Netra j 3.0 Administrator's Guide

THE NETWORK IS THE COMPUTER™

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900 USA
650 960-1300
Fax 650 969-9131

Part No.: 805-5363-10
September 1998, Revision A

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" SANS GARANTIE D'AUCUNE SORTE, NI EXPRESSE NI IMPLICITE, Y COMPRIS, ET SANS QUE CETTE LISTE NE SOIT LIMITATIVE, DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DES PRODUITS A REPONDRE A UNE UTILISATION PARTICULIERE OU LE FAIT QU'ILS NE SOIENT PAS CONTREFAISANTS DE PRODUITS DE TIERS.

Contents

Preface

The *Netra j 3.0 Administrator's Guide* is for system administrators who are using the Netra™ j 3.0 software to set up and configure network computing infrastructures. It describes how to set up and configure network computer (NC) clients in a network environment. It explains how to use the Netra j administration interface, a graphical user interface (GUI), to administer the system.

This preface includes the following topics:

- "Before You Read This Book" on page xxi
- "How This Book Is Organized" on page xxii
- "Using UNIX Commands" on page xxii
- "Typographic Conventions" on page xxiv
- "Shell Prompts" on page xxiv
- "Related Documentation" on page xxv
- "Recommended Reading" on page xxvi
- "Sun Documentation on the Web" on page xxvii
- "Sun Welcomes Your Comments" on page xxvii

Before You Read This Book

You should install the Netra j 3.0 software before using this guide. Refer to the *Netra j 3.0 Installation Guide* for installation and initial configuration instructions. You can install Netra j from a CD or from an Electronic Commerce web site (follow links from http://www.sun.com/netra-j).

After installing Netra j, complete the Network Computer Configuration Form in Appendix A to prepare to configure your network environment with NCs.

How This Book Is Organized

The information in this manual is organized as follows:

Chapter 1 introduces the Netra j 3.0 software.

Chapter 2 describes the minimal configuration to set up and configure an NC network environment.

Chapter 3 describes anonymous FTP, Mail, and Name Service administration.

Chapter 4 describes the software that is available for remote windowing and legacy connectivity.

Chapter 5 describes the NC diagnostic tools.

Chapter 6 describes the network printing services.

Chapter 7 describes LAN, modem, routing, and ATM administration modules.

Chapter 8 describes the Security Administration.

Chapter 9 describes the System Administration (log files, user accounts, adding patches, etc.) modules.

Chapter 10 describes the Proxy Cache modules.

Appendix A provides a form to help you gather information you need to set up and configure NCs.

Appendix B provides reference information about proxy cache.

Appendix C describes the packages included in Netra j software.

Appendix D provides common and known troubleshooting instructions.

Appendix E describes the various page types used by Netra j.

Using UNIX Commands

Netra j 3.0 can be used in conjunction with any Solaris administration tools or UNIX® commands and procedures. However, this document does not contain information on basic UNIX commands and procedures such as shutting down the system, booting the system, and configuring devices.

See the following for this information:

- AnswerBook™ online documentation for the Solaris™ 2.5.1 or 2.6 software environment
- Other software documentation that you received with your system

Typographic Conventions

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output.	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail`.

`AaBbCc123`	What you type, when contrasted with on-screen computer output.	`%` **`su`**
		`Password:`

AaBbCc123	Book titles, new words or terms, words to be emphasized. Command-line variable; replace with a real name or value.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be `root` to do this. To delete a file, type `rm` *filename*.

Shell Prompts

TABLE P-2 Shell Prompts

Shell	Prompt
C shell	*machine_name*%
C shell superuser	*machine_name*#
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell superuser	#

Related Documentation

TABLE P-3 Related Documentation

Application	Title or Product	Part Number/Location
Product Information	*Netra j 3.0 Product Notes*	805-5361, `http://docs.sun.com`
Installation	*Netra j 3.0 Installation Guide*	805-5364, `http://docs.sun.com`, Netra j Main Administration page
	Sun Binary Code License Agreement	804-1722
JavaStation™ Administration	*JavaStation Client Software Guide*	805-5890 `http://docs.sun.com`
Administration	Netra j 3.0 online help	Included with Netra j software
	HotJava™ Views™ Administration online help	Included with Netra j software
	Solaris 2.6 System Administrator Collection Volume 1 • *Solaris Naming Administration Guide (2.5.1)* • *Solaris Naming Setup and Configuration Guide (2.6)*	`http://docs.sun.com`
	Solaris 2.6 System Administrator Collection Volume 2	`http://docs.sun.com`

TABLE P-3 Related Documentation *(Continued)*

Application	Title or Product	Part Number/Location
Other Included Software	HotJava™ Browser	Refer to the online help.
	HotJava Views	Refer to the online help.
	OpenConnect Systems' OpenVista™ and OC://WebConnect Pro™	OC://WebConnect Pro online help; *Netra j 3.0 Administrator's Guide*
	Sun™ WebServer™	Refer to the online help.
	Sun™ Internet Mail Server™	`http://www.sun.com/sims/tech-stuff`
	GO-Joe With RapidX	`README` file included with the GO-Joe software; *Netra j 3.0 Administrator's Guide*; `http:/www.graphon.com`
	Citrix Systems' WinFrame or MetaFrame	`http://www.sun.com/desktop/products/PCCP/remotewindowing/citrix`

Recommended Reading

For more information, refer to the documents listed in the following table.

TABLE P-4 Recommended Reading

Topic	Document	Location
DHCP	• *TCP/IP Data Communication Administration Guide*	*Solaris 2.6 System Administrator Collection Volume 1*, located at `http://docs.sun.com`
	• man pages on `dhcp(4)`, `dhcptab(4)`, `dhcpconfig(1M)`, `dhtadm(1M)`, and `pntadm(1M)`	

TABLE P-4 Recommended Reading *(Continued)*

Topic	Document	Location
DNS	• *DNS and BIND, 2nd Edition*, by Albitz and Liu, O'Reilly	
	• *Solaris Naming Administration Guide* • *Solaris Naming Setup and Configuration Guide*	*Solaris 2.6 System Administrator Collection Volume 1*, located at `http://docs.sun.com`
NFS	• *NFS Administration Guide* • *Managing NFS and NIS*, Stern, OReilly	*Solaris 2.6 System Administrator Collection Volume 1*, located at `http://docs.sun.com`
NIS	• *Naming Services Transition Kit 1.2 Administrator's Guide* • *Solaris Naming Administration Guide (2.5.1)* • *Solaris Naming Setup and Configuration Guide (2.6)*	*NISKit 1.2 AnswerBook*, located at `http://docs.sun.com`

Sun Documentation on the Web

The `docs.sun.comSM` web site enables you to access Sun technical documentation on the Web. You can browse the `docs.sun.com` archive or search for a specific book title or subject at:

`http://docs.sun.com`

Sun Welcomes Your Comments

We are interested in improving our documentation and welcome your comments and suggestions. You can email your comments to us at:

smcc-docs@sun.com

Please include the part number of your document in the subject line of your email. For online documents, also list product and related screen.

CHAPTER 1

Product Description

This chapter describes the software packages, the Netra j administration interface, and how to access the interface. The chapter is organized as follows:

- "Netra j 3.0 Software" on page 29
- "Network Computers Supported" on page 31
- "Netra j Administration Interface" on page 32
- "Network Computing Environment" on page 31
- "Accessing the Netra Administration Interface" on page 32
- "To Access Netra j Documents" on page 35

For information on planning a network computer environment, see the *JavaStation Client Software Guide*.

Netra j 3.0 Software

Netra j 3.0 is a software-only Solaris application for booting and administering network computers (NCs). Netra j software includes NC client software, secure 3270/5250 web-to-host connectivity for any Java-enabled client, and browser-based management of complex network services such as DNS, NIS, and DHCP.

Netra j software can be added to new or existing SPARC™ systems running the Solaris 2.5.1 or 2.6 operating environment. There are some Solaris add-ons required to support NC systems. These are included in the Netra j software.

The Netra j 3.0 software is a graphical user interface (GUI) used to administer the NC network. Command-line administration is also supported, but it is not documented in this guide. For command-line administration, the see the *JavaStation Client Software Guide*.

The Netra j software includes several software packages that are required to set up and configure the network computing environment. The software packages include:

- Netra j administration software
- Network computer software
- Solaris 2.5.1 add-ons
- Open Connect Systems (OCS) software (3.2.4.1)

Netra j Administration Software

The Netra j administration software enables you to set up and configure the servers and clients needed in your network environment. It also contains the following additional software:

Sun WebServer 1.0 – Enables companies to publish and distribute information and deploy web-based applications across any network environment.

GO-Joe (2.01) – A thin client Java X server from GraphOn that provides access to all Solaris X Window applications.

Network Computer Software

These software packages provide the operating system, boot images, and client applications for the NC:

- JavaOS™ 1.1.1
- HotJava Views 1.1.3
- HotJava Views Demo Support
- HotJava Views Documentation
- HotJava Browser (server) 1.1.2
- HotJava Browser (client) 1.1.4

Solaris 2.5.1 Add-ons

Netra j also includes the following Solaris 2.5.1 add-on software packages. These packages are required to support NC clients on systems running the Solaris 2.5.1 operating environment.

- Sun Internet Mail Server
- PPP/IP asynchronous PPP daemon
- Networking UUCP utilities
- System localization
- PPP/IP and IP dialup
- X Windows optional fonts
- NIS Kit 1.2
- Dynamic Host Configuration Protocol (DHCP)

- Sun WebServer 1.0

OCS Software

Open Connect Software (OCS) provides a development tool to create applets for SNA/AS400 legacy systems, and software for enabling legacy connectivity to mainframes, AS400, and VT220 hosts. The following OCS software is included with Netra j:

- Netra j OpenVista 1.0
- OC://WebConnect™ 3.2.4.1

Network Computers Supported

The Netra j software supports a number of NCs.

- JavaStationq™ – Brick model
- JavaStation – Tower model (flash memory)
- Java Engine 1
- JavaPC™

Network Computing Environment

Unlike traditional workstations and PCs, NCs download all their software from a server. To run properly, these clients require a boot server, a domain name service (DNS) server, a network information service (NIS) server, an NFS™ server, a web server, a DHCP server, and a home directory for each user.

NCs can be integrated into an existing network.

The boot server "listens" on the network for a NC booting up and supplies the NC with its boot image (JavaOS) and a main application (usually either the HotJava Browser or HotJava Views). In Netra j Administration, you select which application a particular NC runs.

The Netra j software sets up a basic Netra j server, which includes a boot server with DHCP, TFTP, NFS, and web services. The DNS server and NIS server can be on the Netra j server or on other machines in the network.

Netra j Administration Interface

The Netra j software uses a web-based interface for its administration. A browser running on a client or on the Netra server accesses this interface.

Each administration function in the Netra interface is called a *module*. Each module comprises a set of related tasks. For example, the User Accounts module contains tasks to add user accounts, modify them, or delete them.

These administrative modules are grouped in five categories. The modules are displayed as hypertext links on the main administration page of the user interface. Clicking a link takes you to the module associated with the task.

This book provides system administration information for the Netra j administration interface (web-based administration). It describes the GUI and how to use it to perform administration tasks. The GUI is organized as follows:

- Network Computer Administration
  - "Network Computer Server" on page 37
  - "Network Computer Application Management" on page 57
  - "Monitoring and Debugging Tools" on page 109
- Network Services Administration
  - "Using Network Services" on page 65
  - "Mail Administration" on page 66
  - "Name Service Administration" on page 72
  - "Printer Administration" on page 115
  - "Using Proxy Cache Services" on page 175
  - "Sun WebServer Administration" on page 89
- "Using Network Connection Administration" on page 125
- "Using Security Administration" on page 149
- "Using System Administration" on page 153

For JavaStation specific command-line administration see the *JavaStation Client Software Guide.*

Accessing the Netra Administration Interface

As part of installation, Netra j creates a Solaris user account called `setup` that automatically launches HotJava Browser.

When you login to the Netra j server as userid: setup; password: setup, the Hot Java Bowser provided with Netra j starts up. Login to Netra j Administration as userid: setup; password: setup.

If you login to the Netra j server with any other userid or password, start a browser and use the URL `http://`*hostname*`:81`, to access the Netra j Administration. Login to Netra j Administration as userid: setup; password: setup.

You can login to the Netra j Administration from any computer on the network that has access to the Netra j server. Start a browser and use the URL `http://`*hostname.domainname*`:81.` Login to Netra j Administration as userid: setup; password: setup.

Note – The HotJava Views Administration pages require the HotJava Browser (HJB) provided with the Netra j software. All other Netra j Administration pages can be accessed with any other industry-standard browser. The path to the HJB is `/opt/SUNWnhjb/bin/hotjava`.

You access the web-based Netra administration interface through a dedicated administration web server using one of the following methods.

▼ To Use a Netra Server from the System Console

1. **At the console prompt, log in as the user** `setup` **and type** `setup` **for the password.**

```
% setup
Password:
```

A windowing system and a browser are started. The browser is configured to access the Netra administration framework. A popup dialog box prompts you to enter Netra j administration user name and password.

2. **Type** `setup` **for the user name and** `setup` **for the password to authenticate the browser connection.**

The Netra Welcome page is displayed.

3. **Click Administration.**

If this is the first time you are accessing Netra j, the Initial Configuration page is displayed (see *Netra j 3.0 Installation Guide* for details). Otherwise, the Main Administration page is displayed.

Note – Netra j provides arrows as configuration guides to help you. Please use them in preference over the browser buttons.

▼ To Access the Netra Server from an Other Computer on the Network

1. **Start a browser on another computer system.**
2. **Open the following URL:**

```
http://hostname.domainname:81
```

Where *hostname* is the Netra j hostname and the *domainname* is the name of the domain in which the Netra j server resides.

The Netra password screen is displayed.

3. **Type** `setup` **for the user ID and** `setup` **for the password.**

   The Netra Welcome page is displayed.

4. **Click Administration.**

   If this is the first time you are accessing Netra j, the Initial Configuration page is displayed. Otherwise, the Main Administration page is displayed.

Note – See Appendix E for examples and descriptions of page types and icons.

▼ To View or Modify Properties in Netra j

1. **From the Main Administration page, click the link for the category in which a property resides.**

   In some cases, you have to follow several links.

2. **In the page for that category, view or make changes to the value of a property.**

   Most properties have editable fields. A few have toggles (either one value or another) or pulldown menus.

3. **At the bottom of the category page, click OK.**

   A page is displayed indicating the success or failure of your change. If a change fails, the page is redisplayed with the error indicated. Correct the error and click OK again. With some errors, a new page containing just an error message is displayed. If this occurs, click the back button on your browser to return to the category page.

   If you click Reset, the values for the properties on a page revert to what they were when you first loaded the page.

4. **After a successful change, click the up arrow icon to return to the page at the beginning of the module.**

   Alternatively, you can click the home icon to return to the Netra j Main Administration page.

▼ To Access Netra j Documents

1. **From the Main Administration page, under "Documentation," click Online Documentation.**

   The Documentation page is displayed, listing the languages available for the documentation.

2. **Click on the desired language, then click on the document title to view it.**

   The document is displayed.

Note – Before starting to configure your network complete the Network Computer Configuration Form in Appendix A.

The remainder of this guide is a description of the procedures used to configure Netra j services, broken down by the categories reflected in the links on the Main Administration page.

CHAPTER 2

Network Computer Server

This chapter describes how to configure NCs in your network. The first step in NC configuration involves setting up certain global parameter values that apply to all the NCs in your network. The next step is to set up parameters that are specific to individual NCs; these values override the global values for that NC.

If your network already provides network information service (NIS) and domain name system (DNS), Netra j automatically obtains the information it needs from the system files. You can verify this information by clicking Name Service on the Netra j Main Administration page and following the relevant links. If your system does not have name services, you need to set them up now. See “Name Service Administration” on page 72 for instructions.

This chapter also describes how to modify or delete the configured NC.

If you do not have global parameters and individual NCs configured, then you are guided through the configuration steps (follow the arrows).

This chapter is organized as follows:

Initial Configuration of the NC Server

This section describes the walk-through sequence to configure NCs. You have to follow the walk-through usually after a fresh installation of the Netra j software, or when the Netra j administration interface needs required information to configure NCs.

Note – Before starting to configure your network complete the Network Computer Configuration Form in Appendix A.

▼ To Configure the NC Server

1. **On the Main Administration page, under "Network Computer Administration" click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Click Set Web Server Document Root.**

   The Modify Web Server Document Root page is displayed. See "Web Server Document Root Administration" on page 39 for more information.

3. **Enter full path name of your web server document root, then click OK.**

4. **Click the forward arrow on the Operation Successful page.**

   The Network Computer Configuration page is displayed.

5. **Click Configure Global Parameters.**

   The Modify Global Parameters page is displayed. See "To Configure or Modify Global Parameters" on page 41 for more information.

6. **Enter Global Parameter information, then click OK.**

7. **Click the forward arrow on the Operation Successful page.**

   The Network Computer Configuration page is displayed.

8. **Choose one of the following:**

   - Add Single Network Computer
   - Add Multiple Network Computers

   See "Setting Up Network Computer Clients" on page 49 for more information.

9. **Click OK.**

   This completes the guided initial configuration.

10. **Return to the Main Administration page. Under "Network Service Administration" click Name Service.**

    The Name Service Administration page is displayed.

11. **Check the DNS server and client configurations. Configure them as appropriate.**

    Netra j software checks for an already configured DNS server on the network and automatically uses it. You need to check if the server configuration is the one you want. You always need to configure the Netra j server as a DNS client. See "Configuring the DNS Server" on page 79 and "Configuring the DNS Client" on page 88 for more information.

