9.67.49.0 255.255.240.0 9.67.49.101-9.67.49.200 label:WIRE1/3
subnet 9.67.48.0 255.255.240.0 9.67.48.201-9.67.48.300 label:WIRE1/4
```

A sequence of inOrder or balance statements is cumulative. For example, the statements:

```
inOrder: WIRE1
inOrder: WIRE3
```

have the cumulative effect of the single statement:

```
inOrder: WIRE1 WIRE3
```

Note:

To disable multiple subnets, comment out either the balance or inOrder processing statement or the priority.

## Defining Additional Options

To assign additional configuration parameters, use the Option statement. All clients inherit all globally-defined options. A client defined within a Subnet statement inherits global options and options defined for that address pool. To assign configuration parameters for all clients in a subnet, follow the Subnet statement with option statements surrounded by braces. For information about specifying options, see Specifying DHCP Options.

## Transforming Canonical Addresses

For 802.3 clients, use the canonical keyword to instruct the DHCP server to transform MAC addresses to canonical (byte starts with least significant bit) form. In most cases, you do not want the DHCP server to transform canonical addresses. MAC addresses of 802.3 clients are normally in canonical format on an 802.3 network. When 802.3 MAC addresses are transmitted across a transparent bridge, the bridge reformats the bits that identify an 802.3 client MAC address to a non-canonical (byte starts with most significant bit) form. When the bridge returns the MAC address to an 802.3 network, the bridge again reformats MAC addresses.

To cause the DHCP server to transform MAC addresses, use:

**canonical** *value*

*value*
The value is either NO (the default) or YES. NO prevents the DHCP server from transforming MAC addresses. YES causes the DHCP server to transform MAC addresses.

## Defining Classes

The Class statement specifies configuration parameters for a user-defined group of clients administered by a server. The scope of the Class statement is allowed at a global or subnet level. When the Class statement is specified within a Subnet statement, the server will only serve clients in the class that sre both located in the specified subnet and request the class.

For example, to create a class called "accounting" so member hosts can use the LPR server (option 9) at 9.67.123.2:

At the DHCP server, define a class called "accounting" and set the LPR server for that class to 9.67.123.2

At the client, configure the client to identify itself as belonging to the class "accounting"

When the client requests configuration information, the server sees that it belongs to the accounting class and provides configuration information that instructs the client to use the LPR server at 9.67.123.2. DHCP clients use option 77 to indicate their class to DHCP servers.

The format of the Class statement is:

**class** *class_name* [*range*]

*class_name*
The user-defined label that identifies the class. The class name is an ASCII string of up to 255 characters (for example, accounting). If the class name contains spaces, it must be surrounded by quotes.

*range*
To specify a range of addresses, enter addresses in dotted-decimal notation, beginning with the lower end of the range, followed by a hyphen, then the upper end of the range, with no spaces in between. For example, enter 9.17.32.1-9.17.32.128.

At a global level, a class cannot have a range. A range is only allowed when a class is defined within a subnet. The range can be a subset of the subnet range.

A client that requests an IP address from a class which has exhausted its range, is offered an IP address from the subnet range, if available. The client is offered the options associated with the exhausted class.

To assign configuration parameters such as a lease time for all clients in a class, follow the Class statement with Option statements surrounded by braces. For more information on options, see Specifying DHCP Options.

## Defining Clients

The Client statement is used to:

Specify a unique set of options for a client. You can assign a static address and configuration parameters, or configuration parameters only.

Exclude an IP address from a range of available IP addresses.

For more information on excluding addresses, see Excluding an IP Address for a DHCP Client.

## Configuring Options and an IP Address for a DHCP Client

To configure options for a specific DHCP client, follow the Client statement with Option statements surrounded by braces. For a specific client, the following statement reserves the static address 9.67.99.149 and also specifies a lease time (option 51) of 12 hours (43200 seconds) and a subnet mask (option 1):

```
client 6 10005aa4b9ab 9.67.99.149
{
   option 51 43200
   option 1 255.255.255.0
}
```

**Note:** Parameters to the right of a left parenthesis are used by the DHCP Server Configuration program. The DHCP server parses statements to the right of a left parenthesis as comments.

The format of the Client statement is:

**client** *hw_type clientID ipaddr* [(**alias=***name*]

*hw_type*
The hardware type of the client computer, required to decode the MAC address. For more information on hardware types, see Hardware Types.

*clientID*
The hexadecimal MAC address, or a string such as a domain name, or a name assigned to the client, such as the host name. If you specify a string, you must enclose it in quotes and specify zero as the hardware type.

*ipaddr*
The DHCP client's IP address, in dotted-decimal notation. The variable *ipaddr* must contain an address if unlisted clients are not supported.

**(alias=***name*

A symbolic name for ease in identifying the client. Enter **alias=***name* immediately after a left parenthesis. This symbolic name appears in the display of the server configuration. If no name is entered, the MAC address is used.

For more information about DHCP options, see Specifying DHCP Options.

## Configuring Options for a DHCP Client, Allowing Any IP Address

To specify options, but allow the DHCP server to choose the address from the subnet the DHCP client is in, use the ANY parameter. Do not specify an IP address. For example, to allow any IP address to be assigned to a specific client, but make sure that the lease time is a specific value such as 12 hours (43200 seconds) and the mask is 255.255.255.0, specify:

```
client 6 10005aa4b9ab ANY
{
   option 51 43200
   option 1 255.255.255.0
}
```

## Excluding a Client ID

If you do not want your DHCP server to accept requests from a particular client ID, you can exclude the client ID from service. The Client statement is allowed at global, subnet, or class levels. To exclude a client from service, specify the Client statement as follows:

**client** *hw_type clientID* **NONE**

*hw_type*

A number representing the hardware type, as defined in RFC 1530. The hardware type is needed to correctly interpret a clientID that is a MAC address.

*clientID*

Either the hexadecimal MAC address or a name assigned to the client, such as the host name. If you specify a name, you are required to enclose it in quotes and specify 0 for the hardware type.

**NONE**

NONE specifies no IP address and no options are served to the specified client ID.

For example:

client 6 10005aa4b9ab NONE

## Excluding an IP Address

To exclude one or more IP addresses from the pool of addresses available for lease, specify the Client statement:

```
client 0 0 9.67.3.123
client 0 0 9.67.3.222
```

In this case, the hardware type and the client ID are 0. IP addresses 9.67.3.123 and 9.67.3.222 are excluded. Specify a separate statement for each address to be excluded.

## Excluding a Range of IP Addresses

You can also exclude a range of IP addresses from the pool of addresses available for lease by specifying many Client statements.

**Note:** Using the DHCP Server Configuration program, it is recommended that each range of excluded addresses not contain more than 10 addresses. Each excluded address results in a separate Client statement in the configuration file. To exclude larger numbers of addresses, define subnets that do not include the addresses to be excluded. For example, to exclude addresses 50-75 in subnet 9.67.3.0, specify:

```
inOrder: WIRE1
subnet 9.67.3.0 255.255.240.0 9.67.3.1-9.67.3.49 label:WIRE1/1
subnet 9.67.3.0 255.255.240.0 9.67.3.1-9.67.3.100 label:WIRE1/2
```

## Reserving Values for a Specific BOOTP Client

Use the Client statement to provide a permanent IP address to BOOTP clients. Note, however, that only BOOTP options will be served. Any DHCP options specified will be ignored. For example:

```
client 1 03a5ca4b23cd 9.37.3.415
```

If you provide IP addresses to BOOTP clients, remember to change the value of supportBootP from NO (the default) to YES.

## Specifying the Next Bootstrap Server

To specify whether the DHCP server specifies a bootstrap server for clients, use:

**bootStrapServer** *value*

The *value* is the IP address of the bootstrap server for the client.

This statement can appear at the global level, or within Subnet, Class, or Client statements.

## Specifying the Bootfile Name

For clients that need a boot or to load images to initialize, the Bootfile option is provided by the DHCP server. The server specifies DHCP Option 67, Boot File Name. For additional ifnormation about DHCP options, see Appendix B, “Specifying DHCP Options” on page B-1. The client downloads the image from the BOOTP server.

## Defining Server and Lease Parameters

At a server level, you can define global parameters, including lease length, which clients are served, and additional server parameters, such as statistics snapshots and BOOTP support.

## Defining Lease Length

To specify the default lease duration for the leases issued by this server, use:

**leaseTimeDefault** *value*

The value is a decimal integer followed by a space and a unit of time, which can be years, months, weeks, days, hours, minutes, or seconds. The default is minutes.

**Default interval:** 24 hours (1440 minutes)

**Default unit:** minute

**Minimum:** 180 seconds

**Maximum:** -1, which is infinity

To apply a global lease time for all addresses issued by this server, specify this statement outside braces. To override this statement for a set of clients, use option 51 (IP address lease time) for a specific client, a class of clients, a subnet, or at the global level.

## Checking for Expired Leases

To specify the interval at which the lease condition of all addresses in the address pool is examined, use:

**leaseExpireInterval** *value*

The value is a decimal integer optionally followed by a space and a unit of time, which can be years, months, weeks, days, hours, minutes, or seconds. If the value is not followed by a unit, minutes are assumed. The value specified should be less than the value for leaseTimeDefault to ensure that expired leases are returned to the pool in a timely manner.

**Default interval:** 1 minute

**Default unit:** minute

**Minimum:** 15 seconds

**Maximum:** 12 hours

## Specifying Offering Hold Time

To specify the maximum amount of time the server holds an offered address in reserve while waiting for a response from the client, use:

**reservedTime** *value*

The value is a decimal integer optionally followed by a space and a unit of time, which can be years, months, weeks, days, hours, minutes, or seconds. If the value is not followed by a unit, minutes are assumed.

**Default interval:** 5 minutes

**Default unit:** minute

**Minimum:** 30 seconds

**Maximum:** -1, which is infinity

## Querying In-use Addresses

Before the server allocates an IP address, it PINGs the address to make sure it is not already in use by a host on the network. The server places an in-use address in a special pool and allocates a different address.

To specify the interval a DHCP server holds an in-use address in a special pool before returning the address to the active pool available for assignment, use:

**usedIPAddressExpireInterval** *value*

The value is a decimal integer optionally followed by a space and a unit of time, which can be years, months, weeks, days, hours, minutes, or seconds. If the value is not followed by a unit, minutes are assumed.

**Default interval:** 1000 seconds

**Default unit:** minute

**Minimum:** 30 seconds

**Maximum:** -1, which is infinity

## Specifying DHCP Server Responses to BOOTP Requests

To specify whether the server responds to requests from BOOTP clients, use:

**supportBootP** [**YES** | **NO**]

The default is NO. If this statement is not specified, or if any value other than YES is specified, the server will not respond to requests from BOOTP clients.

If this server previously supported BOOTP clients and has been reconfigured not to support BOOTP clients, the address binding for any BOOTP clients that was established before the reconfiguration will be maintained until the BOOTP client sends another request (when it is restarting). At that time, the server will not respond, and the binding will be removed.

This statement should be specified outside braces and, therefore, is used for all addresses issued by this server.

## Specifying DHCP Server Responses to Unregistered Clients

To specify whether the server responds to requests from DHCP clients other than those whose client IDs are specifically listed in this configuration file, use:

**supportUnlistedClients** [**YES** | **NO**]

The default is YES. If you specify NO, the server will respond only to requests from DHCP clients that are listed (by client ID) in the configuration file.

For example:

```
client 6 10005aa4b9ab ANY
client 6 10a03ca5a7fb ANY
```

If this statement is not specified, or if you specify YES, the server will respond to requests from any DHCP client. This option can be used to limit access to

addresses issued by this DHCP server. Listing the client IDs for all acceptable clients may be time consuming.

This statement should be specified outside braces and, therefore, is used for all addresses issued by this server.

## Specifying Statistics Snapshots

To specify the number of intervals that expire before the DHCP server takes a snapshot of statistics, use:

**statisticSnapshot** *value*

The length of each interval is determined by the leaseExpireInterval keyword. For example, a value of 3 will collect statistics after a span of three intervals, where each interval has a length specified by the leaseExpireInterval keyword. If no value is specified, the server takes a snapshot of statistics at the end of every lease expire interval. For more information on server statistics, see Displaying Server Statistics.

---

# Defining DHCP Log Files

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

Number of DHCP Log Files

Size of DHCP log files

Names of DHCP log files

At least one information type to log

## Defining the Number of DHCP Log Files

Specifiy the number of log files maintained, using:

**num_LogFiles** *value*

The value is the maximum number of log files maintained.

**Default interval:** 1000 seconds

**Default unit:** minute

**Minimum:** 30 seconds

**Maximum:** -1, which is infinity

---

# DHCP Server Configuration Files

The following files are used to manually configure a DHCP server:

\DHCPSD.CFG

Used for DHCP server configuration. The following configuration provides short lease intervals, causing rapid lease renewal for test purposes:

```
logFileName dhcpsd.log
logFileSize 100
numLogFiles 4
logItem SYSERR
logItem ACNTING
logItem OBJERR
logItem EVENT
logItem PROTERR
logItem WARNING
logItem INFO
logItem TRACE
logItem ACTION
supportBootP yes
supportUnlistedClients true