12. **To save your configuration, on the Main Administration page, under "System Administration," click Save and Restore Configuration.**

    The Save and Restore Configuration Administration page is displayed. See "Save and Restore Configuration" on page 163 for detailed information.

Network Computer Configuration

Note – Before starting to configure your network complete the Network Computer Configuration Form in Appendix A.

Web Server Document Root Administration

The web server document root is the root directory of the web server running on your system. The documents under this root are accessible to any system connected to the web server (provided the user has permissions). If a file is not under this root directory, then it cannot be accessed through the web server. Netra j requires the document root information to set up the default applications for the client.

By default, Netra j sets up HotJava Views and HotJava Browser as main application options available through the Network Computer Application Management module. NCs can access these applications by either mounting to the respective application directory or by specifying a URL. Through d`ocument root`, Netra j creates a link to HotJava Views or HotJava Browser. Netra j also sets up the `dhcptab` entries in `document root` so that the file names can be used in `dhcptab.`

Note – Netra j does not allow you to add a new main application or an NC without setting up `document root`.

You need to know the document root of the default web server. If you did not have a default web server configured on port 80 before the Netra j installation, then the Netra j installation process installs the Sun WebServer and configures it as your default web server at port 80. The default `document root` for Sun WebServer on `port 80` is `/var/http/demo/public.`

If you copy the file `spec.html` under the root directory, then any user can access this file using the URL `http://`*hostname.domain*`/specs.html`.

▼ To Modify Web Server Document Root

1. **From the Main Administration page, under "Network Computer Administration" click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Modify Web Server Documentation Root.**

   The Modify Web Server Document Root page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 2-1 Web Server Parameters

Parameter	Description
Full Path Name of the Document Root	Enter the absolute path of the `document root` for the default web server. For example, if Sun WebServer is running on `port 80`, then refer to the file `/etc/http/httpd.conf` and find the keyword `doc-root`. The default `document root` for Sun WebServer is `/var/http/demo/public`. If Netscape web server is running on port 80, then refer to the file `/usr/local/netscape/nse-home/https-ServerName/config/obj.conf` and find the keyword `document root.`

Defining Boot Server Global Parameters

TABLE 2-2 describes the global parameters you can configure through the Netra j GUI. Some of the parameters listed in the table are considered basic whereas others can be configured using the advanced global parameters forms.

Optional parameters have the phrase (optional) mentioned after them. Other parameters are required.

If your server is already on the network and is properly configured, Netra j obtains most of the global parameters automatically. To verify this information or to make any changes, refer to the appropriate modules for instructions.

You can modify the global parameters that are used by the boot server for all NCs. The global parameters are described in TABLE 2-2.

▼ To Configure or Modify Global Parameters

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Configure (or Modify) Global Parameters.**

   The Configure (or Modify) Global Parameters page is displayed.

3. **Complete or modify the form using the information in following table.**

TABLE 2-2 Network Computer Global Parameters

Parameter	Description
NIS Domain Name (optional)	The name of the NIS domain in which the NCs reside.
NIS Server Address(es) (optional)	The list of host address(es) of NIS or servers for the NCs. A list of NIS server addresses configured in the NC server database is displayed.
DNS Domain Name	The name of the DNS domain in which the NCs reside.
DNS Server Address(es)	The host address of the DNS server(s) for the NCs.
Boot Server Address	The host address of the NC boot server on the local network.
Time Server Address	The IP address of a server supporting the network time protocol (NTP).
Router Address(es) (optional)	A list of host address(es) of the routers to be used by the NCs. If not given, JavaOS broadcasts looking for a router. A list of router addresses configured in the NC server database is displayed.

TABLE 2-2 Network Computer Global Parameters *(Continued)*

Parameter	**Description**
Lease Time (in days)	The duration (in days) of the IP address lease to the NC client. By default, this field is set to 3 days. After this period of time, if an IP address lease is not renewed, the NC shuts down its network interface. A value of -1 specifies an infinite (permanent) lease.
Lease Negotiation	A “Yes” or “No” flag indicating whether lease negotiation is to be performed. If the lease time is set to the value “infinite” (-1), "Yes" has no meaning.
Network Interfaces	An access point to a system on a network. Each interface is associated with one physical device (however, a physical device can have multiple network interfaces).
Time Zone	Specifies the time zone in which the NC clients are located. This 3-letter field defaults to the time zone specified in the NC server database.

▼ To Unconfigure Global Parameters

1. **From the Main Administration page, under “Network Computer Administration,” click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under “Global Network Computer Management,” click Unconfigure Global Parameters.**

   The Unconfigure Global Parameters page is displayed.

3. **Click OK.**

Advanced Global Parameters

- To Modify Localization Properties
- To Modify Network Services Properties
- To Modify Printing Properties
- To Modify Video Resolution Properties
- To Modify General Properties
- To Enter JavaOS Command Line
- To Modify network parameters for all network computers on one network interface

▼ To Modify Localization Properties

1. **On the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Modify Advanced Global Parameters.**

   The Advanced Global Parameters page is displayed.

3. **Click Modify Localization Properties.**

4. **Complete the form using the information in the following table:**

TABLE 2-3 Localization Properties

Option	Description
Input Method Server	A server with a language engine to interpret the keyboard input method (for example, Korean, Chinese, and Japanese languages). This server must be running a localized version of Solaris.
Input Method Port	The port number of the Input Method (IIIMP) server for the NC. The IIIMP port number configured in the NC server database is displayed. For example, this is for Asian locales.
Fonts Server	The host address or host name of the fonts server for the NCs. The default is the font server configured in the NC server database. This field is required if the fonts directory is specified. For example, this is required for Asian locales.
Fonts Directory	The directory location on the fonts server of the fonts for the NCs. If a fonts server is specified, a fonts directory is required.
Localized Resources Server	The host address or host name of the localized resources server for the NCs. This field is required if the localized resources directory is specified.
Localized Resources Directory	The directory location on the localized resource server of the localized resources for the NCs. If a localized resources server is specified, this directory is required.
Login Locales List	The list of locales to be presented as choices to the user logging on to an NC. By default, none is specified.

Note – See the *JavaStation Client Software Guide* for more information. See "Setting Up Network Computer Clients" on page 49 for keyboard selection.

▼ To Modify Network Services Properties

1. **On the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Modify Advanced Global Parameters.**

   The Advanced Global Parameters page is displayed.

3. **Click Modify Network Services Properties.**

   The JavaOS Network Service Properties page is displayed.

4. **Complete the form using the information in the following table:**

TABLE 2-4 JavaOS Network Services Properties

Options	Descriptions
Use DNS Protocol	When set to true, host name-to-address and address-to-host name resolution is performed using the DNS protocol. See also javaos.nis. If lookup using NIS is enabled also, NIS is attempted first, and DNS is attempted only if NIS lookup fails. See also javaos.hostaddrmap and javaos.hostnamemap.
Use NIS Protocol	When set to true, login authentication, host name-to-address resolution and address-to-host name resolution are performed using the NIS protocol. See also javaos.dns. If lookup using DNS is also enable, NIS is attempted first, and DNS is attempted only if NIS fails.
NIS hostname-to-address Map Name	The name of the NIS map used to perform host name-to-address resolution.
NIS address-to-hostname Map Name	The name of the NIS map used to perform address-to-host name resolution.
NIS Home Directory Map Name	If NIS is enabled, this property is used to set the name of the NIS map used by JavaOS to determine a user's home directory.

▼ To Modify Printing Properties

1. **On the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Modify Advanced Global Parameters.**

   The Advanced Global Parameters page is displayed.

3. **Click Modify Printing Properties.**

4. **Complete the form using the information in the following table:**

TABLE 2-5 JavaOS Printing Properties

options	Descriptions
NIS Map used to locate printers	The name of the NIS map used to locate printers.
LPD Printers	A semicolon-separated list of printers available for use by the lpd printing client. The format of each entry is printer@server.
Printers available from this host	A semicolon-separated list of the printers available from this host. This property enables administrators to add access to the printer nearest a given NC. The syntax of the printer name is the print service name, a colon, and the full name used by the print service to identify the printer. Example:djavaos.printdialog.always ShowPrinters=lpd:raw@konaprint;lpd:ps@konaprint;NIS:droid@fred
Printers to list in print dialogs	A semicolon-separated list of the printers the user has selected to appear in print dialogs. The format is the same as for alwaysShowPrinters. This is a system property. Example: -Djavaos.printers.selected

▼ To Modify Video Resolution Properties

1. **On the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Modify Advanced Global Parameters.**

   The Advanced Global Parameters page is displayed.

3. **Click Modify Video Resolution Properties.**

4. **Complete the form using the information in the following table.**

   This sets the Frame Buffer Resolution Dimensions, which Specifies a new frame buffer resolution to be set at boot time. The syntax of resolution parameters is widthxheightxdepth@vfreq, where depth is optional. Currently only 8 bit depth is supported. For example, -djavaos.fbDimensions=800x600x 8@60

TABLE 2-6 JavaOS Video Resolution Properties

Option	Description
Frame Buffer Resolution Prompt	If set to true, and if javaos.fbDimensions is specified, the user is prompted by a Video Mode Confirmation dialog. If the user selects OK, the video mode is set to the newly specified mode. The user must then accept the new video mode by selecting YES. If they fail to select YES within a ten second period or if they select NO, the video mode reverts to its original default.
Frame Buffer Width	Width component of frame buffer resolution (specified in pixels).
Frame Buffer Height	Height component of frame buffer resolution (specified in pixels).
Frame Buffer Depth (optional)	Depth component of frame buffer resolution (specified in bits).
Frame Buffer Frequency	Refresh Frequency component of frame buffer resolution (specified in hertz).

▼ To Modify General Properties

1. **On the Main Administration page, under “Network Computer Administration,” click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under “Global Network Computer Management,” click Modify Advanced Global Parameters.**

   The Advanced Global Parameters page is displayed.

3. **Click Modify General Properties.**

4. **Complete the form using the information in the following table:**

TABLE 2-7 JavaOS General Properties

Option	Description
JavaStation Console Hotkey	This property sets the keyboard hotkey that activates the JavaStation console, which displays debugging information. The value of the property is the JDK™ virtual keycode name for the hotkey. The following codes are valid: • VK_F1 • VK_F2 • VK_F3 • VK_F4 • VK_F5 • VK_F6 • VK_F7 • VK_F8 • VK_F9 • VK_F10 • VK_F11 • VK_F12 • VK_PRINTSCREEN • VK_UNDEFINED (to disable the console) The value of this property is case-insensitive; VK_PRINTSCREEN and vk_PrInTSCreen are equivalent. The default value is VK_PRINTSCREEN.
Login Screen	If true, JavaOS displays a login screen after booting and before starting the initial application. If false, JavaOS runs the main application as soon as it boots, without displaying a login screen. This means there is no user home directory, and no system properties are read from a properties file. If you want, you can use the javaos.homedir property to specify an NFS directory to mount (see below).
Always Update Flash Memory	This property specifies that JavaOS is always or never updated in the JavaStation's flash memory, regardless of the value of the JavaOS checksum. It is useful for public kiosks or other systems where user input is not expected. • If not set, the default behavior occurs: if the DHCP-supplied checksum is present and is not zero and does not match the checksum stored in flash, then an Update Flash dialog is displayed. • If set to true, then if the above conditions hold, no dialog is displayed and flash is updated. • If set to any value other than true, then regardless of checksum presence/value, flash is not updated. Note that if the DHCP checksum is not present or is zero, the flash is not updated.

TABLE 2-7 JavaOS General Properties *(Continued)*

Option	Description
Allow Guest Login	If true, the login screen (if displayed at all) contains a guest login button.
Home Server	Name of the server where the Home Directory is stored.
Home Directory	This property specifies the NFS path JavaOS should mount if NFS is not used to find the path based on the user name. The NFS path is specified as hostname:/ path. This property is most often used to determine the directory to use for the properties file that is read by HotJava Browser at start-up. If the javaos.login property is set to false, javaos.homedir is not used.

▼ To Enter JavaOS Command Line

Note – JavaOS commands can be entered here for all NCs (global); for a group of NCs, under Vendor Specific Options in Adding Multiple NCs; or for a single NC, under Vendor Specific Options in Adding Single NC, or To Modify a Network Computer. If the same parameter is entered globally and as a vendor specific option for an NC, the vendor specific option value of the parameter is used.

1. **On the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Modify Advanced Global Parameters.**

   The Advanced Global Parameters page is displayed.

3. **Click Enter JavaOS Command Line.**

   The JavaOS Command Line page is displayed.

4. **Enter the JavaOS command(s) you want delivered to the JavaOS during the boot sequence.**

   The JavaOS command line is a formatted text string containing definitions of either JavaOS or system properties. Property definitions are separated by a white space. Each property definition contains a flag, such as -d or -D, followed by the property_name=property_value. There is no white space between the flag and the property name. The JavaOS command line(s) are stored in a file that is included in the dhcptab. Thus there is no size limitation on the entry.

▼ To Modify network parameters for all network computers on one network interface

1. **On the Main Administration page, under “Network Computer Administration,” click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under “Global Network Computer Management,” click Modify Advanced Global Parameters.**

   The Advanced Global Parameters page is displayed.

3. **Click the network interface you want to modify.**

4. **Complete the form using the information in the following table:**

TABLE 2-8 Network Parameters

Option	Description
MTU Size (bytes)	The maximum transmission unit to be used by the NCs on this network.
Netmask	The netmask of the NCs.
Router Address(es) (optional)	The host address(es) of the routers to be used by the NCs. Host addresses are separated by one white space. If none are specified, JavaOS broadcasts looking for a router. By default this is set to the host address of the default system router (if configured in the system).
Enable Source Routing	This property enables or disables the source routing support in the Token-Ring driver on the NC. If this property is set to Yes, source routing support is enabled. If this property is set to No, source routing support is disabled.

Note – Modifying the global parameters on this form changes the default network parameters for all NCs connected to the Netra j server through the selected specific network interface.

Setting Up Network Computer Clients

You can add one NC at a time or you can very quickly add a group of NCs at one time.

- Adding multiple NCs
  - For adding groups of NC clients (with the same configuration) or setting up many NC clients at one time with identical configurations
  - IP addresses are assigned automatically (dynamic leasing)
  - IP addresses can be leased or permanent
- Adding a single NC
  - For adding individual NC clients
  - You can assign the IP address (static leasing) or choose dynamic leasing by leaving the MAC address blank
  - IP addresses can be assigned for a limited time lease or as a permanent lease

The two methods handle IP addressing differently. When you add multiple NCs, you are asked to specify a starting IP address and the number of NC clients you want to be configured. Netra j then assigns IP addresses to NC clients from this range of addresses. Also, addresses can be leased for a few days or can be assigned permanently.

On the other hand, if you add one NC, you have the option of assigning a unique IP address lease to the NC, and deciding whether that IP address belongs to the NC permanently or only for a few days.

Besides IP address, you can set some other NC specific parameters that override the corresponding global parameter values.

Once you have set up an NC, either individually or as part of a group, you can go back and modify its original parameters with the Modify function.

Adding Multiple NCs

You can use this method to set up many NCs with the same parameters. This module enables you to specify the starting IP address, the number of NCs, the lease time, the NC locale, keyboard, vendor-specific options and the default application for these clients.

Using this method works for NCs that only use DHCP for initial configuration. If your NC uses reverse address resolution protocol (RARP) for initial configuration, you need to assign the Ethernet address of the NC using either the Add single NC, or the Modify Network Computer menu. The Modify menu is only available after you have already added some NCs.

NCs added through this form use dynamic IP address leasing. This means that IP addresses are assigned on a first come first serve basis. The address is assigned for a few days (temporary lease) or forever (permanent lease) depending on the lease time value specified.

You can change NCs with dynamic leases to static leases by modifying them individually once they are added (use the Modify Network Computers option and insert an MAC (ethernet) address). Vendor specific options can also be changed on an individual basis.

▼ To Add Multiple NCs

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Network Computer Management," click Add Multiple Network Computers.**

   The Add Multiple Network Computers page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 2-9 Individual NC Specific Parameters

Parameter	Description
Host Name Prefix	The host name of any NC is generated using the `name_prefix`. If the IP address of the NC is aa.bb.cc.dd, then the generated host name for this computer is `name_prefix-dd`.
Starting IP Address	The initial host address you assign to the NCs being set up. If a host address is already used by some other system in the network, that address is skipped.
Number of NCs	The number of NCs to be set up. If an IP address is already used in the network, that address is not used. So the number of clients actually setup can be less than the number of NCs requested. Maximum number of NCs is 254.
Host Name	The name of a computer within the local domain. It is a text string of up to 24 characters composed of letters (a–z and A–Z), digits (0–9) and hyphens (-). The last character cannot be a hyphen. The first character must be alphabetic.
Host Address	An assigned number that uniquely identifies each computer connected to a TCP/IP network. The address consists of two parts: a network number and a host number. The network number identifies the network to which the computer is connected and the host number identifies the computer on that network. The host address is composed of four integers separated by periods. The first integer must be in the range 0–223, the second and third integers in the range 0–255 and the fourth integer in the range 1–254 (for example, 127.144.0.1).

TABLE 2-9 Individual NC Specific Parameters *(Continued)*

Ethernet Address	This address is a number that uniquely identifies each computer. It is built into the hardware of each computer and is displayed at boot time. The Ethernet address is composed of six hexadecimal numbers separated by colons; each number is in the range 0–ff. Upper- or lower-case letters can be used to specify non-decimal digits.
Enter Lease Time (days)	The duration (in days) of the IP address lease to the NC client. By default, this field is set to 3 days. After this period of time, if an IP address lease is not renewed, the NC shuts down its network interface. A value of -1 specifies an infinite (permanent) lease.
Default Application	The default application that runs on this computer. `views` specifies HotJava Views, `browser` specifies HotJava Browser, you can have none, or you can add other applications. To add other applications as options to the Default Application list use "Network Computer Application Management" on page 57. If you are using the JavaOS image with a statically linked HotJava Browser, you must set the Default Application to `browser`. Otherwise, the HotJava Browser fails to open on the NC.
Select NC Locale	The language the user plans to use with this NC. For Asian languages, input method and fonts need to be configured in global parameters. See "To Modify Localization Properties" on page 43 for more information. See the *JavaStation Client Software Guide* for a detailed description on this topic.
Select Keyboard	Select the keyboard for use with this NC. Currently, PS2 keyboards are supported
Vendor Specific Options (optional)	A formatted text string containing definitions of either JavaOS or system properties.The JavaOS command line is delivered to JavaOS during the boot sequence. It can be delivered by DHCP or other methods. There are no spaces between the option and the value. Different command line options are separated by a space. Exact syntax must be used to specify the command line options. By default, all JavaOS and system properties configured in the NC server database (using `JOScmd1`) are displayed. For example: If you do not want the `login` prompt for an application to be run on the NC, type `-djavaos.login=false`. See *JavaStation Client Software Guide* for additional information.

Adding Single NC

You can add one NC using this form. NCs added through this form use static leasing that means this NC always is assigned the same IP address either for a few days (temporary lease) or forever (permanent lease) depending on the lease time value specified.

▼ To Add an NC

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Network Computer Management," click Add Single Network Computer.**

   The Add A Network Computer page is displayed.

3. **Complete the form using the information in** TABLE 2-9**.**

▼ To List Network Computers

1. **From the Main Administration page, under "Network Computer Administration" click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Network Computer Management,“ click List.**

   A list of the NCs on your network is displayed.

▼ To Modify a Network Computer

1. **From the Main Administration page, under "Network Computer Administration" click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Network Computer Management,“ click Modify.**

   Select one NC, and make the changes in the form using TABLE 2-9 as a reference.

▼ To Delete a Network Computer

1. **From the Main Administration page, under "Network Computer Administration" click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Network Computer Management,“ click Delete.**

   Select one or more NCs, and click OK, then confirm the operation.

Network Computers – Local Printer Setup

You can use this form to configure a printer attached to the serial port of a specific NC. You need to set up the NC before setting up the local printer.

▼ To Set Up a Local Printer

1. **From the Main Administration page, under "Network Computer Administration" click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Network Computer Management,“ click Configure Local Printer for a Network Computer.**

   The Network Computer – Local Printer Setup window is displayed.

3. **Complete the form using the information in the following table.**

TABLE 2-10 Local Printer Setup Options

Option	Description
Select Network Computer	Choose the NC for this local printer setup.
Port	This property sets the communications parameters for the serial port. The port portion of this property is the name of a serial port which can be: • SerialA or SerialB for an onboard JavaStation serial port • One of SerialP1 - SerialP8 for a virtual serial port enabled by the multi-port serial card (MPSC).
Select Bit Rate	The bit rate of the serial port. The bit rate is the rate at which data is sent over a communication line. The default bit rate is 4800.
Number of Data Bits	The number of data bits. The default is 7.

TABLE 2-10 Local Printer Setup Options

Option	Description
Number of Stop Bits	The number of stop bits. Stop bits are extra "1" bits which follow the data and any parity bit. They mark the end of a unit of transmission (normally a byte or character). The default is 1.
Select Parity	The parity. An extra bit added to a byte or word to reveal errors in transmission. Even (odd) parity means that the parity bit is set so that there are an even (odd) number of one bits in the word, including the parity bit. The default is “no parity.”
Enter Handshake	The handshake identifier. A handshake is the exchange of predetermined signals between the NC and local printer to assure each that it is connected to the other (and not to an impostor). The default is hh.

Note – Peripherals other than printers can be added to NC ports. See the *JavaStation Client Software Guide* for more detail.

Example for Adding Groups of NCs

A small company just purchased fifteen NCs with a server. The company plans to have 10 English speaking accountants, 2 French speaking people responsible for operations, and 3 English speaking engineers. The accountants need to connect to a mainframe (OCS) and use HJV; the operations people need HJB; and the engineers need X-windows (GO-Joe). This is how the company set up its network.

First they set up the hardware and installed the Netra j software. Then they filled out the Network Computer Configuration Form in Appendix A.

The system administrator started a web browser on the server with URL servername:81 and logged in (setup, setup). For the initial configuration system defaults, the system administrator, chose CST and English (most users were English speaking). Next the system administrator selected the Sun WebServer as the default web server and set the web server document root.

Because this NC network was not added to an already existing network, there were no NIS or DNS servers. So the system administrator went to Name Service Administration and set up the Netra server as a caching (basic) DNS server, then as a client to itself.

After setting the document root and configuring global parameters, the system administrator selected adding multiple computers. This form was filled out for the ten NCs used by the accountants since that was the largest group. Prefix: acc, starting IP address: 125.144.35.101, Number of NCs: 10, Lease Time: 3, Default Application: views, NC locale: English, Keyboard: Canadian. The system administrator made the leasing dynamic.

The system administrator clicked on OCS; the number of licenses was correct, so the administrator finished the install, chose English as the language for the server, then filled in the configuration page: TN3270 gateway host: xxxxx, TN3270 gateway port:xx.

The system administrator added the remaining five NCs individually. The administrator assigned host addresses, so the leasing is static.

For the operations people:

Host name: ops1, ops2; MAC address: xxx,xxx; Host address: 125.144.35.111, 125.144.35.112; Lease time: -1 (indefinite or permanent lease); Default Application: browser; NC locale: French; Keyboard: Canadian French.

For the engineers:

Host Name: eng1,eng2,eng3;Mac address:ss,xxx,ddd; Host Address: 125.144.35.113, 125.144.35.114, 125.144.35.115; Lease time: -1;Default Application: views; NC locale: English, Keyboard: Canadian.

The system administrator went to Network Computer Application Management to add Go-Joe, an applet that runs in HotJava Views.

Updating Network Computer Operating System

Use this form to update the operating system if you have a new version of the `javaos` binary. If your NC has flash memory, the new binary is stored in flash memory, and is available for use when the NC is rebooted or powered on.

Flash memory enables the JavaStation to store the latest version of JavaOS locally in non-volatile memory. Flash memory enables the JavaStation to boot faster. Use the Update Network Computer Operating System module to reconfigure the existing network environment to the new `javaos` binary.

▼ To Update New `javaos` Binary

Note – You can only update flash memory in JavaStation client tower models.

---

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Server.**

   The Network Computer Configuration page is displayed.

2. **Under "Global Network Computer Management," click Update Network Computer Operating System.**

   The Update Network Computer Operating System window is displayed.

3. **Complete the form using the information in the following table.**

TABLE 2-11 Update NC Operating System Administration

Option	Description
Full path name of the new binary	The absolute path of the new JavaOS binary file.
Select client architecture	The selected architecture for this binary.

Note – If you are using the JavaOS image with a statically linked HotJava Browser, you must set the Default Application for the NCs to browser (see TABLE 2-9). Otherwise, HotJava Browser fails to open on the NCs.

Network Computer Application Management

This section describes how to add custom applications for the NC clients and how to administer HotJava Views(HJV). The applets that provide remote windowing tools (Citrix, GO-Joe, and OC://WebConnect) are added to HJV's selector through HJV's administration. If you intend to use the application version of Citrix, use the Client Application Administration.

In the *JavaStation Client Software Guide*, there are instructions for using an application loader, and using static linking (delivering an application with the JavaOS).

Client Application Administration

The client application is the user's desktop environment on the NC. In the Netra j administration interface, the current list of client applications includes HotJava Views and HotJava Browser. You can add additional applications to the list by using the Network Computer Application Management module.

The application must be a Java application. You cannot use applets as a main application on an NC.

To add a client application, you must know the main class for the application, the home property file, and the`.zip` file that contains all the classes.

Note – See the *JavaStation Client Software Guide* for instructions on creating your application archives.

▼ To Add a Client Application

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Application Management.**

   The Network Computer Application Management page is displayed.

2. **Under "Custom Client Application Administration," click Add a custom application.**

   The Add A Client Application page is displayed.

3. **Complete the form using the information in the following table**

TABLE 2-12 Client Application Administration

Option	Description
Application Name	The name of the application. This name is used in other places within the Netra administrative interface to refer to this application.
Main Class of the Application	The name of the main class where the Java application is defined. The client loads the main class to start the application.

TABLE 2-12 Client Application Administration *(Continued)*

Option	Description
Application Archive (Zip) Path	The archive (zip) file that contains all the classes. The client downloads the application before starting it. If you need to create a archive, see the *JavaStation Client Software Guide*.
Home Property of the Application	The value of this field depends on the application. Applications use different property names for the path to use for their home directory. This needs careful attention. The application needs this attribute to find its configuration files. For example, HotJava Browser uses `hotjava.home` and Marimba Tuner uses `tuner.home`.
Application Startup Options	The value of this field depends on the application. If the application has an option that can be provided while starting up, that option can be specified here. If the URL of the default web page is provided, HotJava Browser can come up with that URL.

4. **Click OK.**

▼ To Modify or Delete a Client Application

1. **From the Main Administration page, under "Network Computer Administration" click Network Computer Application Management.**

   The Network Computer Application Management page is displayed.

2. **Under "Custom Client Application Administration," under "Existing Custom Applications," choose one of the following:**

   - To modify a client application designation, click Modify, and make the changes in the form using TABLE 2-12 as a reference.
   - To delete a client application, click Delete then confirm the operation.

HotJava Views Administration

Note – Netra j automatically installs HotJava Views. If you are upgrading, you can lose groups you have configured, and application icons you have added to Selector, so copy the information elsewhere and replace it after the upgrade.

You can specify HotJava Views as the main application for NC clients. Netra j provides a link to the HotJava Views Administration tool that enables you to configure the HotJava Views application that deploys to NC clients. This section briefly describes HotJava Views administration. See HotJava Views Administration online help for complete information.

HotJava Views offers the following integrated components:

- *Selector* - An environment manager with a push-button interface for switching between applications.
- *MailView* - An IMAP4 mail client for composing, sending, and saving messages and handling a variety of attachments.
- *CalendarView* - A calendar client for managing personal and group calendars
- *NameView* - An enterprise name directory service client that retrieves and displays a configurable set of fields and enables contact via email, URLs, and calendar data
- *WebView* - An HTML 3.2-capable web browser (URL access can be restricted by the system administrator)

HotJava Views Model

HotJava Views enables the zero client-administration NC and also attempts to minimize server-side administration. Users are organized into groups in HotJava Views, and each group has its own profile, or set of properties.

Through HotJava Views Administration, you can define groups of users that share client properties, specify applications to appear in the Selector, specify any sliding panels that appear from the edges of the screen, administer other properties that affect the user's experience, and specify properties for particular NCs.

Selector refers to the vertical bar on the left side of the HotJava Views window where the applications buttons are located. It is easiest to think of Selector as being synonymous with HotJava Views itself. MailView, CalendarView and NameView are all applets that run within Selector, and their icons appear on the Selector bar.

When the NC client boots, a URL is passed to Selector. The URL points to the initial configuration file. Once Selector locates the web server, it loads HotJava Views' set of properties files.

Properties

HotJava Views is controlled by a set of eight properties files. There are property files at the group, user, and client levels.

- *Group properties* - Each user is normally a member of a group and inherits the group properties. Group properties are usually the main source of the final properties. Users who are not members of a group inherit the group properties of the group currently designated as the "default" group. There are both initial and final group property files.
- *User properties* - Stored in the user's home directory. Initial group properties are overridden by the user's individual property file. Note that user properties cannot be administered by this Web-based interface.
- *Client properties* - Client properties are specific to a given NC. They typically control a few items, such as the default printer, that are specific to the physical location of the NC.

Administering Views

The HotJava Views administration is conducted from within a web browser. There is a link from the Netra j 3.0 software to this set of web pages. The link points to a web page that offers the choice of configuring the HotJava Views client applications or configuring the back-end services (for example, NameView database).

See "To Access HotJava Views Administration" on page 62 for instructions on accessing the link to this administration tool.

Note – To access the HotJava Views Administration module, use the HotJava Browser provided with the Netra j software. All other Netra j administrative modules are supported by any industry-standard browser. The path to the HJB is `/opt/SUNWnhjb/bin/hotjava`.

Client-Side Administration

Upon selecting the HotJava Views client-side administration, a web page with an embedded applet is displayed. The applet contains the major tasks needed to configure HotJava Views client applications:

- *Overview* – Explanatory text that describes the overall flow of the administration applet. When first entering this applet, this button is highlighted and the overview text is displayed. This page also has some pointers to task-based help (how to configure a selector, how to configure drawers, and other tasks).
- *Application Palette* – To add and configure the global properties of the applications that can be used in the selector and drawers.
- *Groups & Configuration* – Configuring what users are in what groups and defining the selector applications, sliding panels, and application properties specific to each group.

- *Network Computer Props* – Properties that are specific to an NC hardware client, overriding properties set by the user or group. For example, you can have a public-use NC that uses the printers nearest to it, rather than the printers assigned by the group or user.

Server-Side Administration

Configuring the server-side application services includes properties associated with the back-end server that the client applications connect to. These applications include Welcome, WebView, MailView, CalendarView and NameView.

▼ To Access HotJava Views Administration

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Application Management.**

   The Network Computer Application Management page is displayed.

2. **Under "Netra Client Application Administration," click HotJava Views.**

   The HotJava Views Administration window is displayed.

3. **At the Main HotJava Views Administration page, on the HotJava Bowser menu click Edit —> Preferences —> Applet Security.**

4. **Set preferences to LOW for signed applets and MEDIUM for unsigned applets.**

   - Signed applets contain a signature (a sequence of data embedded in the applet's code) that protects the applet against tampering. It is placed in the code by the originator of the applet.
   - Unsigned applets do not have protection against tampering.

5. **Click Apply.**

6. **Refer to the HotJava Views Administration online help for information on how to use HotJava Views Administration.**

Adding an Application Icon to the HotJava Views Selector

At installation, the application properties are set in the `selector.apps` file located in `/opt/SUNWjdt/lib/props`. There are several `selector.desktop` files corresponding to their group located under `/opt/SUNWjdt/lib/props/`*group*`/selector.desktop`. You should add the application entry to the appropriate group's `selector.desktop` file.

Upon installation of the application, the icon and all associated properties are added to the HotJava Views application palette automatically.

See the HotJava Views Administration online help for additional information.

You should specify the server parameters before configuring the client. For Citrix' WinFrame and GraphOn's GO-Joe, you specify the server through the Network Computer Application Management module.

▼ To Add an Application Icon to the HotJava Views Selector

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Application Management.**

   The Network Computer Application Management page is displayed.

2. **Click HotJava Views.**

   The HotJava Views Administration page is displayed.

3. **Select Client-side Configuration —> Groups and Configuration.**

4. **Select the Group to which you want to add the application icon and click the Selector Applications button.**

5. **Choose the application entry in the Application Palette and click Add.**

   For example, GO-Joe and OC://WebConnect can be application entries.

6. **Click OK.**

7. **Click Set Default Group to set this group as default.**

   The default is Basic.HotJava Views Selector is now configured with the icon.

CHAPTER 3

Using Network Services

This chapter describes some of the Network Services Administration modules:

- “Anonymous FTP Administration” on page 65
- “Mail Administration” on page 66
- “Name Service Administration” on page 72
- “Sun WebServer Administration” on page 89

Anonymous FTP Administration

The Internet File Transfer Protocol (FTP) enables you to copy files from one computer to another over a network. You run an FTP client program on one computer and it connects to the FTP server program running on the other.

To use FTP, you must have a valid login account on the computer with the FTP server, unless the server is set up to accept *anonymous FTP*. An anonymous FTP server enables users without local accounts to access a specially designated FTP directory. From this directory, they can copy files to the computer running the FTP client ("downloading files"). Optionally, users can also be allowed to copy files into a subdirectory of the FTP directory ("uploading files").

The Anonymous FTP module enables you to configure your server in one of three states:

- *Anonymous FTP disabled (the default)*
- *Anonymous FTP enabled with download capability only*
- *Anonymous FTP enabled with upload and download capability*

By default, Netra j designates `/export/ftp` as the anonymous FTP directory. However, if you have installed Netra on top of an existing configuration, any changes you make to the anonymous FTP configuration preserve the current directory setup.

▼ To Configure Anonymous FTP

1. **From the Main Administration page, under "Network Service Administration," click Anonymous FTP.**

   The Anonymous FTP Administration page is displayed with the current state of the server.

2. **Complete the form using the information in the following table.**

   TABLE 3-1 Anonymous FTP Information

Option	Description
Enable anonymous FTP with upload and download capability	Users without accounts on the Netra server can connect to the Netra server using FTP. The anonymous FTP account has a directory called `/pub` that contains files available for downloading, and a directory called`/incoming` into which users can upload files.
Enable anonymous FTP with download capability only	Users without accounts on the Netra Server can connect to the Netra server using FTP. The anonymous FTP account has a directory called `/pub` that contains files available for downloading. Users cannot copy (upload) files into the directory `/incoming`.
Disable anonymous FTP	Only users with valid accounts on the Netra server can connect to it using FTP.