option 15  raleigh.ibm.com

# Addresses 8.67.112.24 through 8.67.112.25 do not inherit
# options defined for 8.67.112.26 through 8.67.112.30

subnet 8.67.112.0 255.255.255.0 8.67.112.24-8.67.112.25 label:network1/1
  (alias=network1
subnet 8.67.112.0 255.255.255.0 8.67.112.26-8.67.112.30 label:network1/2
  (alias=network1
{
  Option 1 255.255.255.0
  Option 3 8.67.112.1
  Option 6 8.67.112.10
  Option 33 8.0.0.0:8.67.72.1 8.67.112.0:8.67.72.1 8.67.96.0:8.67.72.1 8.
    112.9:8.67.72.1 8.67.96.10:8.67.72.1 8.67.112.19:8.67.72.1
}
```

\DHCPSD.LOG

Used to collect logging information. DHCPSD.LOG is specified by the logFileName statement in the DHCPSD.CFG file.

# Appendix B. Specifying DHCP Options

DHCP allows you to specify options, also known as BOOTP vendor extensions, to provide additional configuration information to the client. RFC 2132 defines the options that you can use. Each option is identified by a numeric code.

Architected options 0 though 127 and option 255 are reserved for definition by the RFC. The DHCP server, the DHCP client, or both server and client use options in this set. Some architected options can be modified by the administrator. Other options are for exclusive use by the client and server, Options which the administrator cannot or should not configure at the DHCP server include:

52, Option overload

53, DHCP message type

54, Server identifier

55, Parameter request list

56, Message

57, Maximum DHCP message size

60, Class identifier

Options 128 through 254 represent non-architected options that can be defined by administrators to pass information to the DHCP client to implement site-specific configuration parameters. Additionally, IBM provides a set of IBM-specific options such as option 192, TXT RR.

The format of user-defined options is:

**Option** *code value*

*code* can be any option code 1 through 254.

*value* must always be a string. At the server, it can be an ASCII string or a hexadecimal string. At the client, however, it always appears as a hexadecimal string as passed to the processing program.

The server passes the specified value to the client. You must, however, create a program or command file to process the value.

This section describes:

Configuration File Option Data Formats

Option Categories

## Configuration File Option Data Formats

RFC 2132 defines the following data formats for DHCP options:

**IP Address**, which is a single IP address in dotted-decimal notation.

**IP Addresses**, which is one or more IP addresses in dotted-decimal notation separated by white spaces.

**IP Address Pair**, which is two IP addresses in dotted-decimal notation separated by a single colon.

**IP Address Pairs**, which is one or more IP address pairs, each pair separated from another by a white space.

**Boolean**, which is 0 or 1.

**Byte**, which is a decimal number between -128 and 127 (inclusive).

**Unsigned Byte**, which is a decimal number between 0 and 255 (inclusive). You cannot specify a negative value for an unsigned byte.

**List of Unsigned Byte**, which is one or more decimal numbers between 0 and 255 (inclusive) separated by white spaces. You cannot specify a negative number for an unsigned byte.

**Short**, which is a decimal number between -32768 and 32767 (inclusive).

**List of Unsigned Short**, which is a decimal number between 0 and 65535 (inclusive). You cannot specify a negative number for an unsigned short.

**Unsigned Shorts**, which is one or more decimal numbers between 0 and 65535 (inclusive) separated by white spaces. You cannot specify a negative number for an unsigned short.

**Long**, which is a decimal value between -2147483648 and 2147483647 (inclusive).

**Unsigned Long**, which is a decimal value between 0 and 4294967295 (inclusive). You cannot specify a negative number for an unsigned long.

**String**, which is a string of characters. If embedded spaces are used, the string must be enclosed in double quotes.

**N/A**, which indicates no specification is needed because the client generates this information.

## Option Categories

There are 7 option categories:

Base Options
IP Layer Parameters per Host Options
IP Layer Parameters per Interface Options
Link Layer Parameters per Interface Options
TCP Parameter Options
Application and Service Parameter Options
DHCP Extensions Options

## Base Options

Following are the base options provided to the client:

1, Subnet Mask

2, Time Offset

3, Router

4, Time Server

5, Name Server

7, Log Server

8, Cookie Server

9, LPR Server

10, Impress Server

11, Resource Location Server

12, Host Name

13, Boot File Size

14, Merit Dump File

15, Domain Name

16, Swap Server

17, Root Path

18, Extensions Path

## Option 1, Subnet Mask

The client's subnet mask, specified in 32-bit dotted decimal notation.

Configuration file format: Unsigned long

## Option 2, Time Offset

The offset (in seconds) of the client's subnet from Coordinated Universal Time (CUT). The offset is a signed 32-bit integer.

Configuration file format: Long

## Option 3, Router

IP addresses (in order of preference) of the routers on the client's subnet.

Configuration file format: IP addresses

## Option 4, Time Server

IP addresses (in order of preference) of the time servers available to the client.

Configuration file format: IP addresses

## Option 5, Name Server

IP addresses (in order of preference) of the IEN 116 name servers available to the client.

Configuration file format: IP addresses

## Option 7, Log Server

IP addresses (in order of preference) of the MIT-LCS UDP Log servers available to the client.

Configuration file format: IP addresses

## Option 8, Cookie Server

IP addresses (in order of preference) of the Cookie or quote-of-the-day servers available to the client.

Configuration file format: IP addresses

## Option 9, LPR Server

This option can be specified at both the DHCP client and DHCP server. However, if specified only at the DHCP client, the configuration will be incomplete.

IP addresses (in order of preference) of the line printer servers available to the client. Option 9 eliminates the need for the client to specify the LPR_SERVER environment variable.

Configuration file format: IP addresses

## Option 10, Impress Server

IP addresses (in order of preference) of the Imagen Impress servers available to the client.

Configuration file format: IP addresses

## Option 11, Resource Location Server

IP addresses (in order of preference) of the Resource Location (RLP) servers available to the client. RLP servers allow clients to locate resources that provide a specified service, such as a domain name server.

Configuration file format: IP addresses

## Option 12, Host Name

This option can be specified at both the DHCP client and DHCP server. If the DHCP client does not provide a host name, the DHCP server does nothing with option 12.

Host name of the client (which may include the local domain name). The minimum length for the host name option is 1 octet and the maximum is 32 characters. See RFC 1035 for character set restrictions.

Configuration file format: String

## Option 13, Boot File Size

The length (in 512-octet blocks) of the default boot configuration file for the client.

Configuration file format: Unsigned short

## Option 14, Merit Dump File

The path name of the merit dump file in which the client's core image is stored if the client crashes. The path is formatted as a character string consisting of characters from the Network Virtual Terminal (NVT) ASCII character set. The minimum length is 1 octet.

Configuration file format: String

## Option 15, Domain Name

This option can be specified at both the DHCP client and DHCP server. For more information on the DHCP server appending a domain name if the DHCP client does not provide a domain name, see Appending Client Domain Names.

Domain name that the client uses when resolving host names using the Domain Name System. The minimum length is 1 octet.

Configuration file format: String

## Option 16, Swap Server

IP address of the client's swap server.

Configuration file format: IP address

## Option 17, Root Path

Path that contains the client's root disk. The path is formatted as a character string consisting of characters from the NVT ASCII character set. The minimum length is 1 octet.

Configuration file format: String

## Option 18, Extensions Path

The extensions path option allows you to specify a string that can be used to identify a file that is retrievable using Trivial File Transfer Protocol (TFTP).

The minimum length is 1 octet.

Configuration file format: String

---

## IP Layer Parameters per Host Options

Following are the options that affect the operation of the IP layer on a per host basis:

19, IP Forwarding

20, Non-Local Source Routing

21, Policy Filter

22, Maximum Datagram Reassembly Size

23, Default IP Time-To-Live

24, Path MTU Aging Timeout

25, Path MTU Plateau Table

## Option 19, IP Forwarding

Enable (1) or disable (0) forwarding by the client of its IP layer packets.

Configuration file format: Boolean

## Option 20, Non-Local Source Routing

Enable (1) or disable (0) forwarding by the client of its IP layer datagrams with non-local source routes. The length is 1 octet.

Configuration file format: Boolean

## Option 21, Policy Filter

IP address-net mask pair used to filter datagrams with non-local source routes. Any datagram whose next hop address does not match one of the filter pairs is discarded by the client. The minimum length for the policy filter option is 8 octets.

Configuration file format: IP address pair