3. **Place all files that are to be available through FTP in the** `/export/ftp/pub` **directory (if you are using the default Netra setup).**

   Anonymous FTP users see this directory as `/pub`. If the server is configured with upload capability, anonymous users are able to copy files to the `/export/ftp/incoming` directory. FTP users see this directory as `/incoming`.

Mail Administration

This section describes how to use Mail Administration module.

If a server is configured to provide mail services, it becomes a mail server (a mail gateway between clients on the LAN and the Internet) and a mail host (incoming mail to users is available in the directory `/var/mail`). The Netra server runs both IMAP4 and POP3 daemons.

Note – The server can be a mailhost / mail server without being configured as such from Netra j. In that case, the module says “Netra mail services are inactive.” It says that about any configuration except one created by Netra i 3.2 or Netra j 2.0 or 2.0.1.

You can use Netra j to set the following aspects of the mail server configuration.

- The directory where the users' mailboxes are kept
- Whether this is shared (can be mounted on to other computers)
- The format of the return address on outgoing mail

The choices made when activating the mail services can be changed at a later time. If the Mail Administration page is loaded when Netra mail services are active, the following links: "Modify the mail services" and "Disable the Netra mail services configuration" are displayed. The first link shows the same form as for the initial configuration, while the latter link restores the mail services to the state they were in before Netra mail services were activated.

Mail Directories

The first choice concerns where users' incoming mail is kept. To users, the mailboxes appear to be in the directory `/var/mail`, but if space on the relevant disk partition is limited, you may prefer for `/var/mail` to be a link to another directory. Earlier versions of Netra (Netra j 1.0 or Netra i 3.1) linked `/var/mail` to `/export/mail`. The form shows whether `/var/mail` is currently linked to another directory, and gives the option of either keeping the mail in `/var/mail` or to link it.

If the location of the mailboxes changes, the mailboxes are moved to the new location from the current mail directory unless the `/var/mail` directory was mounted onto the Netra server from another server. In the latter case, the remote directory is unmounted without moving the mailboxes.

Directory Sharing

The second choice concerns whether the mailbox directory should be shared so that it can be mounted onto other computers. If the directory is to be shared, other computers can mount the Netra server's `/var/mail` directory so that it appears to be part of their own file system. (The directory `/var/mail` can be mounted as such even if it is actually linked to another directory.)

Mail Return Address Path Format

The third choice determines the format of the return address on outgoing mail, which can be either *user@host.domain* or *user@domain*. For example, suppose the Netra server's host name is `stimpy` and that `stimpy` resides in the domain `cartoon.net`. With the `user@host.domain` format, mail from the user `setup` goes out as from the sender `setup@stimpy.cartoon.net`, while with the *user@domain* format it is `setup@cartoon.net`.

The return address is used when people reply to messages sent out by the Netra server. For mail using the *user@domain* format to find its way back, the DNS server needs to know what server(s) deal with mail on the domain. This is accomplished by adding an MX record to the DNS database. If the Netra server is acting as the primary domain name server for the domain in which the server resides, this can be done through the Name Services module (See "Name Service Administration" on page 72). With reference to the example above, you would modify the domain `cartoon.net` by making an entry in the Mail Addresses/Preferences/Mail Servers box; in this case the mail address would be `cartoon.net`, the preference can be 5, and the mail server `stimpy.cartoon.net`.

▼ To Configure a Server to Provide Mail Services

1. **From the Main Administration page, under "Network Service Administration," click Mail, then click Configure this server as mailhost and a mailserver.**

   The Configure Mail Services Administration page is displayed.

2. **Complete the form using the information in the following table.**

TABLE 3-2 Mail Administration

Option	Description
Store Mail in `/var/mail`	Store mail in `/var/mail` directory
Link `/var/mail` to directory	Link `/var/mail` to the directory specified in the textbox and store the mail in that directory.

TABLE 3-2 Mail Administration *(Continued)*

Do you want the mail directory to be shared?	Determine whether other computers can mount the mailbox directory. Select yes or no.
Mail return address path format is: *user@host.domain*	The return address on mail includes the host name of the Netra server.
Mail return address path format is: *user@domain*	The return address on mail does not include the host name of the Netra server. For the mail format of *user@domain* to be used, the DNS primary server must have a mail exchanger record (MX record) for the Netra server in its database.

▼ To Modify Mail Services

1. **From the Main Administration page, under "Network Service Administration," click Mail, then click Modify the mail services.**

   The Modify Mail Services Administration page is displayed.

2. **Complete the form using the information in** TABLE 3-2**.**

▼ To Disable Netra Mail Services

1. **From the Main Administration page, under "Network Service Administration," click Mail, then click Unconfigure the mail services configuration.**

   The Unconfigure Mail Services Administration page is displayed.

2. **Click OK to confirm the operation.**

   This restores the mail configuration to what it was before being configured by Netra j.

Mail Alias Administration

The Netra Mail Administration module enables you to add and modify aliases that mail a copy of a message sent to the name to one or more users. Typically, such aliases are used to distribute messages to an interest group or to redirect a single users' mail, either because their mail should go to another server, or because they receive mail under an alternate name. Mail aliases that map names to a group of recipients are called as *mailing lists*, while mail aliases that map a name to a single user are called *alias names*.

In addition to creating new aliases, the mail administration module also allows you to modify two important system aliases: `root` and `postmaster.` These are standard names that people use for convenience: if you do not know who is in charge of a system, you use `root` to reach the systems administrator, and `postmaster` to reach the person who administers mail. Note that although `root` is a valid user, mail to `root` should always be redirected to a regular user (previous versions of the Netra software had a special form to administer the system administrator alias).

Mailing Lists

An example of how you might use a mailing list is to send messages to members of a volleyball team. You could create an alias with the name "vball" that has the email addresses of all the team members as the recipients. This way, mail sent to "vball" reaches the whole team without the sender needing to know the members' individual addresses (or even exactly who is on the team at any given point). When a member leaves or a new member joins, you update the alias.

Alias Names

Alias names redirect mail to single users. For instance, the user Tom Jones with user name "tom" may want to receive mail as "tjones". In this case, you would add an alias with the name "tjones" and the single recipient "tom." If John Smith, with user name "john," has left and wants to receive mail at his new address of jsmith at "otherdomain," add an alias that maps "john" to "jsmith@otherdomain."

▼ To Modify the System and Mail Administrator Aliases

1. **From the Main Administration page, under "Network Service Administration," click Mail.**

   The Mail Administration page is displayed.

2. **Click Modify either System Administrator alias or Mail Administrator alias.**

3. **Enter the mail addresses of the alias members (see the following table).**

TABLE 3-3 System Administrator Alias Administration

Option	Description
Alias Members	A list of people, one per line, who receive mail sent to `root` or `postmaster`. Each line must be a valid email address.

Note – If the Netra software has been installed onto a server that mounts `/var/mail` from a remote server, mail is handled by the remote server. This situation requires that the members of the administrator aliases are valid mail addresses on the remote server.

4. **Click OK.**

Configuring Aliases

▼ To Create a Mail Alias

1. **From the Main Administration page, under "Network Service Administration," click Mail, then click Add a mail alias.**

   The Add A Mail Alias page is displayed.

2. **Type the information in the form using the following table.**

TABLE 3-4 Information for Mail Alias Administration

Option	Description
Alias Name	The name of the mail alias. A copy of all mail sent to the alias is sent to each member of the alias. Alias names: • Must be at least one character and no more than 20 characters • Must begin with a letter, and can include letters, digits, hyphens, underscores, and periods • Are case insensitive • Must be unique
Alias Members	A list of people, one per line, who receive mail sent to the alias. Each line must be a valid email address. There is a limit on the size of the entry made to the system (the entries together with comma separators must not exceed 1000 characters). Netra issues a warning if your alias exceeds this limit. You can use nested aliases to circumvent this restriction.

Note – You can use Netra to administer only aliases whose member list is other users specified in the alias file. You cannot administer aliases that send mail to programs or to files.

▼ To Modify or Delete a Mail Alias

1. **From the Main Administration page, under "Network Service Administration," click Mail.**

   The Mail Administration page is displayed.

2. **Choose one of the following options:**
   - To modify an existing alias, click Modify for the required alias and make the changes in the form using TABLE 3-4.
   - To delete an alias, select an alias, click Delete to remove the alias, and then confirm the operation.

Mail Log File

Log files should be viewed and cleared periodically.

▼ To View or Clear the Mail Log

1. **From the Main Administration page, under "Network Service Administration," click Mail.**

   The Mail Administration page is displayed.

2. **Choose View or Clear the Mail log.**
   - Click View; the Mail Server Log File is displayed.
   - Click Clear, then confirm the operation to flush the file.

Name Service Administration

Every machine on a network must have a unique identifier to distinguish itself from other machines on the network. This is also true for all machines on the Internet. Thus, every machine is given a *host address*. This is also referred to as the IP address. A host address has the form 115.144.79.5, where each of the four numbers separated by periods can be in the range of 0 to 255. Such addresses are difficult to memorize, so each machine is also given a *host name* that is associated with its host address. Users generally use a host name, such as `stimpy.comedy.cartoon.net`, to access a specific machine on a given network.

The process by which a host name is associated with or translated to its host address is called *name resolution*. It is usually performed by a *name service*.

The Name Services module enables you to do the following:

Name Services on the Netra Server

The Netra server provides three types of name services:

- *Local name service (host only)* – Translation is done locally (by looking up the name in a file)
- *Network Information Service (NIS - LAN, WAN)* – Translation is done by a NIS server (running either on the Netra server or on another host)
- *Domain Name System (DNS - whole internet)* – Translation is provided by a DNS server (running either on the Netra server or on another host).

The Netra server can use any or all of the name services at the same time. If you decide to use more than one name service, the default order configured by Netra j is NIS, local, DNS.

For example, suppose your Netra server is configured to use the local name service and DNS. When a name service query is made, the server attempts name resolution by looking up the host name in the local database first. If the host name is found, the server returns the host address. If not, the query is passed to a DNS server. If the DNS server resolves the query, it returns the information.

Correct Hosts Policy for /etc/nsswitch.conf

The name service configuration file, `/etc/nsswitch.conf,` should not be configured to only search the NIS database for host information. The search should include a `files` option to search in the local files.

For example, the name service ignores information in the local host if the `/etc/nsswitch.conf` file contains the following entry:

```
hosts: nis [NOTFOUND=return] dns
```

For the Netra j server and the NC clients to work correctly, change the `/etc/nsswitch.conf` file to include one of the following entries:

```
files nis [NOTFOUND=return] dns
```

or

```
nis files dns
```

Configuration Options

The four name service options (local, NIS, DNS server/client, and DNS client) work independently of each other.

- The local name service component enables you to add or delete hosts and their respective addresses (edit the local host table).
- The NIS component enables you to add/configure or delete the Netra server as an NIS client, NIS master server, or NIS slave server.
- The DNS server component enables you to set up a DNS server. The various options are described in detail below.
- The DNS client component enables you to configure the Netra server as a DNS client.

Local Name Service

The local name service provides a local database that associates the names of hosts with their host addresses. This name service is only available to programs running on the Netra server.

For the local name service, the Netra server is both client and server. As a local name server, your Netra server contains a list of host-name-to-host-address mappings for its own use. These mappings are available only to applications running on the Netra server. Information entered in the local database is automatically available to programs running locally.

If the Netra server is configured as a NIS master, the Local Host information is pushed to the hosts NIS map.

▼ To Configure Local Name Services

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click Local Name Service.**

   The Local Name Server Administration page is displayed.

2. **Complete the form using the information in the following table.**

TABLE 3-5 Local Name Server Administration

Host Information	Description
Host Addresses/ Host Names/ Aliases	The host addresses and corresponding host names and aliases. The host names can be partially or fully qualified to be compatible with other name services. However, this database resolves only host names that have an exact match in the database. Maximum 2000 records.

NIS

The network information service (NIS) provides name services and other information, such as users on the network, for a local network. If there is a NIS server on the network, use the Netra Name Service module to configure the Netra server as a NIS client. This means that it uses NIS to resolve host names, host addresses, and host aliases.

The Netra j software provides NIS client/slave/master capability. The following maps are specifically required by NCs: `passwd.byname`, `passwd.byuid`, `printers.conf.byname`, `auto.home,hosts`, and `bootparms`.

▼ To Configure NIS for the Netra Server

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click NIS (Network Information Name Service).**

   The NIS Administration page is displayed.

2. **Click Configure.**

   The NIS Configuration page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 3-6 NIS Configuration

NIS Domain	Description
NIS Domain Name	The NIS domain in which the Netra server resides.
NIS Client	Select this option to be a NIS client only. A NIS server for this domain must exist on the same subnet as the Netra server.
NIS Master Server	Select this option to provide NIS information to other NIS clients. The Netra administration provides only the following maps: `auto.home`, `passwd.byname`, `passwd.byuid`, `printers.conf.byname, auto.master, hosts, bootparms and ypservers.`
NIS Slave Server	Select this option to provide NIS information to other NIS clients when there is no other NIS server on your subnet. The NIS maps must exist on a different server (the NIS master server) and must be transferred to the Netra server. If this option is selected, all maps are transferred from the master server immediately.
Map Master	The host name or host address of the NIS master server. This field is relevant only for slave servers.

▼ To Modify or Unconfigure NIS Configuration

Note – The Modify and Unconfigure options are displayed only when the Netra server is configured.

1. **From the Main Administration page, under “Network Service Administration,” click Name Service, then click NIS (Network Information Name Service).**

   The NIS Administration page is displayed.

2. **Choose one of the following:**

   - To modify NIS configuration, click Modify, update the form using the information in TABLE 3-6, and click OK to confirm the operation.
   - To unconfigure an NIS configuration, click Delete NIS Configuration, and confirm the operation. The Netra server no longer uses NIS to resolve host names, and the NIS domain name is ignored.

DNS

The Domain Name System is the name resolution system used by the Internet. It is a hierarchical naming system based on the concept of domains. At the top level, there is the domain . (the root domain), below it are domains such as com, edu, or ie, which act as a first partition of the name space. Individual organizations have their own domains below these domains. Below com you find companies in the US (for example, sun.com), below edu are American educational institutions (for example, stanford.edu), and below ie you find institutions in Ireland (for example, tcd.ie). The individual organizations often divide these domains into subdomains.

DNS works by delegation. Each domain is served by one or more DNS servers, which has a database of the hosts in the domain. In addition, the DNS servers also have a list of other DNS servers to query in case they cannot resolve a name locally. This list typically consists of a set of DNS servers called root servers at the top of the DNS hierarchy, which in turn know what DNS servers hold data about the different top-level domains.

Individual hosts use the Domain Name System to resolve name queries by becoming DNS clients. To configure a DNS client, you specify the IP address of the DNS server that you want to respond to the queries for you. You have to do this even if the individual host is a DNS server, in which case you typically set it to answer the queries itself.

The hostname of a computer together with its full domain name (ending in the top level domain) makes up its complete DNS name. If the host stimpy resides in a domain called comedy, which is a subdomain of cartoon under the top level domain net, then stimpy.comedy.cartoon.net is the complete name for stimpy.

An important distinction used in the text below is that between a fully qualified name or a partially qualified name. When referring to the fully qualified name of a host of a domain, it means the complete DNS name ending in a trailing period. The fully qualified name for stimpy is stimpy.comedy.cartoon.net..

A partially qualified name is a name that does not specify the domain branch all the way up to the top. Partially qualified names are used as a shorthand when the name resolution software can attach the rest of the domain name. If you are in the domain comedy.cartoon.net and use stimpy to mean stimpy.comedy.cartoon.net, then you are using a partially qualified name. If a DNS name does not end with a trailing period, it is treated as partially qualified.

The distinction between fully and partially qualified names is important in many of the DNS configuration tasks - if you experience any problems, please refer to the help pages, which always tell you which one to use.

DNS Server Options

There are several different types of a DNS server. At the most basic, the server does not hold any permanent data about any domains itself, but simply forwards queries to other servers (*a cache-only server*) and stores the result. A *DNS primary server* has a master database for a domain. A *DNS secondary server* provides a local copy of master database for a domain that it copies from a primary server. DNS server can be both a primary and a secondary domain server at the same time.

All DNS servers store the results of successful queries (whether it resolved the query itself or forwarded it to another DNS server). If the server receives another query for the same name, it replies with the stored answer. This is called *caching*. A server that only does this (a cache-only server) can be useful to shorten the response time compared with contacting a more remote DNS server.

There are two different ways in which a DNS server can provide data for a domain; it can be a primary, or a secondary server for the domain. For the primary server, the DNS administrator maintains the master database for the hosts in the domain on the server. For the secondary server, the server keeps a local copy of the master database for the domain that it retrieves from the primary server. It periodically compares its database to the one on the primary server and requests a new copy if a difference is detected.

The difference between normal caching and being a secondary server for a domain is that normal caching only stores the results from previous queries. A secondary server actively retrieves the information in anticipation of future requests. This reduces the load on the primary server, and also makes it a backup in case the primary server cannot be contacted. If your server is a primary server for a domain, you should have a secondary as a backup.

There are two different types of DNS server configuration that you use depending on what the structure of your local domain is. The first type, which is referred to as *Basic DNS Server*, involves specifying a list of other DNS servers to query if a name cannot be resolved locally. The second type is called a *DNS Internal Root Server*. It is used on Intranets without an Internet connection (in other words, without access to any other DNS servers), and also on large Intranets with several subdomains, where there is a need for special DNS servers for the internal hierarchy.