## Option 22, Maximum Datagram Reassembly Size

Maximum size datagram the client will reassemble. The minimum value is 576.

Configuration file format: Unsigned short

## Option 23, Default IP Time-To-Live

Default time-to-live (TTL) the client uses on outgoing datagrams. TTL is an octet with a value between 1 and 255.

Format: Unsigned byte

## Option 24, Path MTU Aging Timeout

Timeout in seconds used to age Path Maximum Transmission Unit (MTU) values discovered by the mechanism that is described in RFC 1191.

Configuration file format: Unsigned long

## Option 25, Path MTU Plateau Table

Table of MTU sizes to use in Path MTU discover as defined in RFC 1191. The minimum MTU value is 68. The minimum length for the path MTU plateau table option is 2 octets. The length must be a multiple of 2.

Configuration file format: Unsigned shorts

## IP Layer Parameters per Interface Options

Following are the options that affect the operation of the IP layer on a per interface basis. The client may issue multiple requests, one per interface, when configuring interfaces with their specific parameters.

26, Interface MTU

27, All Subnets are Local

28, Broadcast Address

29, Perform Mask Discovery

30, Mask Supplier

31, Perform Router Discovery

32, Router Solicitation Address

33, Static Route

## Option 26, Interface MTU

Maximum Transmission Unit (MTU) to use on this interface. The minimum MTU value is 68.

Configuration file format: Unsigned short

## Option 27, All Subnets are Local

Client assumes (1) or does not assume (0) all subnets use the same Maximum Transmission Unit (MTU). A value of 0 means the client assumes some subnets have smaller MTUs.

Configuration file format: Boolean

## Option 28, Broadcast Address

Broadcast address used on the client's subnet.

Configuration file format: IP address

## Option 29, Perform Mask Discovery

Client performs (1) or does not perform (0) subnet mask discovery using Internet Control Message Protocol (ICMP).

Configuration file format: Boolean

## Option 30, Mask Supplier

Client responds (1) or does not respond (0) to subnet mask requests using Internet Control Message Protocol (ICMP).

Configuration file format: Boolean

## Option 31, Perform Router Discovery

Client solicits (1) or does not solicit (0) routers using router discovery as defined in RFC 1256.

Configuration file format: Boolean

## Option 32, Router Solicitation Address

Address to which a client transmits router solicitation requests.

Configuration file format: IP address

## Option 33, Static Route

Static routes (destination address-router pairs in order of preference) the client installs in its routing cache. The first address is the destination address and the second address is the router for the destination. Do not specify 0.0.0.0 as a default route destination.

Configuration file format: IP address pairs

---

# Link Layer Parameters per Interface Options

Following are the options that affect the operation of the data link layer on a per-interface basis:

34, Trailer Encapsulation

35, ARP Cache Timeout

36, Ethernet Encapsulation

## Option 34, Trailer Encapsulation

Client negotiates (1) or does not negotiate (0) the use of trailers when using Address Resolution Protocol (ARP). For more information, see RFC 893.

Configuration file format: Boolean

## Option 35, ARP Cache Timeout

Timeout in seconds for Address Resolution Protocol (ARP) cache entries.

Configuration file format: Unsigned long

## Option 36, Ethernet Encapsulation

For an Ethernet interface, client uses IEEE 802.3 (1) Ethernet encapsulation described in RFC 1042 or Ethernet V2 (0) encapsulation described in RFC 894.

Configuration file format: Boolean

## TCP Parameter Options

Following are the options that affect the operation of the TCP layer on a per-interface basis:

37, TCP Default TTL

38, TCP Keep-alive Interval

39, TCP Keep-alive Garbage

## Option 37, TCP Default TTL

Default time-to-live (TTL) the client uses for sending TCP segments.

Configuration file format: Unsigned byte

## Option 38, TCP Keep-alive Interval

Interval in seconds the client waits before sending a keep-alive message on a TCP connection. A value of 0 indicates the client does not send keep-alive messages unless requested by the application.

Configuration file format: Unsigned long

## Option 39, TCP Keep-alive Garbage

Client sends (1) or does not send (0) TCP keep-alive messages that contain an octet of garbage for compatibility with previous implementations.

Configuration file format: Boolean

## Application and Service Parameter Options

Following are options that can be used to configure miscellaneous applications and services:

40, Network Information Service Domain

41, Network Information Servers

42, Network Time Protocol Servers

43, Vendor-Specific Information

44, NetBIOS over TCP/IP Name Server

45, NetBIOS over TCP/IP Datagram Distribution Server

46, NetBIOS over TCP/IP Node Type

47, NetBIOS over TCP/IP Scope

48, X Window System Font Server

49, X Window System Display Manager

## Network Information Service Domain Option 40

The client's Network Information Service (NIS) domain. The domain is formatted as a character string consisting of characters from the NVT ASCII character set. The minimum length is 1 octet.

Configuration file format: String

## Option 41, Network Information Servers

IP addresses (in order of preference) of Network Information Service (NIS) servers available to the client.

Configuration file format: IP addresses

## Option 42, Network Time Protocol Servers

IP addresses (in order of preference) of Network Time Protocol (NTP) servers available to the client.

Configuration file format: IP addresses

## Option 43, Vendor-Specific Information

Option 43 is specified only at the DHCP server, which returns this option as an encapsulated packet to a client that sends option 60, Class Identifier.

This information option is used by clients and servers to exchange vendor-specific information. This option has been added to allow for expansion of the number of options that can be supported.

Configuration file format: String

## Option 44, NetBIOS over TCP/IP Name Server

IP addresses (in order of preference) of NetBIOS name servers (NBNS) available to the client.

Configuration file format: IP addresses

## Option 45, NetBIOS over TCP/IP Datagram Distribution Server

IP addresses (in order of preference) of NetBIOS datagram distribution (NBDD) name servers available to the client.

Configuration file format: IP addresses

## Option 46, NetBIOS over TCP/IP Node Type

Node type used for NetBIOS over TCP/IP configurable clients as described in RFC 1001 and RFC 1002.

Values to specify client types include:

| Value | Node Type |
|---|---|
| **0x1** | B-node |
| **0x2** | P-node |
| **0x4** | M-node |

**0x8** H-node

Configuration file format: Unsigned byte

## Option 47, NetBIOS over TCP/IP Scope

NetBIOS over TCP/IP scope parameter for the client, as specified in RFC 1001/1002. The minimum length is 1 octet.

Configuration file format: Unsigned byte

## Option 48, X Window System Font Server

IP addresses (in order of preference) of X Window System font servers available to the client.

Configuration file format: IP addresses

## Option 49, X Window System Display Manager

IP addresses (in order of preference) of systems running X Window System Display Manager available to the client.

Configuration file format: IP addresses

---

## DHCP Extensions Options

Following are the available options that are specific to DHCP.

50, Requested IP Address

51, IP Address Lease Time

58, Renewal (T1) Time Value

59, Rebinding (T2) Time Value

60, Class-Identifier

62, NetWare/IP Domain Name

63, NetWare/IP

64, NIS Domain Name

65, NIS Servers

66, Server Name

67, Boot File Name

68, Home Address

69, SMTP Servers

70, POP3 Server

71, NNTP Server

72, WWW Server

73, Finger Server

74, IRC Server

75, StreetTalk Server

76, STDA Server

77, User Class

78, Directory Agent

79, Service Scope

80, Naming Authority

## Option 50, Requested IP Address

This option is specified only at the DHCP client. The DHCP server can refuse a DHCP client request for a specific IP address.

Allows the client to request (DHCPDISCOVER) a particular IP address.

Configuration file format: N/A

## Option 51, IP Address Lease Time

This option can be specified at both the DHCP client and DHCP server. The DHCP client can use option 51 to override the defaultLeaseInterval value the DHCP server offers.

Allows the client to request (DHCPDISCOVER or DHCPREQUEST) a lease time for an IP address. In a reply (DHCPOFFER), a DHCP server uses this option to offer a lease time.

This option may be specified in a network, subnet, or class of client definition. Use 0xffffffff to indicate an infinite (permanent) lease.

Configuration file format: Unsigned long

## Option 58, Renewal (T1) Time Value

Interval in seconds between the time the server assigns an address and the time the client transitions to the renewing state.

Configuration file format: Unsigned long

## Option 59, Rebinding (T2) Time Value

Interval in seconds between the time the server assigns an address and the time the client enters the rebinding state.

Configuration file format: Unsigned long

## Option 60, Class-Identifier

This option is sent by the DHCP client. This information is generated by the client and does not have to be specified.

Type and configuration of the client, supplied by the client to the server. For example, the identifier may encode the client's vendor-specific hardware configuration. The information is a string of **n** octets, interpreted by servers. For example:

```
hex"01 02 03"
```

Servers not equipped to interpret the class-specific information sent by a client must ignore it. The minimum length is 1 octet.

Configuration file format: N/A

## Option 62, NetWare/IP Domain Name

Netware/IP Domain Name.

The minimum length is 1 octet and the maximum length is 255.

Configuration file format: String

## Option 63, NetWare/IP

A general purpose option code used to convey all the NetWare/IP related information except for the NetWare/IP domain name. A number of NetWare/IP sub-options will be conveyed using this option code.

The minimum length is 1 and the maximum length is 255.

Configuration file format: String

## Option 64, NIS Domain Name

Network Information Service (NIS)+ V3 client domain name. The domain is formatted as a character string consisting of characters from the NVT ASCII character set. Its minimum length is 1.

Configuration file format: String

## Option 65, NIS Servers

IP addresses (in order of preference) of Network Information Service (NIS)+ V3 servers available to the client.

Configuration file format: IP addresses

## Option 66, Server Name

Trivial File Transfer Protocol (TFTP) server name used when the "sname" field in the DHCP header has been used for DHCP options

Configuration file format: String

## Option 67, Boot File Name

Name of the boot file when the 'file' field in the DHCP header has been used for DHCP options. The minimum length is 1.

**Note:** Use this option to pass a boot file name to a DHCP client. The boot file name is required to contain the fully-qualified path name and be less than 128 characters in length. For example:

```
option 18 c:\usr\lpp\tcpip\nstation\standard\kernel
```

This file contains information that can be interpreted in the same way as the 64-octet vendor-extension field within the BOOTP response, with the exception that the file length is limited to 128 characters by the BOOTP header.

Configuration file format: String

## Option 68, Home Address

IP addresses (in order of preference) of the mobile IP home agents available to the client. The option enables a mobile host to derive a mobile home address, and determine the subnet mask for the home network. The usual length will be four octets, containing a single home agent's home address.

Configuration file format: IP addresses

## Option 69, SMTP Servers

IP addresses (in order of preference) of the Simple Mail Transfer Protocol (SMTP) servers available to the client.

Configuration file format: IP addresses

## Option 70, POP3 Server

IP addresses (in order of preference) of the Post Office Protocol (POP) servers available to the client.

Configuration file format: IP addresses

## Option 71, NNTP Server

IP addresses (in order of preference) of the Network News Transfer Protocol (NNTP) servers available to the client. For example:

```
option 71 "9.24.112.2"
```

Configuration file format: IP addresses

## Option 72, WWW Server

IP addresses (in order of preference) of the World Wide Web (WWW) servers available to the client.

Configuration file format: IP addresses

## Option 73, Finger Server

IP addresses (in order of preference) of the Finger servers available to the client.

Configuration file format: IP addresses

## Option 74, IRC Server

IP addresses (in order of preference) of the Internet Relay Chat (IRC) servers available to the client.

Configuration file format: IP addresses

## Option 75, StreetTalk Server

IP addresses (in order of preference) of the StreetTalk servers available to the client.

Configuration file format: IP addresses

## Option 76, STDA Server

IP addresses (in order of preference) of the StreetTalk Directory Assistance servers available to the client.

Configuration file format: IP addresses

## Option 77, User Class

DHCP clients use option 77 to indicate to DHCP servers what class the host is a member of.

Configuration file format: string

## Option 78, Directory Agent

The Dynamic Host Configuration Protocol provides a framework for passing configuration information to hosts on a TCP/IP network. Entities using the Service Location Protocol need to find out the address of Directory Agents in order to transact messages. In certain other instances they may need to discover the correct scope and naming authority to be used in conjunction with the service attributes and URLS which are exchanged using the Service Location Protocol.

A directory agent has a particular scope, and may have knowledge about schemes defined by a particular naming authority.

Configuration file format: IP address

## Option 79, Service Scope

This extension indicates a scope that should be used by a service agent, when responding to Service Request messages as specified by the Service Location Protocol.

Configuration file format: string

## Option 80, Naming Authority

This extension indicates a naming authority (which specifies the syntax for schemes that may be used in URLs for use by entities with the Service Location Protocol.

Configuration file format: string

---

# IBM-Specific Options

IBM provides a set of IBM-specific options that fall within non-architected options 128-254 that administrators use to implement site-specific configuration parameters.

Additionally, architected option 43 allows the definition of encapsulated, vendor-specific options. IBM Corporation, for example, has added the following IBM-specific options, denoted by an IBM-specific file in Option 60.

Options encapsulated as vendor-specific information must be carefully defined and documented to permit interoperability between clients and servers from different vendors. Vendors defining vendor-specific information must:

Document those options in the form specified in RFC 2132.

Choose to represent those options either in data types already defined for DHCP options or in other well-defined data types.

Choose options that can be readily encoded in configuration files for exchange with servers provided by other vendors.

Be readily supportable by all servers.

Servers not equipped to interpret the vendor-specific information sent by a client must ignore it.

Clients which do not receive desired vendor-specific information should make an attempt to operate without it. Refer to RFC 2131 and RFC 2132 for additional information about this option.

## Option 200, LPR Printer

Eliminates the need for the client to specify the LPR_PRINTER environment variable, which can be the name of a device such as LPT1 or a printer name (queue name) such as Printer.

For example:

```
option 200 "lpt1"
```

An OS/2 client stores the updated option value in the TCPOS2.INI file.

The length is 1 octet.

Configuration file format: String

# Appendix C. Hardware Types

Possible hardware types are:

| Type | Description |
|---|---|
| **0** | Unspecified. If you specify a symbolic name for the client ID, specify 0 for the hardware type. |
| **1** | Ethernet (100Mb) |
| **6** | IEEE 802 Networks (which includes 802.5 Token Ring) |

# Appendix D. Trouble Shooting and Problem Solving

This appendix contains information to help you recover from error situations such as:

PANIC mode at an IBM Network Station

Problems with monitors

Cursor problems

Java problems

## Trouble Shooting

Table D-1 contains potential problem situations, a symptom description, and possible recovery actions you should try.

*Table D-1 (Page 1 of 5). Problem Determination Chart*

| **Problem Description Table** | |
|---|---|
| **Symptom** | **What you should do** |
| **Monitor Problems** | |
| Display image too large to fit on monitor | IBM Network Station may be set to automatically detect which monitor you are using. For autodetect to work correctly, you must have the monitor turned on before you boot the IBM Network Station System unit. |
| **BOOTP Problems (for VM)** | |
| BOOTP table can not be read | The BOOTP table will have to be restored from a backup copy. |
| **PTF Problems** | |
| PTFs not working | If the PTFs being installed are for the IBM Network Station Manager product, you may have to reboot the IBM Network Station system unit. This causes a new software download to the system unit to take place. The new downloaded software contains the program fixes for the IBM Network Station system unit. |
| **No Login Window (for VM)** | |
| No Login window on monitor - User Services window appears instead | The most likely cause is an incorrect entry for this IBM Network Station in the BOOTP table. See Chapter 6, “Configuring the Bootstrap Protocol Server for VM” on page 6-1 to display the information about this IBM Network Station.<br>Another possible cause is that the default configuration file on the server has been corrupted or deleted. The default configuration file, standard.nsm, is located in the /configs subdirectory of the directory indicated in the hd tag of the BOOTP table entry. A reinstallation of the IBM Network Station Manager for S/390 licensed program may be required. |
| **Java Problems** | |
| Java error messages: Can not find class, too many copies, out of memory, IO exception. | See “Problem Analysis when Running Java” on page D-6 for more information about recovery when these messages occur. |
| Text does not appear or is a different style. | Check the font sizes and styles. They may need to be changed to a different setting. Not all fonts are available on all JVMs. |

| *Table D-1 (Page 2 of 5). Problem Determination Chart* | |
|---|---|
| **Problem Description Table** | |
| Data written to a file does not appear in the file. | Make sure the Java applet or application closes the file to force all data to be written to the file. |
| Applet cannot read Properties or get a Security Exception while trying to read the System Properties | Applets may only read properties which are explicitly allowed by the system configuration. A property can be configured to be accessible by defining a new property of the form .applet and assigning it a value of true. This may be done through the Network Station Manager in the AppletViewer configuration section. The default properties which may be read by an applet are:<br>java.vendor<br>java.version<br>java.vendor.url<br>java.class<br>os.name<br>os.version<br>os.arch<br>file.separator<br>path.separator<br>line.separator<br>If the class sun.applet.AppletViewer is used to view applets, the accessible property list will differ from above and depend on the property file defined within the users' home directory. |
| Cursor does not appear in text field or Window layout (for example, button positions) appears different from the way it appears when the applet is run on another platform | The Java Abstract Window Toolkit (AWT) is designed to create a development environment independent of the underlying windowing mechanisms. These classes utilize the native window calls to do the work, but provide a uniform interface to programmers. However, Java Abstract Window Toolkit cannot hide all the differences. Thus appearances may change from one Java Virtual Machine on one platform to another Java Virtual Machine on a different platform. |
| Can not close Java error message box | Scroll to the end of the error message box and click OK. |
| **Environment Variables - Java Applet Viewer** | |
| Environment variable not replaced | Environment variables cannot be used when working with properties in the Java Applet Viewer section of the IBM Network Station Manager. The property value does not get replaced with the Environment Variable value. For example, if you declared name=${IP} in the properties box, you might expect to get the IP address of workstation user. Instead, you get ${IP}. |
| **Panic Appears on your workstation** | |
| P A N I C appears on your workstation | See “PANIC Mode at an IBM Network Station” on page D-5 for more information on recovering from a PANIC situation. |
| **Cursor Problems** | |
| 3270 cursor will not reposition using mouse | To reposition the cursor using the mouse, you must first use the mouse to position the mouse pointer. Then, press the Shift key and click the left mouse button. The cursor will move to that position. |

| *Table D-1 (Page 3 of 5). Problem Determination Chart* | |
|---|---|
| **Problem Description Table** | |
| Busy cursor (cursor seems busy trying to perform a task) | The first time you open an application from the workstation menu bar the cursor stays busy until the application finishes loading. Additional requests for another session of the same application will show the cursor only being busy for 3 seconds. Depending on network traffic, the application may take longer than 3 seconds to appear. The application is loading; however, the cursor will not show busy for over 3 seconds. |
| Cursor in wrong position within an application | When you leave one application to go to another application using the mouse, the cursor may not be at the same position when you return. The cursor probably repositioned itself to the place where you clicked the mouse to re-enter the application. You can reposition the cursor using the directional arrow keys. |
| **Color Problems** | |
| Colors appear incorrectly in applications | Color capabilities are fixed at 256 available colors. Some applications will use as many colors as possible, thus leaving no colors for additional applications. Try to start other applications before starting an application that uses a large number of colors. Applications that do not use 256 colors may have to be changed to use 256 color support. |
| **Keystrokes** | |
| Unwanted keystrokes appearing in applications | If the screen saver comes on while you are in an application and you press a key to end the screen saver, that keystroke will appear in your application. Remove the unwanted keystroke. |
| **Host Unknown or Unknown Host Message** | |
| Host Unknown message appears on workstation | This message could appear if:<br>a wrong system name or IP address was specified while using the program or menu functions of Startup Tasks in the IBM Network Station Manager program<br>a wrong system name or IP address was specified when opening a 3270 or 5250 session<br>TCP/IP name resolution is not occurring while using the program or menu functions of Startup Tasks in the IBM Network Station Manager program<br>You should validate the system name or IP address. Also, you should access the Hardware Setup Task and specify to use the Update host table and DNS configuration from server field. Updating this field refreshes your TCP/IP name resolution information for the IBM Network Station. Therefore, if new systems were integrated into your network, their IP address or system names would be known. You must log off and log on for the name information to become available. |
| **Screen Flashes** | |
| Screen flashing or crackling sound | Screen flashes, along with some crackling sounds, can occur when you are logging out of the workstation. The flashing will not harm any hardware or applications. |
| **IBM Network Station Manager Program** | |

| *Table D-1 (Page 4 of 5). Problem Determination Chart* | |
|---|---|
| **Problem Description Table** | |
| Changed Hardware workstation settings not being applied | Some changes require the IBM Network Station to be rebooted before they take effect. If you have rebooted the IBM Network Station and the changes are still not applied, use the IBM Setup Utility, Select F5 (Set Network Parameters) and make sure the IP Addressed from parameter value is Network. If the IP Addressed from parameter value is NVRAM, the IBM Network Station will not be able to use DHCP or BOOTP to determine the name of its workstation-specific settings file. It is recommended that the IP Addressed from parameter be set to Network to use DHCP or BOOTP. See Chapter 12, “Working with the IBM Network Station Setup Utility” on page 12-1 for more information.<br><br>**Note:** The DHCP or BOOTP server must specify the host name. |
| Inactive Navigational buttons in Help | In Help text, the navigational buttons (Back and Next) will not become active until you have linked to other topics. Once you have moved, by linking other topics, you establish a history of that movement. The buttons use this history to determine if the Back and Next buttons can be used. |
| Pulldown box will not stay open to accept Hardware setting changes. | If you are running a browser in a Windows environment, change the screen size to something other than 640 X 480.<br><br>You can also try resizing your current window and then try to open the pulldown again.<br><br>Try scrolling the window to change the position of the pulldown. This may give pulldowns that contain many items space to display the pulldown items. |
| Resizing the Netscape window causes problems | If you resize the Netscape window while the IBM Network Station Manager program is being loaded into it, Netscape may stop the load and you will not get a sign-on screen. You will have to close the IBM Network Station Manager browser window and restart the program; wait until after the logon screen is displayed before you resize the window.<br><br>After signing on, resizing the Netscape window may cause the server name or name of the user whose defaults you are displaying to disappear. This will not affect the operation of the IBM Network Station Manager program. |
| Resizing the Netscape window when using AIX causes loss of data input on IBM Network Station Manager program panels | Do not resize the window after you have entered data. Resizing the window resets the values. |
| Microsoft Internet Explorer windows are displayed behind the main window | In the IBM Network Station Manager program, if you request help or a list of users, a popup window is opened to contain the requested information. Internet Explorer may open the popup window behind the larger main window from which you made the request. To find the popup, you may need to move or minimize the larger window. |
| Changed keyboard setting has not been applied | Reboot your IBM Network Station in order for the changed keyboard setting to take effect. |
| Update of boot monitor has not been installed. | Reboot your IBM Network Station in order for the updated boot monitor to take effect. |
| Changes made to Hardware settings (other than keyboard and boot monitor), Startup Programs, Menus or Environment Variables, Desktop Manager, or Internet Network settings have not been applied. | Logoff the IBM Network Station, then logon to the IBM Network Station in order for the changes to take effect. |

| *Table D-1 (Page 5 of 5). Problem Determination Chart* | |
|---|---|
| **Problem Description Table** | |
| Changes made to 5250, 3270, or IBM Browser have not been applied. | End your application session and restart a new application session in order for the changes to take effect. |
| Changes made to the Applet Viewer have not been applied. | Logoff the IBM Network Station, then logon to the IBM Network Station in order for the changes to take effect. |
| IBM Network Station Manager program will not start. | This could be because:<br>The ICS server is not running.<br>The ICS server is not configured correctly. |
| **Browser Problems** | |
| The IBM Network Station Browser will not start. | This could be because you deleted the IBM Network Station Manager for S/390 licensed program and then reinstalled it.<br>In deleting the licensed program, some of the files that support the IBM Network Station Browser were also deleted.<br>Reinstall the IBM Network Station Browser licensed program. |
| Error message 404 - file not found | Verify the spelling and case sensitivity of the URL you used to access the IBM Network Station Manager program.<br>If the spelling and case of the URL are correct, you can check the directives specified in the ICS server configuration. Directives are statements in the ICS server configuration that allow access to the ICS server. See Chapter 4, “Configuring the Internet Connection Secure Server for OS/390” on page 4-1 for more information. |

## PANIC Mode at an IBM Network Station

A panic is an irrecoverable error condition that causes the IBM Network Station operating system to stop running.

To recover the IBM Network Station from this condition, power off the IBM Network Station system unit and then power it back on.

To receive assistance on the cause of the error condition, you must upload the DUMP file to the host system.

To determine the name of the DMP file, add the last 8 digits of the MAC address to the letters DMP. For example 80964234.DMP.

## File Transmission and Maximum Transmission Units

The Token Ring Network Station ships with a Token Ring Maximum Transmission Unit (MTU) of 1492 bytes. This value is used to determine the size of an MTU, or frame of data, when the IBM Network Station is sending data to a host. This value should work well for most network configurations. You should make sure that this value does not exceed the value of the MTU for token ring in your TCP/IP profile for an S/390, if specified.

**Note:** Even if the MTU is set to an acceptable value, other components in your network such as routers and bridges may support (or be configured to support) a smaller MTU value.

The MTU value set in the IBM Network Station should not exceed the MTU value of the system or any network component which is part of the communications path between the IBM Network Station and the system.

The current maximum values for the MTU on the Token Ring line description are 4060 for 4 Mbit Token Ring and 16393 for 16 Mbit Token-Ring. In future releases, these maximum values may change. Consult your system documentation for details. You can set the value of the Token Ring MTU on the IBM Network Station. At the Boot Monitor command entry prompt (">"):

1. Reboot your IBM Network Station.
2. When you see the message *NS0500 Search for host system*, or while the status bar is displayed showing the progress of loading the IBM Network Station kernel, press the Escape key.
3. Press the Ctrl-Alt-Shift-F1 key combination.
4. Enter "TM xxxxx", where xxxxx is the new MTU value (in bytes).
5. Reboot your IBM Network Station.

## Problem Analysis when Running Java

If the Java applet or application does not start, examine the messages that are displayed in the User Services' console. These should give an indication of any problems that are found by the JVM in running the program. In addition, you can determine whether the JVM is loaded by noting a change in the amount of memory currently being used as found in User Services' Statistics. See Chapter 11, “Working with User Services” on page 11-1 for more information.

Examples of some Java error messages follow:

**Cannot find class or class not found**

The JVM cannot find the class file requested by the Java applet or application. If the error is returned while running a Java application, inspect the class path that is specified in the IBM Network Station Manager Startup programs or menus. Confirm that the directories which include class files that are associated with the program are contained within the class path and that they have the correct format. Also, ensure that the name in the Application (Class) Name field does not contain the .class file name extension.

If the classes are provided in a zip file, the fully qualified zip file name must explicitly appear within the class path. In addition, due to differences in file systems, the classes may not be found since they are referred to in a case-sensitive manner. It may be possible to rename the class to the name that is indicated in the console messages.

For an applet, the codebase portion of the applet tag within the HTML file lists the locations where classes are found.

Also, check the file access permissions on the directories and files to make sure that users are allowed to read the files.

**Too many copies are already running**

If you already have a Java application that is running, you cannot start another Java application or a Java applet.

If you have one or more Java applets running (including applets within a browser), you cannot start a Java application.

**Out of memory**

The IBM Network Station system unit may not have enough memory to run the application or applet. Possible causes include:

Other applications are using memory, and not enough memory is left for the Java application or applet to run.

The stack size and heap size parameters need to be adjusted. The stack and heap sizes can be set using the IBM Network Station Manager. For applications, the parameters are set in the Startup Tasks (programs or menus) section. For an applet, the parameters are set in the Network Tasks (Applet Viewer section).

**IO exception while reading: (a remote server name)**

An HTTP address rather than a file system location was passed to the applet viewer. AppletViewer is essentially a browser that needs to have a defined proxy server and port before it can load HTTP files. To do this, you need to set the HTTP proxy or Socks Host parameter by using the IBM Network Station Manager program. Select the Internet Setup Task and then the Network section.

If you are loading the applet from your host, you do not need to use an HTTP address. Instead, you can simply fill in the local path and HTML file name.

**IO exception while reading: (a file name)**

Ensure that you specified a valid HTML file name as the startup programs or menus URL name in the IBM Network Station Manager program. Also, ensure that the file is readable by the user.

**Launcher Shutdown Monitor**

If your applet does not start and the next message in the console is Launcher Shutdown Monitor, ensure that you specified a valid HTML file name as the startup programs or menus URL name in the IBM Network Station Manager program. Also ensure that the file is readable by the user.

**Unusable class name: (name)**

Check the name in the field Application (Class) Name field in the startup programs or menus section in the IBM Network Station Manager program. Do not include a path or the .class file name extension in this field.

**Other**

If you do not see any messages in the User Services Console window that explain your problem, set Verbose messages on using the IBM Network Station Manager program. For applications, Verbose messages can be set in the Startup Tasks (programs or menus) section. For an applet, Verbose messages can be set in the Network Tasks (Applet Viewer section). Additional messages will now be displayed when your application or applet is run.

# Appendix E. National Language Support

Only selected S/390 national languages are supported at this time. The following list contains the software feature number and the language.