Finally, a DNS Primary Server may need to provide reverse maps (IP address to name) as well as forward maps (name to IP address). Please consult with your ISP to find out whether this responsibility is delegated to you or not.

Configuring the DNS Server

Basic DNS Server

▼ To Configure a Basic DNS Server

This configures the Netra Server as a DNS Server with a list of DNS root servers to query. If you configure the Netra server as a DNS server, you would normally configure it to be a DNS client of itself. Set up the server before you configure the client.

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**
2. **Under "DNS Server," click Configure as a basic DNS Server.**

   The Basic DNS Server Configuration page is displayed.
3. **Complete the form using the information in following table.**

TABLE 3-7 Basic DNS Server Configuration

Option	Description
DNS Domain Name	The DNS domain in which the Netra server resides. This name is used for two purposes: • as a contact address for the DNS administrator. • when creating the DNS server record for this server for any primary domains for which it is responsible. The domain name is assumed to be fully-qualified whether or not you enter a period at the end. Example: `comedy.cartoon.net.`
DNS administrator's user name	Enter the name or alias of the local user (for example, `root`) who is responsible for DNS. All DNS database files contain a contact address - the address for this server consists of the name of this user, the name of the Netra server, and the domain name entered into the domain field.
Root Name Servers/ IP Address	The fully qualified host names and host addresses of a set of DNS servers to contact to resolve name service queries. Use the default servers if the Netra server is connected directly to the internet. If the Netra server is behind a firewall, enter a set of servers that it can reach.

After successfully configuring a DNS server, the module checks to see if the DNS server is configured as a client of itself. The Operation Successful message, displays information about the server configuration, and if the DNS server is not configured as a DNS client of itself, provides a link to the DNS client configuration form.

Note – If you change the name of the domain in which the server resides, the DNS resource files for the primary domains are updated with respect to the contact address and the name server address of the Netra server. Review the individual primary domains to update any other references to the old domain name.

▼ To Modify or Delete a Basic DNS Server

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

   The DNS Server Administration page is displayed.

2. **Choose one of the following:**
   - To modify a Basic DNS server, click Modify, and make the changes in the form using TABLE 3-7 as a reference.
   - To delete a Basic DNS server, click Delete, then confirm the operation.

DNS Internal Root Server

▼ To Configure a DNS Internal Root Server

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

2. **Under "DNS Server," click Configure as a internal root server).**

   The Configure as an Internal DNS Root Server page is displayed.

3. **Complete the form using the information in following table.**

TABLE 3-8 DNS Internal Root Server Configuration

Option	Description
DNS Domain Name	The DNS domain in which the Netra server resides. This name is used for two purposes: • as a contact address for the DNS administrator. • when creating the DNS server record for this server for any primary domains for which it is responsible. The domain name is assumed to be fully-qualified whether or not you enter a period at the end. Example: `cartoon.net.`
DNS administrator's user name	Enter the name or alias of the local user (for example, `root`) who is responsible for DNS. All DNS database files contain a contact address - the address for this server consists of the name of this user, the name of the Netra server, and the domain name entered into the domain field.
Internal Root Server / IP Address	This field is only relevant if the internal network has other DNS internal root servers (an entry for this server is created automatically). If there are none, leave this field blank. Enter the fully qualified host names and host addresses of each DNS internal root server.
DNS Server / IP Address	This field is only relevant if the internal network has non-root DNS servers that reside in the top-level domain and to which this server delegates responsibility for primary domains. If there are none, leave this field blank. Enter the fully qualified host names and host addresses of each DNS server. If a server has more than one IP address, create an entry for each address
in-addr.arpa Domain Name / DNS Server	This field is only relevant if this root server delegates responsibility for reverse maps (in-addr.arpa domains) to other DNS servers on the internal network. If it does not, leave this field blank. Create domain name/name server entries for the in-addr.arpa domains maintained on the other DNS servers. Use fully qualified names in both cases.

Create the primary domain corresponding to the name entered in the DNS Domain Name field with the "Add a Primary Domain" form.

The Operation Successful page displays information about the server configuration, and if the Netra server is not configured to be a DNS client of itself, informs you of this and provides a link to the DNS client configuration form.

Note – If you change the name of the domain in which the server resides, the DNS resource files for the primary domains are updated with respect to the contact address and the name server address of the Netra server. Review the individual primary domains to update any other references to the old domain name.

▼ To Modify or Delete a DNS Internal Root Server

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

   The DNS Server Administration page is displayed.

2. **Choose one of the following:**

   - To modify a DNS internal root server, click Modify, and make the changes in the form using TABLE 3-8 as a reference.
   - To delete a DNS internal root server, click Delete; then confirm the operation.

DNS Primary Server

▼ To Configure the Netra Server as a DNS Primary Server

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

2. **Under "DNS Server," click Add a primary domain.**

   The Add DNS Primary Domain page is displayed.

3. **Complete the form using information in the following table.**

TABLE 3-9 DNS Primary Server Administration

DNS Primary Server Information	Description
Primary Domain Name	The name of the primary domain, for example: mydomain.com. The name you enter is assumed to be fully qualified whether or not it ends in a trailing period.
Host Names/Host Addresses	The host names and corresponding host addresses of the hosts within the domain. For example, `myhost     1.2.3.4`
Host Aliases/Host Names	Enter alias names for hosts in the domain followed by a known name of the host. For example, `www       myhost`
Mail Addresses/ Preferences Mail Servers/	Use this field if people are expected to send mail to the domain rather than directly to the mail server. Each entry consists of the name of the domain, followed by a preference value and the host name of the mail server. For example, if you are entering data for `mydomain.com` in which the server that deals with mail is called `mailhost`, make an entry as follows: `mydomain.com.          5            mailhost` The preference value is an integer: the lower the value, the higher the priority of that mail server.
Domains/ DNS Servers	Enter records for other DNS servers. Each record consists of the name of the domain that the server is responsible for followed by the name of the server. You do not need to create a record specifying that the Netra server is the name server for this domain - the Netra software does that automatically (the record is shown on the success page, and also on this form if you modify the domain data at a later time).

4. **Click OK.**

If the Netra server is not configured to generate reverse maps automatically, the success page displays a link to the DNS Reverse Map Generation form.

▼ To Modify or Delete a DNS Primary Domain

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

The DNS Server Administration page is displayed.

2. **Choose one of the following:**
   - To modify a DNS primary domain, click Modify, and make the changes in the form using TABLE 3-9 as a reference.
   - To delete a DNS primary domain, click Delete, then confirm the operation.

Example of a Primary Domain Configuration

It will be useful to configure a sample primary domain configuration. This example sets up a domain called `comedy.cartoon.net` on the name server `stimpy`. There are various hosts in the domain that have different functions.

In the Primary Domain Name field, specify:

```
comedy.cartoon.net
```

In the Host Names/Host Addresses field, type a list of those hosts whose presence are to be broadcast to any machine that can connect to this DNS server. For this example, type `ren` and `stimpy`, and for a host called `homer` that resides in (located) in the DNS subdomain `black.comedy.cartoon.net`, type `homer.black`.

```
ren          118.1.1.2
homer.black  118.2.1.2
stimpy       118.1.1.3
```

The Internet community uses conventional names for hosts that provide certain types of services, in order to make them easy to locate. For instance, the WWW server for a domain is usually known as `www.domain,` and an anonymous FTP server is typically called `ftp.domain`. On `comedy.cartoon.net`, `ren` is an FTP and WWW server, while `stimpy` is a name server. Standard aliases for these machines are added into the Host Aliases/Host Names field. For example:

```
www             ren
ftp             ren
ns              stimpy
```

`stimpy` is going to handle mail sent to `comedy.cartoon.net,` so an MX record needs to be created.

```
comedy.cartoon.net.   5      stimpy
```

Finally, to the name server records, are added a single record for a host called homer that resides in a subdomain of comedy.cartoon.net called black – homer.black.comedy.cartoon.net is the name server for that domain.

```
black.comedy.cartoon.net.   homer.black.comedy.cartoon.net.
```

If a domain contains subdomains that are maintained on another DNS server, the domain data must include records for the DNS servers for the subdomains. Note that in our example, since homer resides in the black subdomain, a Host Name/Host Address record for homer had to be added so that stimpy can reach it.

There is no need to create a name server record which says that stimpy is a name server for comedy.cartoon.net, because the Netra j software does that automatically. Next time you visit this form to modify the domain, the following record shows up next to the one for homer.

```
comedy.cartoon.net.     stimpy.comedy.cartoon.net.
```

Automatic Reverse Map Generation

Use this form to configure the Netra server to generate reverse maps (address to name records) corresponding to the host records in the primary domains for which the server is responsible automatically. A link to the form appears on the DNS Server Administration form if the Netra server is responsible for at least one primary domain. The reverse maps will be based on the first three octets of the IP address, which assumes that the Netra server is authoritative for the entire block of class C hosts.

▼ To Generate Reverse Maps

1. **From the Main Administration page, under “Network Service Administration,” click Name Service, then click DNS (Domain Name Service) Server Administration.**

2. **Under “DNS Server,” click Enable Automatic Reverse Map Generation.**

   The DNS Reverse Map Generation page is displayed.

3. **Click OK.**

▼ To Disable Automatic Reverse Map Generation

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

2. **Under "DNS Server," click Disable Automatic Reverse Map Generation.**

   The DNS Reverse Map Generation page is displayed.

3. **Choose one of the following:**

   - Disable automatic reverse map generation. Leave the current reverse maps in place.
     This leaves the reverse maps in place, but stops updating them.
   - Disable automatic reverse map generation. Remove the current reverse maps.
     This both stops updating reverse maps and removes the current files.

4. **Click OK.**

DNS Secondary Domain

▼ To Configure the Netra Server as a DNS Secondary Server

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

2. **Under "DNS Server," click Add a secondary domain.**

   The Add DNS Secondary Domain page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 3-10 DNS Secondary Server Administration

DNS Secondary Server Information	Description
Secondary Domain Name	The name of the secondary domain. A secondary DNS server copies domain information from another DNS server, called the master server. It can also act as a backup name server for clients when the primary server is unreachable. The domain name is assumed to be fully qualified whether or not it ends in a trailing period. Example: horror.`cartoon.net.`
Master DNS Servers' Host Addresses	The host addresses of the master DNS name servers in the order in which they should be queried. A master DNS server can be either an existing primary or secondary DNS server. Example: `118.144.102.6`

▼ To Modify or Delete a DNS Secondary Domain

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Server Administration.**

2. **Choose one of the following:**
   - To modify a DNS secondary domain, click Modify, and make the changes in the form using the information in TABLE 3-10.
   - To delete a DNS secondary domain, click Delete, and then confirm the operation.

Notes to Those Who Also Administer DNS Manually

If you edit the DNS files manually as well as using the Netra DNS Server configuration component, the following information explains what changes Netra makes. You do not have to read this section if you always use Netra to configure DNS.

- The "Modify the DNS Server Configuration" form edits the "local" file (the file with the reverse lookup for the local machine) and depending on the type of DNS server, either the "cache" file or the "root" file. If you change the name of the domain in which the server resides or the DNS administrator, all the primary resource files are rewritten to create a new SOA record and to update the name server record.
- If you modify a primary domain, the corresponding resource file and the entry in the named boot file are rewritten.

- If you modify a primary domain, only the entry in the named boot file is rewritten.
- When recreating resource files, Netra does not change the values in the SOA (other than the revision number). Resource Records of other types than those that can be entered on the forms are left intact. TTLs from individual resource records that are edited by Netra are removed.

Configuring the DNS Client

▼ To Configure the Netra Server as a DNS Client

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Client Administration.**

   The DNS Client Administration page is displayed.

2. **Click Configure as a DNS Client.**

   The DNS Client Administration page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 3-11 DNS Client Administration

Option	Description
DNS Domain Name	The DNS domain that is appended to qualified host names. Usually, this is the name of the domain in which the Netra server resides. Example: `comedy.cartoon.net`
Name Server 1	The host address of the DNS server that is tried first for all DNS queries. Example: `118.144.79.5`
Name Server 2 (optional)	The host address of the DNS server to use, if the first name server is unreachable. Example: `118.144.79.6`
Name Server 3 (optional)	The host address of the DNS server to use, if the first two name servers are unreachable. Example: `118.144.102.6`

If the Netra server is configured to be a DNS server and is to be a client of itself, then set Name Server 1 to be `127.0.0.1` (the loopback address).

▼ To Modify or Delete DNS Client Setup

1. **From the Main Administration page, under "Network Service Administration," click Name Service, then click DNS (Domain Name Service) Client Administration.**

   The DNS Client Administration page is displayed.

2. **Choose one of the following:**

   - To modify a DNS client setup, click Modify, and make the changes in the form using TABLE 3-11 as a reference.
   - To delete a DNS client setup, click Delete then confirm the operation.

Sun WebServer Administration

▼ To Access Sun WebServer Administration

1. **From the Main Administration page, under "Network Service Administration," click Sun WebServer (port 80).**

   The Sun WebServer Administration page is displayed.

2. **Login.**

   The Sun WebServer console is displayed.

3. **See the Sun WebServer online help for administration procedures.**

CHAPTER 4

Connectivity Software

Network computers (NCs) can provide access to applications and data on UNIX, PC, mainframe, and midrange host systems through a variety of connectivity technologies. NCs with JavaOS, such as Sun’s JavaStation systems, also run Java applications and applets natively.

Sun’s windowing products enable Sun Workstation and NC users to run Microsoft Windows (3.x, 95, and NT) applications on an application server and display them back to their desktops. UNIX X windows applications can also be run. The remote windowing products include the WinFrame product from Citrix Systems, Inc., and GO-Joe from GraphOn.

For legacy connectivity, Sun provides OC://WebConnect™ software, which enables users on clients with the capability of using Java technology to access data and applications on IBM mainframes and on midrange computers from many vendors.

This chapter is organized as follows:

Citrix Software

Citrix software provides for the NC a thin-client that can access virtually any Windows application across any type of network connection. Citrix produces a client/server product for Windows NT 3.5.1 called WinFrame. Citrix also produces a client product for Windows NT 4.0 called MetaFrame. MetaFrame works with Microsoft Windows NT Server, Terminal Server Edition (the server portion for Windows NT 4.0).

For additional information, and to download the Citrix software refer to: `http://www.sun.com/desktop/products/PCCP/remotewindowing/citrix`.

After downloading the client software from the web and uncompressing it read the `README` file for detailed installation instructions.

After configuring the Windows NT server with the appropriate server software, use the Netra j Network Computer Application Management module to specify the host name or IP address of the NT server for the Netra server (see "To Reference Remote Windowing Servers" on page 104). In the rest of this section, NT Server refers to the NT server that has been configured with the appropriate server software for use with NCs.

Running the Citrix ICA Client, Java version as an Applet

The Citrix ICA Client, Java version, running as an applet requires that the applet be inside an HTML file. The HTML file is the default HTML file for the web server running (at port 80) on the WinFrame server, or the Microsoft Windows NT Server Terminal server. See the `README` for any modifications that need to be made to the server. Use the HotJava Views Administration module to add this Citrix Client applet as a HotJava Views application (see "Adding an Application Icon to the HotJava Views Selector" on page 62).

Create an HTML page or modify the example (see "Example" on page 93) to suit your environment. The example assumes that the `.class` files are located in the same directory as the `.html` file, but you can store them elsewhere by using the CODEBASE applet tag. The applet class is named `JICA.class`.

The following parameters can be specified in the HTML file. The Address parameter is the only required parameter.

1. Address – This is the address of the NT server, or the name of the published application if the TCPBrowserAddress parameter is present. This parameter is required.

2. TCPBrowserAddress – This is the address of the NT server, used when specifying the name of a published application instead of the name of a NT server.

3. Start – Values for Start are manual or auto. This is used to specify whether the Citrix ICA Client, Java version starts immediately (auto) or after user interaction (manual). The default value is manual.

4. Username – This is the user name to use during login.

5. Domain – This is the name of the domain for the user name.

6. Password – This is the password of the user.

7. InitialProgram – This is the name of the initial program to run after connecting to the WinFrame server.

8. WorkDirectory – This is the path of the working directory for the initial program to run after connecting to the WinFrame server.

9. EndSessionTimeout – When users leave a page containing an open ICA session for more than 300 seconds (5 minutes), the session is disconnected. Use this parameter to specify a different value in seconds.

10. Border – This parameter turns the border on or off. Values for this parameter are on or off (the default).

11. BorderWidth – This parameter enables the user to specify a border width in pixels. The default value is 6.

12. ICAPortNumber – The default ICA port number is 1494. A different port number can be specified using this parameter or by appending the port number to the address value. For example, WFServer:1495.

13. LargeCacheSize – This parameter can be used to modify the size of the client system’s cache in bytes. Ordinarily, the size of the cache is determined automatically based on the dimensions of the connection.

Example

This example shows the applet part of the HTML file:

```
<applet archive=JICA.zip code=JICA.class width=640 height=480>
        <param name="Address"            value="llama2">
        <!param name="Start"             value="manual">        <!default>
        <!param name="Start"             value="auto">
        <param name="Border"             value="on">
        <!param name="Border"            value="off">           <!default>
        <!param name="BorderWidth"       value="6"> <!default when border on>
        <!param name="Username"          value="jack">
        <!param name="Domain"            value="llama2">
        <!param name="Password"          value="">
        <!param name="InitialProgram"    value="notepad.exe">
        <!param name="WorkDirectory"     value="c:users\jack">
        <!param name="TCPBrowserAddress" value="llama2">
        <!param name="ICAPortNumber"     value="1494">          <!default>
        <!param name="LargeCache"        value="5000000">
    </applet>
```

Running the Citrix ICA Client, Java version as an Application

You can run the Citrix ICA Client, Java version, as an application if you have the `.class` files stored locally on your client system (Netra j server). The `.class` file to run is the same as the applet class, `JICA.class`.

The same parameters apply to the client in application mode as to the client in applet mode, with the exception of the Start, Border, BorderWidth, and EndSessionTimeout. These parameters have no meaning when running the client as an application.

Use "Client Application Administration" on page 58 to add the Citrix ICA Client as an application for an NC (see the `README` for the values of the options). After you have added the application, it is displayed as one of the choices for default application when adding NCs.

GO-Joe

The GO-Joe client-server solution enables access to Solaris/X environments from an NC.

GO-Joe comes in two packages. The GO-Joe host software, which you install, and the GO-Joe client software, which the Netra j 3.0 installation installs automatically.

The GO-Joe host software (SUNWgjvxs) is provided on the Netra j 3.0 CD in the /Misc directory to be installed on the Solaris 2.5.1 or Solaris 2.6 server of your choice. The host software sits on top of the X/CDE software on the server, taking advantage of the extended features already built into the Solaris/X server (for example, Display PostScript).

The client portion of the GO-Joe package (SUNWgjvxv) is installed with the other Netra j packages. This is the GO-Joe Java applet enabling the user to access Solaris and X applications via your GO-Joe host server. It is setup under the web server document root (system default port 80) of the Netra j server in the GO-Joe directory. In order to set up the HTML/applet file provided with this package, you must enter the name of the server where the GO-Joe host software is installed. See "To Reference Remote Windowing Servers" on page 104.

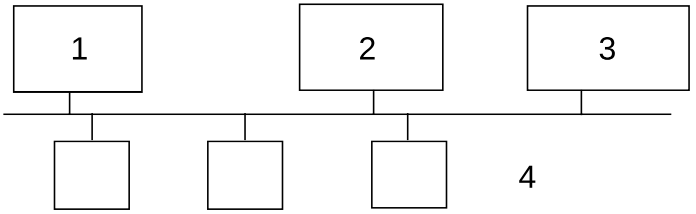


FIGURE 4-1 GO-Joe Architecture

Legend:

1. Remote X applications

2. Netra j / web server houses the GO-Joe applet

3. Solaris/X server with GO-Joe host software

4. NCs run the GO-Joe applet

System Requirements

You can install and run GO-Joe host software on SPARC™ systems running the Sun Solaris operating environment, version 2.5.1 or 2.6.

Note – The `netra_install` script does not install the `SUNWgjvxs` host software package. Use `admintool` or `pkgadd` to install this package on the Solaris 2.5.1 or 2.6 server of your choice.

Dependencies

GO-Joe host software requires additional Solaris software to run properly. The following table lists the Solaris dependencies.

TABLE 4-1 Solaris Dependencies for GO-Joe

Package ID	Description	Location
`SUNWcsr`	Core Solaris, (root)	Netra j 3.0 software (Solaris 2.5.1 add-on cluster) and Solaris 2.6 CD
`SUNWcsu`	Core Solaris, (usr)	Netra j 3.0 software (Solaris 2.5.1 add-on cluster) and Solaris 2.6 CD
`SUNWcar`	Core architecture, (root)	Solaris 2.5.1 or 2.6 CD
`SUNWkvm`	Core architecture, (usr)	Solaris 2.5.1 or 2.6 CD
`SUNWlibms`	Solaris bundled shared libm	Solaris 2.5.1 or 2.6 CD
`SUNWtltk`	ToolTalk runtime	Solaris 2.5.1 or 2.6 CD
`SUNWxwplt`	X Window platform software	Solaris 2.5.1 or 2.6 CD
`SUNWolrte`	OPEN LOOK toolkits runtime environment	Solaris 2.5.1 or 2.6 CD
`SUNWoldte`	OPEN LOOK desktop environment	Solaris 2.5.1 or 2.6 CD
`SUNWxwdv`	X Window system kernel drivers	Solaris 2.5.1 or 2.6 CD
`SUNWxwfnt`	X Window system fonts	Solaris 2.5.1 or 2.6 CD
`SUNWdtcor`	Solaris desktop `/usr/dt` file system anchor	Solaris 2.5.1 or 2.6 CD
`SUNWmfrun`	Motif runtime kit	Solaris 2.5.1 or 2.6 CD

GO-Joe uses JDK™ 1.1 application program interfaces (APIs), including AWT 1.1 (abstract windowing toolkit) and the New Event Model. Therefore, GO-Joe requires a browser that is fully compliant with the JDK1.1 technology.

Components and Session Overview

A GO-Joe session involves several components working together to bring X Windows to NC desktops:

- The NC client (GO-Joe applet)
- The X-to-RapidX converter (part of the GO-Joe host software)

- A Web server to deliver the GO-Joe applet (web server on the Netra j server used as default)

The GO-Joe session proceeds as follows:

1. Enter a URL in the client system's browser or Java environment, which loads the HTML page containing the GO-Joe applet from the Web server.
2. The GO-Joe applet prompts you for a login and password to authenticate you to the GO-Joe host server.
3. When you click the Start X Session button (or press Return, depending on the browser), the login and password are sent to the GO-Joe host server (default port is 491 set up automatically) at the port specified in the HTML page loaded in step 1.
4. The GO-Joe host server accepts the applet's connection and passes it off to the `go-login` program.
5. The `go-login` program receives the user name and password specified in Step 3. If the user name and/or password are incorrect, an error is returned by the applet and it returns to Step 3.
6. If the user name and password are valid, the `go-login` program starts an X session.
7. Initialization scripts check for a GO-Joe token, and if present, modify the session startup behavior as specified by the controls in the token parameter.

After these steps, the session is displayed within the GO-Joe applet and you are able to run X clients from the network.

Advanced Configuration Options

The GO-Joe applet ships with an example startup HTML file, `xsession.html`. This file is used by Netra j administration and should not be modified manually. To make advanced configurations, copy the `xsession.html` file to another file (for example, `x.html`) and use it for modifications.

The sample `x.html` file contains an example startup session that exercises some of the available parameters for the applet, but this file must be customized before it can be used.

TABLE 4-2 Applet Parameters

Parameter	Description
width	This parameter is specified in the `APPLET` tag and determines the width of the GO-Joe frame in the HTML file. Its format is browser-specific, but it can generally be an absolute number of pixels (for example, “width=800”) or a percentage of the browser window's width (for example, “width=100%”).
height	This parameter is specified in the `APPLET` tag and determines the height of the GO-Joe frame in the HTML file. Its format is browser-specific, and it can generally be an absolute number of pixels (for example, “height=600”) or a percentage of the browser window's height (for example, “height=90%”).
server	This parameter specifies the name or IP address of the host machine that runs the X session.
port	This parameter specifies the port number that is contacted by the GO-Joe applet. Usually, this is port 491; however, it can be different if the port is being used by a service other than the `go-login` service on the GO-Joe host server.
token	This parameter specifies an optional “token” value to be passed into the environment of the X session. See “Token Parameter” on page 101 for information on the token parameter.

The following is a sample `x.html` file that initiates a default session. This sample does not demonstrate all of the available parameters.

```
<HTML>
<HEAD><TITLE>GO-Joe Example Session</TITLE></HEAD>
<BODY>
<HR>
<APPLET ARCHIVE=”gojoe.jar” CODE=”gojoe.class” WIDTH="800"
HEIGHT="600">
    <PARAM NAME=”server” VALUE=”myhost”>
    <PARAM NAME=”port” VALUE=”491”>
</APPLET>
</BODY>
</HTML>
```

The GlobalHost Loadable ddx Module

The GO-Joe applet communicates through a dynamically loaded Xsun device driver. This driver appears to the Xsun server to be a standard display driver, but transmits display operations to the GO-Joe applet. This is referred to as the GlobalHost loadable ddx module.

To start the Xsun server with the GlobalHost loadable ddx module, you need to reference the device files created in `/devices` similar to the following:

```
/usr/openwin/bin/goinit /usr/dt/bin/Xsession --
/usr/openwin/bin/Xsun :1  -dev /dev/fbs/goglobal0 -I -inetd
```

When the Xsun queries this device, it loads the correct module for GO-Joe.

Note that you would never type this command at the command line. It is started by a script after the `go-login` program has authenticated the user through `inetd` or started by the `go-login` program itself.

The `go-login` Authentication Program

The `go-login` program is started by `inetd` and receives user authentication information from the applet before starting the session. The `go-login` program is designed to be called directly from `inetd`. Some implementations of `inetd` software limit the number of command-line arguments that can be passed to the `go-login` program, making it necessary to call the `go-login` program from a `goshim` script. The `goshim` ensures that all of the arguments are passed to the `go-login` program. To use a `goshim`, `go-login` must be installed into your `inetd.conf` file as follows:

```
go-login stream tcp nowait root /usr/openwin/server/etc/goshim
goshim
```

Adding the GO-Joe Icon to the HotJava Views Selector

Note – You should specify the server parameters before adding an icon to HotJava Views Selector.

Icons in the HotJava Views Selector are part of a HotJava Views group's configuration. To add the GO-Joe icon to a group's configuration, follow the procedure "To Add an Application Icon to the HotJava Views Selector" on page 63. See the HotJava Views Administration online help for additional information.

Note – To access the HotJava Views Administration module, use the HotJava Browser provided with the Netra j software. The path to the HotJava Browser is `/opt/SUNWnhjb/bin/hotjava`.

Running GO-Joe

To start a GO-Joe session, load the HTML file with the GO-Joe applet into your Java environment. GO-Joe prompts you for a user name and password for the session, and after authentication, provides the X display on your Java desktop.

This session is almost identical to running an X session on the system console, with a few differences, which are described below.

$DISPLAY Environment Variable

The `$DISPLAY` environment variable tells X clients where to contact your X server. GO-Joe sets this variable to point to an alternate display on your host machine. For example, if your UNIX host is named `workstation` and the Java device is named `java`, you might expect the `$DISPLAY` variable to set `java:0` as its value. However, GO-Joe uses the host name for its `$DISPLAY` variable value, in this case, `workstation:1`.

GO-Joe makes an additional optimization that can be somewhat confusing. In X parlance, if the `$DISPLAY` variable is set to `unix:#,` the JavaStation client attempts to connect using a local transport. For example, instead of using TCP/IP, it connects using a named pipe. This connection is faster than using TCP/IP for clients running on the same host. However, the `unix:#` value cannot be used if you run clients from different hosts.

Instead, use the following shell script to change the `$DISPLAY` variable to point to the host name of your machine. This translates `$DISPLAY` from `unix:3`, for example, to `workstation:3` enabling X clients on other machines to successfully contact GO-Joe on the workstation host. This can be included in the `.profile` file:

```
DISPLAY=`/bin/uname -n``/bin/expr $DISPLAY : '[^:]*\(:.*\)'`
```

Using a Two-Button Mouse

X requires and assumes the availability of a three-button mouse. Most Java environments provide a two-button mouse. In an X session, the left and right mouse buttons correspond to the left and right mouse buttons under X. GO-Joe maps the simultaneous pressing of both mouse buttons into a middle mouse button press.

The Mouse Arrow

Current AWT implementations provide only limited support for specifying the shape of the mouse arrow in the Java environment. For this reason, GO-Joe currently does not change the shape of the mouse arrow.

Token Parameter

The GO-Joe applet accepts an optional token parameter in its HTML file. If the token parameter is present, the applet transmits it to the `go-login` program, along with the user name and password. The `go-login` program creates an environment variable, `$GG_TOKEN`, which is available for other startup scripts to process.The following three controls are supported by the token parameter.

- *Session Control* `[session=<openwin|cde>;]` – This control is used to specify the session as either OpenWindows™ or CDE. If this control is not set, OpenWindows is the default desktop on Solaris version 2.5 and earlier, and CDE is the default for Solaris version 2.6 and higher. The session control is optional.
- *Window Manager Control* `[wm=</path/to/window/manager>|nowm>;]` – This control is used to specify alternate window managers. For security reasons, you must specify an absolute path corresponding to an executable window manager. Therefore, no arguments can be passed to the window manager. The window manager control is optional.

Note – The X session terminates when the key client terminates. Normally, the window manager is the key client and provides a menu item or button to exit the session. If you specify `nowm`, one of the clients started in the case specified by the Startup Control needs to become the key client. Therefore, if `nowm` is specified, a startup control is required.

- *Startup Control* – The startup control must correspond with a `$GG_TOKEN` case in either `$HOME/.gotoken-init` or `/usr/openwin/lib/gotoken-init`.

The Solaris session startup files (OpenWindows or CDE) are initiated when the GlobalHost loadable ddx module is installed.

When starting an OpenWindows session, the token parameter is used in $OPENWINHOME/lib/gotoken-init or in $HOME/.gotoken-init. If $HOME/.gotoken-init exists, it is used before $OPENWINHOME/lib/gotoken-init. System administrators and system integrators can create system-wide token processing routines by modifying $OPENWINHOME/lib/gotoken-init, while still enabling users to override these settings in the $HOME/.gotoken-init file. In addition, if the $GG_TOKEN variable is not set, the session startup is the same as a standard OpenWindows session.

The CDE startup mechanism is somewhat different from the OpenWindows mechanism. Unlike OpenWindows, which uses a single openwin-init file, CDE stores its session initialization as a directory filled with several files. Because of this, the CDE token is used to specify a session to be started. Sessions are stored in /usr/dt/config/dtgotokens, in subdirectories that match the name of the startup control. When the session is started with the CDE token, the session directory is copied into the user's home directory, and CDE starts this session for the user.

Structure of gotoken-init

The gotoken-init is based on the standard openwin-init file, with the addition of the following section:

```
    if [ "$OW_WINDOW_MANAGER" = ’:’ ]; then
       toolwait=
    else
       toolwait=toolwait
    fi
    unset OW_WINDOW_MANAGER
    case "$GG_TOKEN" in
    xterm)
      $toolwait $OPENWINHOME/bin/xterm
     ;;
    *)
        echo>&2"$OPENWINHOME/lib/gotoken-init:error:\'$GG_TOKEN\':
case not found."]
    echo >&2 "    Using defaults."
    . $OPENWINHOME/lib/openwin-init
    ;;
esac
```

This section parses the $GG_TOKEN (with any session or window manager controls removed) and starts the appropriate client or clients. In the example, only one startup control, xterm, is defined. Any other token returns an error and use the default OpenWindows startup.

If nowm is specified, the $toolwait variable sets the $OW_WINDOW_MANAGER variable (in conformance with the standard OpenWindows method of specifying an alternate window manager) to the colon. This results in no window manager being executed when the shell interprets the colon as a null command.

If you modify the $toolwait variable when there is a window manager running, the $toolwait program is invoked to start xterm (which runs in the background). When no window manager is running, the last client started by gotoken-init must not run in the background, or the GlobalInit program thinks that the session is over and shuts down the X server. Conditionally running the toolwait program solves this problem.

Structure of dtgotokens Directory

The dtgotokens directory (/usr/dt/config/dtgotokens) contains subdirectory names that match the possible values for the startup control in $GG_TOKEN. Each subdirectory contains the files necessary to start a CDE session with the X applications that are appropriate. The example directory, xterm, starts a single xterm window.

▼ To Create Additional Tokens

1. **Run a CDE session and start the appropriate clients and applications.**

2. **Exit the CDE session.**

   The session is saved in ~/.dt/ sessions. Copy the session files into the dtgotokens directory using a command similar to the following:

```
# cp -R ~/.dt/sessions /usr/dt/config/dtgotokens/sampletoken
```

   The -R argument is used to copy recursively (including subdirectories). You do not have to create the sampletoken directory before executing this command.

Remote Windowing Procedures

Configure the Netra j server by using the Netra j Network Computer Application Management module to reference remote windowing servers.

▼ To Reference Remote Windowing Servers

Note – Remote windowing servers must be accessible to the Netra j server.

1. **From the Main Administration page, under “Network Computer Administration,” click Network Computer Application Management.**

   The Network Computer Application Management page is displayed.

2. **Under “Netra Client Application Administration,” select one of the following:**
   - To reference a Citrix Windows NT server, click Citrix.
   - To reference a GO-Joe X server, click GO-Joe.
   - To install OC://WebConnect, click OC://WebConnect-Server. See “To Access the OC://WebConnect Server” on page 107 for details.

3. **Complete the form using the information in the following table.**

TABLE 4-3 Remote Windowing Information

Item	Description
Citrix Server Host Name or IP Address	The host name or IP address of the server running Windows NT.
Go-Joe Server Host Name or IP Address	The host name or IP address of the server running GlobalHost module.
Go-Joe Port Number	The port number in which the GO-Joe host server (X server) is running. The default port is 491 and should not be changed unless the port is already being used by another service.

OC://WebConnect Server

OC://WebConnect Pro™ software from OpenConnect Systems consists of OC://WebConnect 3.2.4.1 and OpenVista™ 1.0 software. It is sold and supported by Sun Microsystems Inc. Support for OC://WebConnect Pro also can be purchased directly from OpenConnect Systems.

For additional information on OpenConnect Systems software, refer to `http://www.oc.com`.