```
2922   Portuguese
2923   Dutch
2924   U.S. English
2925   Finnish
2926   Danish
2928   French
2929   German
2931   Spanish
2932   Italian
2933   Norwegian
2937   Swedish
2939   German MNCS (multinational character set)
2940   French MNCS
2942   Italian MNCS
2958   Icelandic
2963   Belgian Dutch
2966   Belgian French
2980   Brazilian Portuguese
2981   Canadian French
2996   Portuguese MNCS
```

**Notes:**

1. IBM Network Station NLV support is ASCII code page 819 (ISO equivalent of code page 850).
2. Code Page 819 supports all languages supported by the 3270 emulator of the IBM Network Station by using the configured language that is supplied by IBM Network Station Manager (or its equivalent function).
3. Software will be NLV-enabled, not translated (U.S. English MRI only).

# Appendix F. IBM Network Station Manager Program Shipped Default Settings

The following table contains all the IBM Network Station Manager Program shipped default settings. The settings are presented in the same order that is found in the Setup Tasks frame when you open the IBM Network Station Manager program.

*Table F-1. IBM Network Station Hardware Default Settings*

| **Hardware Default Settings** | |
|---|---|
| **Item:** | **Default Value:** |
| Mouse settings: | Right-handed |
| Mouse button configuration | Medium |
| Mouse pointer speed | |
| Keyboard settings: | Medium |
| Keyboard Repeat rate | Medium delay |
| Keyboard Repeat delay | Default from terminal |
| Keyboard mapping language | |
| Monitor settings: | 10 |
| Minutes before screen saver turns on | IBM bitmap |
| Screen saver | 20 |
| Minutes before monitor standby | 40 |
| Minutes before monitor suspend | 60 |
| Minutes before monitor power down | IBM bitmap |
| Desktop background | |
| Miscellaneous settings: | On |
| Parallel printer port | No |
| Allocate memory to speed window refresh | No update |
| Update boot monitor from the hardware settings file | |

| *Table F-2. IBM Network Station Desktop Manager Default Settings* | |
|---|---|
| **Desktop Manager Default Settings** | |
| **Item:** | **Default Value:** |
| Screen colors: | Mint green |
| Background color for window frame in focus | Gray |
| Background color for window frame not in focus | Black |
| Foreground color for window frame not in focus | |
| Icon preferences: | on desktop |
| Icons placed | bottom left |
| Icon location | |
| Fonts: | 12 |
| Font size for icons and menus | |
| Window focus | Windows become active by clicking on the window |

| *Table F-3. 5250 Default Settings* | |
|---|---|
| **5250 Default Settings** | |
| **Item:** | **Default Value:** |
| Key remapping capability | Disabled |
| Default keyboard file for: | None |
| PC Keyboard (101 keys) | None |
| PC Keyboard (102 keys) | None |
| 5250 Keyboard (122 keys) | |
| Color Settings: | Basic |
| Color customization capability | None |
| Default color scheme | None |
| Additional color schemes to make available | |
| Record/Playback Settings: | Enabled |
| Record/Playback capability | None |
| Playback sequences to make available | |
| Miscellaneous Settings: | 27 rows, 132 columns |
| Screen size | Disabled |
| Image/Fax display | Disabled |
| Column separators | No |
| Allow use of the pop-up keypad | Yes |
| Allow use of the control menu | Yes |
| Allow use of the edit menu | |

| *Table F-4. 3270 Default Settings* | |
|---|---|
| **3270 Default Settings** | |
| **Item:** | **Default Value:** |
| Key remapping capability | Disabled |
| Default keyboard file for: | None |
| PC Keyboard (101 keys) | None |
| PC Keyboard (102 keys) | |
| Color Settings: | Basic |
| Color customization capability | None |
| Default color scheme | None |
| Additional color schemes to make available | |
| Miscellaneous Settings: | 32 rows, 80 columns |
| Screen size | No |
| Allow use of keypad | No |
| Allow use of graphics | Control key |
| Key for Enter function | No |
| Use Auto Action | 23 |
| Telnet 3270 port to connect to | |

| *Table F-5. Internet Network Default Settings* | |
|---|---|
| **Internet Network Default Settings** | |
| **Item:** | **Default Value:** |
| Web server port on the boot host | 80 |
| Applet launcher port | 5555 |
| IBM Network Station browser version | Non-encrypted |
| Navio NC Navigator browser version | Non-encrypted |

*Table F-6. IBM Network Station Browser Defaults*

| **IBM Network Station Browser Defaults** | |
|---|---|
| **Item:** | **Default Value:** |
| Allow user to override settings | No |
| Security Settings:<br>Enable JavaScript<br>Enable Java Applets | Yes<br>Yes |
| Network Settings:<br>Disk cache<br>TCP/IP maximum connections | 5000 KB<br>5 |
| Print headers and footers:<br>Left header<br>Right header<br>Left footer<br>Right footer | &w<br>&p<br>&D<br>&t |
| Print margins:<br>Top margin<br>Bottom margin<br>Left margin<br>Right margin<br>Paper size | .5 inches<br>.5 inches<br>.5 inches<br>.5 inches<br>Letter |
| Miscellaneous:<br>Auto load images<br>Show toolbar | Yes<br>Yes |

*Table F-7. Java Applet Viewer Settings*

| **Java Applet Viewer Settings** | |
|---|---|
| **Item:** | **Default Value:** |
| Verbose mode | off |
| Verify classes | remote only |
| Maximum heap size | 3 MB |
| JAVA stack size | 256 KB |
| Native code stack size | 32 KB |
| Garbage collection:<br>Verbose<br>Only when needed | off<br>off (garbage collection runs as an asynchronous thread in parallel with other threads) |
| **NOTE**: The Java Applet Viewer setting defaults are also the defaults for the Java Applications found on the Startup Programs and Menus screens. | |

# Appendix G. IBM Network Station Manager Program Shipped Environment Variables

The following sections include the environment variables whose values cannot be altered for OS/390 and VM. These values are set when a user logs onto the IBM Network Station.

## Environment Variables for OS/390

**PATH**
/usr/lpp/tcpip/nstation/standard/mods

**HOME**
/etc/nstation/user/ *username*

**Note:** *username* is the identity of the person that is signed onto the IBM Network Station.

**DISPLAY**
:0.0

**HOSTNAME**
Name of the IBM Network Station terminal

**BOOTHOST**
The host from which the IBM Network Station was booted

**BOOTPATH**
/usr/lpp/tcpip/nstation/standard

**USER**
User ID of the person logged onto the IBM Network Station

**NSM_ADMIN_SYSDEFAULTS**
/usr/lpp/tcpip/nstation/standard/defaults

**NSM_PROD_SYSDEFAULTS**
/usr/lpp/tcpip/nstation/standard/SysDefaults

**NSM_USER_PREFS**
/etc/nstation/user/*username*/nsm

**Note:** *username* is the identity of the person that is signed onto the IBM Network Station.

## Environment Variables for VM

**PATH**
/QIBM/ProdData/NetworkStation/mods

**HOME**
/QIBM/UserData/NetworkStation/*username*

**Note:** *username* is the identity of the person that is signed onto the IBM Network Station.

**DISPLAY**
:0.0

**HOSTNAME**
Name of the IBM Network Station terminal

**BOOTHOST**
The host from which the IBM Network Station was booted

**BOOTPATH**
/QIBM/ProdData/NetworkStation

**USER**
User ID of the person logged onto the IBM Network Station

**NSM_ADMIN_SYSDEFAULTS**
/QIBM/UserData/NetworkStation/SysDefaults

**NSM_PROD_SYSDEFAULTS**
/QIBM/ProdData/NetworkStation/SysDefaults

**NSM_USER_PREFS**
/QIBM/UserData/NetworkStation/*username*

**Note:** *username* is the identity of the person that is signed onto the IBM Network Station.

# Index

## Numerics



## A



## B



## C



## D

## E



## H



## I



## J



## L

# Communicating Your Comments to IBM

Network Station Manager for S/390
To view or print the update, go to:http://www.as400.ibm.com/networkstation/s390

Publication No. SC31-8546-00

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

If you prefer to send comments by mail, use the RCF at the back of this book.

If you prefer to send comments by FAX, use this number:

USA and Canada: 1-800-277-5088

If you prefer to send comments electronically, use this network ID:

- USIB2HPD at IBMMAIL
- usib2hpd@vnet.ibm.com

Make sure to include the following in your note:

Title and publication number of this book
Page number or topic to which your comment applies.

# Readers' Comments — We'd Like to Hear from You

**Network Station Manager for S/390**
**To view or print the update, go to:http://www.as400.ibm.com/networkstation/s390**

**Publication No. SC31-8546-00**

**Overall, how satisfied are you with the information in this book?**

| | Very Satisfied | Satisfied | Neutral | Dissatisfied | Very Dissatisfied |
|---|---|---|---|---|---|
| Overall satisfaction | □ | □ | □ | □ | □ |

**How satisfied are you that the information in this book is:**

| | Very Satisfied | Satisfied | Neutral | Dissatisfied | Very Dissatisfied |
|---|---|---|---|---|---|
| Accurate | □ | □ | □ | □ | □ |
| Complete | □ | □ | □ | □ | □ |
| Easy to find | □ | □ | □ | □ | □ |
| Easy to understand | □ | □ | □ | □ | □ |
| Well organized | □ | □ | □ | □ | □ |
| Applicable to your tasks | □ | □ | □ | □ | □ |

**Please tell us how we can improve this book:**

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

**Readers' Comments — We'd Like to Hear from You**
SC31-8546-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

# BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM CORPORATION
ATTN DEPT CGMD
P.O. BOX 12195
Research Triangle Park, North Carolina 27709

Fold and Tape **Please do not staple** Fold and Tape

SC31-8546-00

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC31-8546-00

*Spine information:*

Network Station Manager for S/390

*To view or print the update, go to:http://www.as400.ibm.com/networkstation/s390*