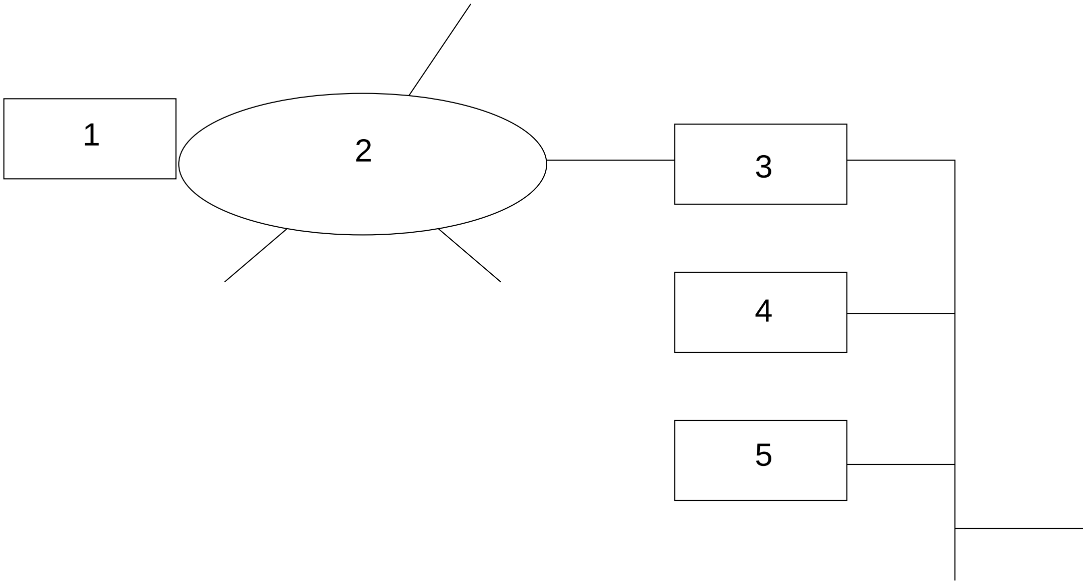


FIGURE 4-2 Network Using OpenConnect Systems Software

Legend:

1. Mainframe or AS400
2. SNA network
3. 3270 server
4. Netra j server
5. Network computer

OC://WebConnect

The OC://WebConnect software enables users on clients with the capability of using Java technology to access data and applications on IBM mainframes and on midrange computers from many vendors. OC://WebConnect is a Java applet that provides 3270, 5250, and VT220 terminal emulation with any web browser with the capability of using Java technology. OC://WebConnect adds the client-side right-to-use license for the optional OpenVista graphical user interface, which can be used to rejuvenate classic 3270/5250 “green-on-black” screens. OC://WebConnect software's unique Java version implementation provides end-to-end "persistent" and secure SNA sessions over the potentially insecure internet/intranet for information access and host data and application publishing on the web.

The following features in OC://WebConnect requires a browser with the capability of using JDK 1.1 technology. Because the quantity of new features in OC://WebConnect software increased the applet size, the user is presented with three applet options; Ultra-Lite, Enhanced, and Power User. The Ultra-Lite version is the same applet as found in WebConnect 2.6.2, with no new 3.0 functionality, and does not require a JDK 1.1 browser. The Enhanced applet includes all the functionality listed with the exception of file transfer. The Power User applet includes all of the features listed.

Security

- *Enhanced Encryption* – 128-bit encryption (Domestic Security Option), configurable for 40 or 128 Bit.
- *SSL Support* – The OC://WebConnect software uses SSL (secure socket layer) to secure connections between its emulation clients and the emulation server.

Management

- *Response Time Monitoring Statistics Support* – Support for timing marks that allow for collection of RTM statistics for use in IBM NetView/390.

Note – Requires TN3270E gateway support to extend RTM calculations past the traditional SNA boundaries.

- *Additional National Language Support* – Client-only language support for Japanese, Traditional and Simplified Chinese, and Swedish (in addition to the European languages)
- *Graphical Configuration Utility* – An interface that enables the administrator to create session files, graphically remap keyboard and colors. All configurable options are managed from this Administration console. Where appropriate, the user is prompted to select from list boxes, check boxes, radio buttons, etc.
- *Year 2000 Compliance* – OC://WebConnect is Y2K compliant.

Usability

- *Hot Spots* – Provides the ability to administer server and session configurations. Keyboard mapping, color mapping, attribute mapping, and server configuration functionality are implemented.

- *Automatic GUI* – Provides the ability to automatically convert 3270 and 5250 screens to a graphical equivalent and the generation of hot spots for the standard screens.
- *Copy & Paste* – Provides the ability to highlight portions of a screen and paste it into other applications or back into the same screen.
- *Local and 3287 Printing Capability* – Applet support for both "local screen copy" and 3287 type LU1 and LU3 printing.
- *File Transfer* – Support for `IND$FILE` from the host.

OpenVista

The OpenVista software is a cross-platform integrated development environment (IDE) for creating custom Java applets for 3270 and 5250 clients.

The OpenVista software enables the design, development, and deployment of applications for simplified enterprise information access and for legacy host-based data and application publishing on the Web. The OpenVista software enables on-the-fly development of 3270 and 5250 front-end Java applets, without any prior Java knowledge or programming experience. The OpenVista software's unique visual metaphor enables developers to create simplified user screens and environments, or to automate processes normally associated with multiple mainframe views such as logging on, finding, accessing, manipulating, and viewing information located within traditional legacy data applications and repositories.

Note – When upgrading OC:WebConnect Pro, only the session configuration files are maintained during an upgrade and all other configuration information is lost and must be reconfigured.

▼ To Access the OC://WebConnect Server

Note – The OpenConnect software must be installed before you can access it through the Netra j administration interface. It is installed if you used the Netra j installation script.

1. **From the Main Administration page, under “Network Computer Administration,” click Network Computer Application Management.**

   The Network Computer Application Management page is displayed.

2. **Under “Netra Client Application Administration,” click OC://WebConnect-Server.**

   The OC://WebConnect Administration page is displayed.

3. **Select Finish install.**

   The OC://WebConnect server language selection page is displayed.

4. **Select the server language.**

   The OC://WebConnect default sessions page is displayed.

5. **Specify the host names and port numbers for the TN servers and UNIX host.**

   The OC://WebConnect SSL configuration page is displayed.

6. **If you plan to use the OC://WebConnect server’s SSL capabilities, select Yes and click OK. If not, select No, click OK and then go to step 8.**

7. **A series of pages take you through the SSL certification generation process.**

   Refer to the online documentation for more information. After the SSL certificate is generated, the Restart OC://WebConnect Server page is displayed.

8. **Select Yes and click OK.**

   The Main OC://WebConnect Administration page is displayed.

9. **The server is minimally configured. Click on the ADMINISTRATION icon to start the OC://WebConnect GUI Configuration applet for further configuration.**

   This takes awhile; the initial password is OCS. The Help icon gives the details on the GUI configurator and on the advanced features.

To Add the OCS Icon to the HotJava Views Selector

At installation, the OC://WebConnect Pro properties are put into the `selector.apps` file located in `/opt/SUNWjdt/lib/props`. There are several `selector.desktop` files corresponding to their group located under `/opt/SUNWjdt/lib/props/`*group*`/selector.desktop`. You should add the WebConnect entry to the appropriate groups `selector.desktop` file.

Upon installation of the OC://WebConnect Pro packages, the Icon and all associated properties are added to the HotJava Views application palette automatically.

To add the OC://WebConnect icon to a group’s configuration, follow the procedure “To Add an Application Icon to the HotJava Views Selector” on page 63. Use the HotJava Browser provided with the Netra j software to administer HotJava Views. See the HotJava Views online help for additional information.

CHAPTER 5

Monitoring and Debugging Tools

This chapter describes the monitoring and debugging tools:

- “Network Computer Service Diagnostics” on page 109
- “Network Computer Debug” on page 110
- “Network Computer Monitor” on page 112

Network Computer Service Diagnostics

This tool checks the health of each of the critical network services that are required to boot and run a network computer (NC). It also validates advanced DHCP service.

The network services checked are:

- TFTP
- NFS
- DHCP
- NIS
- DNS
- HTTP

This tool checks that the service is running, that it is up, and that the configuration files are OK.

▼ To Check the Status of All Network Services

1. **From the Main Administration Page, under “Network Computer Administration,” click Network Computer Diagnostic Tools.**

   The Network Computer Diagnostic Tools page is displayed.

2. **Click Network Computer Service Diagnostics.**

   The Network Computer Services Diagnostics page is displayed.

3. **Click General network Services Status.**

   The results from polling the system are displayed.

▼ To Validate Advanced DHCP Service

The Advanced DHCP Diagnostic emulates the broadcast of a DHCP DISCOVER request from a particular NC and captures the response from every DHCP server that replies. From this list we can determine whether the local DHCP server is responding properly and if there are any other DHCP servers errantly responding to our requests.

1. **From the Main Administration Page, under "Network Computer Administration," click Network Computer Diagnostic Tools.**

   The Network Computer Diagnostic Tools page is displayed.

2. **Click Network Computer Service Diagnostics.**

   The Network Computer Services Diagnostic page is displayed.

3. **Click Advanced DHCP Service Validation.**

   The Advanced DHCP Service Validation page is displayed.

4. **Highlight the NC you plan to validate the proper operation of the DHCP service for and click OK.**

   The Responding DHCP Servers Page is displayed.This page states if the local DHCP service responded or not, and lists all the other DHCP servers responding.

5. **Click on the hostname of a responding server to view the decoded response.**

Network Computer Debug

This debug tool puts a graphical user interface (GUI) front end on the `snoop` command. It traces the data traffic in and out of a particular NC. The information helps the administrator determine the source of any boot problems. The trace data is written to a file and can be viewed at any time during the trace.

See the *JavaStation Client Software Guide* for a sample `snoop` trace with brief description.

▼ To Start a Debug Trace

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Diagnostics Tools.**

   The Network Computer Diagnostics Tools page is displayed.

2. **Click Network Computer Line Trace.**

   The Network Computer Line Trace page is displayed.

3. **Click New Trace.**

   The next Network Computer Line Trace page is displayed.

4. **Select one NC from the NC to trace list.**

5. **Enter a Trace Filename.**

6. **Select one Trace Limit:**

   - Unlimited - continues trace until you stop it
   - Time (minutes) - trace ends when time has elapsed
   - File size (KB) - trace ends when file is full

7. **Click OK.**

   The Trace Started Success page is displayed.

8. **Select either Terse or Verbose.**

   This formats the trace data, then displays it in the mode you selected.

▼ To Delete a Debug Trace

1. **From the Main Administration page, under "Network Computer Administration," click Network Computer Diagnostic Tools.**

   The Network Computer Diagnostic Tools page is displayed.

2. **Click Network Computer Line Trace.**

   The Network Computer Line Trace page is displayed.

3. **Click Delete for the selected trace.**

   The Deletion confirmation page is displayed listing the tracefile name.

4. **Click OK.**

   The listed tracefile is deleted.

▼ To Stop a Debug Trace

1. **From the Main Administration page, under “Network Computer Administration,” click Network Computer Diagnostic Tools.**

   The Network Computer Diagnostic Tools page is displayed.

2. **Click Network Computer Line Trace.**

   The Network Computer Line Trace page is displayed.

3. **Click Stop Trace for the selected trace.**

   The Stop Trace confirmation page is displayed.

4. **Click OK.**

   The trace is stopped.

Network Computer Monitor

This tool displays a table with the status of each configured NC. The attributes of an NC that can be monitored are:

- Host Name
- MAC Address
- IP Address
- IP Lease
- Lease Time Expiration
- State, Up Time
- Home Directory
- Home Directory Server
- DNS Domain
- NIS Domain
- Hardware Platform
- JavaOS Version
- JavaOS Build
- RAM Size (kilobytes)
- Desktop Application

The NC Monitor only runs in a JDK1.1 compliant browser with RMI capabilities.

You can select as many attributes to monitor and as many NCs as you want. The static information is retrieved from the DHCP configuration file server; the dynamic information is from polling each NC for its current state.

▼ To Monitor Network Computers

1. **From the Main Administration Page, under "Network Computer Administration," click Network Computer Diagnostics Tools.**

   The Network Computer Diagnostics Tools page is displayed.

2. **Click Network Computer Monitor.**

   The Network Computer Monitor page is displayed.

3. **Select one or more of the attributes listed under "Check attributes to monitor."**

4. **Select one or more of the NCs listed under "Highlight NCs to monitor.“**

5. **Click OK.**

   The table with the selected NCs and attributes is displayed.

CHAPTER 6

Printer Administration

This chapter describes how to configure print services on a Netra server.

The print services available include:

- "Local Printer Administration" on page 118
- "Network Printer Spooler" on page 120
- "Remote Printer Administration" on page 122
- "Set Default Printer" on page 124

Overview

Netra j print services are focused towards systems where no prior print services are configured.The Netra GUI provides a clear and simple interface to configure Netra print services.

- Local Printer Administration – Configure printers attached directly to the Netra Server's serial and/or parallel ports. This automatically configures the Netra server as a Solaris print server so that print jobs can be sent to the printer from the Netra server, or from clients anywhere on the network. As a print server, the Netra server is capable of scheduling, queuing, and printing jobs submitted to it either locally or from other clients on the network.
- Network Printer Spooler – A Netra j server can be configured as a Network Printer Spooler. This allows the Netra Server to become a spool server for a network printer (a printer connected directly to the network via its own network adapter). A spool server is a server that accepts and manages print jobs from print clients and submits them to the network printer. In effect, the Netra j server acts as a printer server, as far as print clients are concerned.

Note – The Network Printer Spooler feature is supported only on Netra j servers installed on Solaris 2.6. Netra j spool server capabilities apply only to new spool servers configured through the Netra administration interface, or spool servers configured according to the Solaris 2.6 documentation, (using the “netstandard” interface script).

- Remote Printer Administration – You can configure the Netra server with access to remote printers elsewhere on the network. Remote printers can be either network printers, or printers attached to other Solaris or ‘bsd’ print servers. The Netra Server can act as a print server with multiple local printers connected to it, while simultaneously accessing multiple remote printers.
- Set Default Printer – When at least one printer is configured on the system, this link will appear. This allows the Netra Administrator to configure any of the local or remote printers to be the Netra j “default printer”.

Before You Begin

Supported Print Mechanisms

The print server is based on UNIX SVR4 LP print services, which ship with the Solaris 2.5.1 and 2.6 operating environments. The Netra server can print to SunOS™ 4.1.x (standard BSD printing), Solaris 2 and subsequent compatible releases (standard LP or SVR4 printing) remote print servers, and any network printer that conforms to these print models. It can also service requests sent from clients running SunOS 4.1.x, and Solaris 2 and subsequent compatible releases; since it also runs a BSD listener, it can receive jobs from remote hosts running Solaris 1, other types of UNIX, and any client capable of using the BSD print mechanism.

If You Have an Existing Setup...

When installing Netra j software onto a system that is already configured with a local printer, or is already configured as a print network spooler to a network printer, caution is advised. Print services available to the Solaris environment include many third-party software packages. Netra should not interfere with existing network printer spoolers configured on the system prior to the Netra j software installation. However, continue to administer these printers with the third-party administration tool, rather than through the Netra j interface.

When installing Netra j software onto a system that is already configured for access to remote printers, you can safely administer this printer access from the Netra j interface.

Solaris 2.6 and NIS Considerations

On Netra j servers that are running the Solaris 2.6 operating environment, printer administration behaves slightly differently, depending on whether the Netra j server is configured as a NIS client or as a NIS master server.

- NIS client

As a NIS client, the Netra j administration interface displays a list of printers configured ONLY on the local system. Any information about remote printers and print servers that is broadcast by a remote NIS server is not displayed through the Netra j administration interface. However, such printers are still available for printing from the Netra j server using standard Solaris commands.

As a NIS client, the Netra j server does not broadcast its `/etc/printers.conf` file as a NIS `printers.conf.byname` map.

One method NCs use to access printers is by specifying a NIS `printers.conf.byname` map. Since no such map exists on the Netra j server when configured an a NIS client, the NCs can NOT use this method to access the Netra j locally configured printers. An alternative method does exist (see the printing properties section in the *JavaStation Client Software Guide*) where you explicitly specify the server name and printer name. In this case, the server name is the name of the Netra j server, and the printer name is the name of the locally configured printer.

To provide access to the Netra j printers, include information about those printers in the network NIS server `printers.conf` file. That way, the NCs can use all NIS printers, which will include the printers configured locally on the Netra j server.

- NIS master server

As a NIS master server, the Netra j server makes the `etc/printers.conf` file into a NIS map so that NCs and other clients on the same NIS domain have access to the Netra j printer configuration information.

Note – There CANNOT be another NIS `printers.conf` file on the same NIS domain; this confuses the Netra j printer administration.

Local Printer Administration

▼ To Add a Local Printer

1. **From the Main Administration page, under "Network Service Administration," click Printer Administration.**

2. **Under "Local Printer Administration," choose one of the following**:
   - Add Printer to Serial Port a
   - Add Printer to Serial Port b
   - Add Printer to Parallel Port

3. **Complete the form using the information in the following tables.**

TABLE 6-1 Printer Characteristics

Option	Description
Printer Name	Enter a printer name with up to 14 characters (A–Z, a–z, 0–9,-,_). Do not start the printer name with "-" or "_".
Printer Type	Choose PostScript, ASCII, HP (PCL ASCII), HP(PCL), or Unknown for a printer that is not listed. See TABLE 6-2 for more detail.
File Contents	Choose PostScript, ASCII, or Any. Use Any for a printer that is not PostScript or ASCII.
Fault Notification	Choose Console (print fault messages to console), Root Mail (email fault messages to root), or none (do not send fault notification messages).
Description (optional)	Enter an optional description of the printer (up to 28 characters).
Enable BannerControl?	Specify whether banner page control is enabled.

TABLE 6-2 Printer and Content Type

Printer Type	Content Type
PostScript	PostScript
ASCII	ASCII

TABLE 6-2 Printer and Content Type

Printer Type	Content Type
HP Laserjet (PCL ASCII)	ASCII
HP Laserjet (PCL)	ASCII
Unknown (All other printers)	Any

4. **When adding a printer to a serial port, also specify the serial port baud rate, parity, and character size to match those of the printer.**

TABLE 6-3 Serial Port Attributes

Option	Description
Baud Rate	Choose 9600, 19200, or 38400.
Parity	Choose none, even, or odd.
Character size	Choose 7 bits, or 8 bits.

5. **Click OK.**

▼ To Modify or Delete a Local Printer

1. **From the Main Administration Page, under "Network Service Administration," click Printer Administration.**
2. **Under "Local Printer Administration," choose one of the following:**
   - To modify a local printer, click Modify, and make the changes in the form use the information in TABLE 6-1, TABLE 6-2, and TABLE 6-3.
   - To delete a local printer, click Delete, and then confirm the operation.

   Choose from the following options:

   - Modify or Delete Printer *Printer name* attached to Serial Port a
   - Modify or Delete Printer *Printer name* attached to Serial Port b
   - Modify or Delete Printer *Printer name* attached to Parallel Port

Note – If you do not know what printer type and file content type to use, or if you think that your printer is not one of the specified types, then choose Printer Type: Unknown and Content Type: Any. Then Netra makes no assumptions about the printer or the files being printed. However, if you are sure that your application is submitting a print job of the correct format to the printer, it should print without trouble.

Network Printer Spooler

Note – This option is only for servers that run on the Solaris 2.6 operating environment.

This option enables the Netra j server to be set up as a network printer spooler. This means that the Netra j server accepts, queues, and manages print jobs for a network printer (in other words, a printer with a built-in network adapter attached directly to the network with its own host name and IP address).

Configuration is compatible with new functionality added to the LP print model for Solaris 2.6, and uses the new “netstandard” interface script developed for Solaris 2.6 to manage Network Printers.

Note – Netra j does not display third-party printer configurations. Any existing or subsequently configured third-party network spoolers on a Netra j server need to be managed through the supplied third-party software. Netra j Printer Administration does NOT interfere with third-party printer configurations.

Currently, the Network Spooler form prompts for Network Printer Access Name. There is no default format for this field; it is dependent on the printer model and network configuration. In most cases, and in the case of TCP/IP networks in particular, enter either the printer name, or IP address of the network printer in this field. This is most likely sufficient information to establish connectivity with the printer. Some printers can require specification of a TCP port number also. In this case, after the printer name or IP address, add a colon (:), followed by the port number. If difficulties remain, contact the printer manufacturer regarding the correct format of the Network Printer Access Name.

▼ To Add a Network Printer Spooler

1. **From the Main Administration Page, under “Network Service Administration,” click Printer Administration.**

2. **Under “Network Printer Spooler Administration,” click Add Network Printer Spooler.**

3. **Complete the form using the information in the following table.**

TABLE 6-4 Network Printer Spooler Attributes

Option	Description
Printer Name	Enter a printer name with up to 14 characters in the range (A–Z, a–z, 0–9,-,_). Do not start the printer name with “-” or “_”
Network Printer Access Name	Enter the Network Printer Access Name. Usually this is the same as the printer name, or the IP address of the printer. However, there is no default format for this field. Contact the printer vendor for the correct format of this field if difficulties arise.
Protocol	Set the over-the-wire protocol used to communicate with the printer. Both BSD and raw TCP are supported.
Retry timeout	Sets the retry timeout value that represents a number of seconds to wait between attempting connections to the printer.
Printer Type	Choose PostScript, ASCII, HP (PCL ASCII), HP (PCL), or Unknown for a printer that is not listed.
File Content type	Choose PostScript, ASCII, or Any for a printer that is not PostScript or ASCII.
Fault Notification	Specify how printer error messages are treated. Choose Console (print fault messages to console), Root Mail (email fault messages to root), or none (do not send fault notification messages).
Description (optional)	Enter a description of the printer (up to 28 characters).
Enable Banner Control	Enable/Disable the ability of the user print command to specify whether a banner page is printed.

▼ To Modify or Delete a Network Printer Spooler

1. **From the Main Administration Page, under “Network Service Administration,” click Printer Administration.**

2. **Under “Network Printer Spooler Administration,” choose one of the following:**

- To modify a network printer spooler, click Modify for the appropriate spooler, and make changes in the form using TABLE 6-4 as a reference.
- To delete a network printer spooler, click Delete for the appropriate spooler, then confirm the operation.

Remote Printer Administration

Remote Printer Administration provides a way of adding access to remote printers on the Netra j server. Any remote printer configured through the Netra j administration interface is added to the local printer configuration files.

Note – For a Netra j server installed on Solaris 2.6, and configured as a NIS client, a remote NIS server may be already broadcasting remote printer access for certain printers. In this case, Netra j detects the presence of such printers, and DOES NOT allow them to be configured again through the Netra j administration interface. This would lead to potential inconsistencies in information stored in the local printer configuration file with that being broadcast by the remote print server. Even though you cannot configure such printers through the Netra j administration interface, access to print to the remote printers is still available in the normal way and to all applications. To convince yourself that these printers are available, execute the command `lpstat -v` on a shell command line.

▼ To Add Access to a Remote Printer

1. **From the Main Administration Page, under "Network Service Administration," click Printer Administration.**

2. **Under "Remote Printer Administration," click Add access to Remote Printer.**

3. **Complete the Add Remote Printer form using the information in the following table.**

TABLE 6-5 Remote Printer Attributes

Option	Description
Printer Name	Enter a printer name with up to 14 characters in the range (A–Z, a–z, 0–9,-,_). Do not start the printer name with "-" or "_". The printer name must correspond to a known printer on the network, either a network printer (a printer attached directly to the network that knows its own host name and IP address), or a printer attached to another Solaris or BSD print server.
Print Server Name	The print server name must correspond to a known host on the network, and the host name must be resolvable to its IP address. To do this, add the *hostname - IP address* pair to the `/etc/hosts` file through the Local Name Services module. Alternatively, if the Netra j server is a NIS client in a NIS domain, confirm that the print server host name is registered with the NIS server for that domain. The print server corresponds to one of three types of hosts: • If the print server is a remote host with a printer attached locally to it, then the print server name is the name of the remote host. • If the print server is a network printer, the print server name is the same as the printer name. • If the print server is a network print spool server for a network printer, then the print server name entered is the name of the network print spool server.
Description (optional)	Enter a description of the printer (up to 28 characters).

4. **Click OK.**

▼ To Modify or Delete Access to a Remote Printer

1. **From the Main Administration Page, under "Network Service Administration," click Printer Administration.**

2. **Under "Remote Printer Administration," choose one of the following:**

   - To modify a remote printer, click Modify for the appropriate printer, and make changes in the form using TABLE 6-5 as a reference.

- To delete a remote printer, click Delete for the appropriate printer, and then confirm the operation.

Set Default Printer

When at least one local or remote printer has been configured on the system, the 'Set Default Printer' option is available on the Printer Administration main page.

Netra printer administration sets a system-wide default printer.

However, there are a number of ways for individual users to override this value: by using a `~/.printers` file; by setting the `LPDEST` environment variable; or by setting the `PRINTERS` environment variable. Once any of these are set, an `lpstat -d` reveals their value for the default printer, not the one quoted in `/etc/printers.conf`.

If the system contains a `/etc/printers.conf` file, and there is also a NIS `printers.conf` file available, the NIS default value may be the one used.

If the user unsets the LPDEST, PRINTERS variables and removes the `~/.printers` file, then the Netra setting of default printer is the one quoted by lpstat -d.

▼ To Set the Default Printer

1. **From the Main Administration Page, under "Network Service Administration," click Printer Administration.**
2. **Under "Set Default Printer," click Set Default Printer.**
3. **Select the printer you want to be the default printer from the list.**
4. **Click OK.**

CHAPTER 7

Using Network Connection Administration

This chapter describes how to configure the different network connections available:

- “Local Area Network Administration” on page 125
- “Modem Administration” on page 127
- “Routing Administration” on page 133
- “ATM Administration” on page 137
- “High-Speed Serial Interface” on page 143
- “ISDN Administration” on page 145

Local Area Network Administration

This section describes how to configure the local area network (LAN) interfaces on your Netra server.

Note – The Netra software only displays information about network interface hardware that is currently attached to the Netra server.

A network interface consists of three elements: the network port, the network protocol, and the interface definition.

- Network port – The *network port* provides the physical link between machines that comprise a network. Ports can be built into the Netra server, or they can be provided by SBus or PCI cards in the server. The Netra server supports the following types of network hardware:
    - Lance Ethernet
    - Fast Ethernet
    - Fast Ethernet 100BASE-T

  - Quad Fast Ethernet
  - Token Ring
  - Fiber Channel (FDDI)
- Network protocol – The *network protocol* defines the communication that travels over the network. The Netra server supports TCP/IP network protocols. The TCP/IP network protocol suite supports the definition of multiple interfaces for a network hardware port and network protocol.
- Interface definition – The interface definition is the configuration information that is specific to the Netra server. For example, the Netra server requires host addresses for TCP/IP interfaces.

Note – If no network interface is configured, or if the network interface is improperly configured, the Netra server has difficulty rebooting.

▼ To Add a Network Interface

You cannot administer the Netra server from a remote client without first defining the network interface.

1. **From the Main Administration page, under "Network Connection Administration," click Local Area Network.**

   The Local Area Networking Administration page is displayed with a list of network interface hardware to configure.

2. **Click Add a TCP/IP Interface for the required network interface.**

   An administration page for the selected interface and protocol is displayed.

3. **Complete the form using the information in the following table.**

TABLE 7-1 Network Interface Administration: TCP/IP

Option	Description
Host Name/Address	The host name and address for the network interface. This address should not be on the same network as any other configured interface. Example: 129.144.79.5
Netmask	The netmask address that determines the network with which the host address is associated. Example: 255.255.255.0

4. **Click OK.**

▼ To Modify a Network Interface

1. **From the Main Administration page, under "Network Connection Administration," click Local Area Network.**

   The Local Area Networking Administration page is displayed with a list of network interface hardware to configure.

2. **Click Modify a TCP/IP Interface for the required network interface.**

   An administration page is displayed with existing configuration information for the selected interface and protocol.

3. **Complete the form using the information in** TABLE 7-1**.**

4. **Click OK.**

▼ To Delete a Network Interface

1. **From the Main Administration page, under "Network Connection Administration," click Local Area Network.**

   The Local Area Networking Administration page is displayed with a list of network interfaces to delete.

2. **Click Delete for the interface you want to remove, then confirm the operation.**

Modem Administration

This section describes how to set up a point-to-point protocol (PPP) link between the Netra server and a remote host using a modem.

PPP enables two computers to be connected over a two-way communications link. The connection is established as needed. Using the Netra j interface, you can administer connections to a remote host system (for example, your ISP) using PPP. The following PPP protocol options are supported:

- Dynamic assignment of your Netra system's host address
- Addition of the remote system's host address to your routing table

Connecting to a Remote Host Using a Modem

To connect to a remote host using a modem and PPP do the following general tasks:

1. Define a modem.

Examine the existing modem definitions in the Netra server using the View modem definitions option described on page 129. If an initialization definition for your modem has already been created, skip this task. If not, add an initialization definition and a unique name for your modem using the Add a modem definition option described on page 128.

2. Assign the modem to a port.

Your modem must be physically connected to the Netra server on one of the serial ports. Assign your modem to a specific port by using "Modem Port Assignments" on page 129.

3. Add a remote host connection.

After you assign a modem to a serial port, set up a connection to a remote host using "Connecting to a Remote Host Using a Modem" on page 127. (Note that this option is not displayed until at least one modem is assigned to a port.)

Modem Definitions

Note – The Netra server defines 33 modems. You cannot change these definitions or use any of them as your modem name.

▼ To Add a Modem Definition

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Under "Modem Definitions," click Add a modem definition.**

   The Add a Modem Definition page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 7-2 Adding/Modifying a Modem Definition

Option	Description
Modem Name	The name associated with the modem. The name must be unique. It must start with a letter, and can include letters, digits, hyphens, and underscores up to 12 characters. Example: *myhayes*
Initialization String	The string passed to the modem when the connection to it is first established. Example: `\" AT\r\c\ OK ATM1L)\r\c OK ATDT\D\r\c CONNECT\"`

▼ To View Modem Definitions

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Under "Modem Definitions," click View modem definitions.**

   A list of definitions is displayed in a scrolling window. The modems you defined are shown under Your modem definitions; the system-defined modems are listed next under System modem definitions.

▼ To Modify or Delete a Modem Definition

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Choose one of the following.**

   - To modify an existing modem definition, click Modify, and complete the form using the information in TABLE 7-2 as a reference.
   - To delete a modem definition, click Delete, and then confirm the operation.

Modem Port Assignments

You can assign a modem to a serial port using the Network Connection Administration page.

▼ To Assign a Modem to a Serial Port

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Under "Port Assignments," click Assign a modem to Port *x*.**

   (Choose the port to which your modem is connected.)

   The Modem Port Assignment page is displayed with current port assignments.

3. **From the scroll list, select the name of the modem connected to the port (see the following table).**

TABLE 7-3 Modem Assignments

Option	Description
Modem assigned to port x	All modems are listed, including those defined by the system. "No modem" is not a valid selection if the port is in use by a remote host. If you do not assign modems to any ports, you cannot make a remote connection.

Remote Host Connections

Note – You must assign a modem to a port before the "Add a remote host connection" option becomes available.

▼ To Add a Modem Remote Host Connection

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Complete the form using the information in the following table.**

TABLE 7-4 Modem Remote Host Administration

Option	Description
Remote Host Address	The host address of the system at the other end of the PPP connection (presumably the ISP). Example: 129.144.102.6
Local Host Address	The host address of the Netra server. Example: 129.144.102.27 If the remote host assigns the host address dynamically, enter `dynamic` in this field.
Phone Number	The phone number for the remote host. Example: 17005554141
Login String	The UUCP-style chat script used to log in to the remote PPP server once the modem connection is established. Example: `\" in: LOGIN\r\c word: PASSWORD\r\c\"`
Timeout (minutes)	The time, in minutes, after which an idle connection is terminated.
Use Remote Host As Default Route	Select this option if you want the remote host address to be added to the route table as the default destination. This default route is removed when the connection is terminated.
Serial Port Name	The name of the serial port on the Netra server through which to connect to the remote host. Choices: ports that have connected modems.
Connection Speed	The bits-per-second speed at which the serial port on the Netra server should communicate with the modem.

▼ To Modify or Delete a Remote Host Connection

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Choose one of the following:**

   - To modify an existing remote host connection, click Modify, and complete the form using the information in TABLE 7-4 as a reference.
   - To delete a remote host connection, click Delete, and then confirm the delete operation.

Modem Log Files

You can change, view or delete modem log files using the Network Connection Administration.

▼ To Change the Log File Detail Level

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Under "Modem Log file," click Change log file detail level.**

   The Change Modem Log File Detail Level page is displayed.

3. **Choose a level of detail (see the following table):**

TABLE 7-5 Modem Log File Detail Levels

Option	Description
Log File Detail Level	• errors only • minimal information • some uucp chat script information • all uucp chat script information • maximum uucp information • PPP message traces • everything, including IP packets

4. **Click OK.**

▼ To View or Clear the Log File

1. **From the Main Administration page, under "Network Connection Administration," click Modem.**

   The Modem Administration page is displayed.

2. **Choose one of the following options:**

   - To view information in the log file, click View log file.
   - To clear information in the log file, click Clear log file, and then confirm the operation.

Routing Administration

This section describes how to configure the Netra server as a router.

Routing is the mechanism by which systems on different networks can communicate with each other. Each network usually has at least one system called a *router*. A router is a system that is connected to multiple networks; it maintains information that defines routes between host systems and networks.

The Netra system can be configured as one of the following:

- A dynamic router
- A static router
- Not a router

Dynamic Router

A *dynamic router* relies on information broadcast from other routers to update its routes and reflect changes in the network topology. It also broadcasts this information to other dynamic routers.

Dynamic routers are typically required when systems act as gateways between networks or within large networks where route information is constantly changing. The Netra server supports the following dynamic routing protocols:

- The Xerox NS Routing Information Protocol (RIP)
- The ICMP router discovery protocol

If client host systems are required to use the dynamic router, they must either run programs that can communicate using these protocols, or they must specify the dynamic router as a default router.

When the Netra server is configured as a dynamic router, broadcasting RIP information over point-to-point (PPP) links can be enabled or disabled. If additional PPP links are defined after the dynamic router is configured, you must reconfigure the dynamic router to ensure that it is aware of the new links.

▼ To Configure the Netra System as a Dynamic Router

1. **From the Main Administration page, under "Network Connection Administration," click Routing.**

   The Routing Administration page is displayed.

2. **Click Configure dynamic router.**

   The Dynamic Router Administration page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 7-6 Dynamic Router Administration

Option	Description
Host/Net	Specify if a destination address is a Network or a Host. If a value of "net" is entered incorrectly, the system attempts to add the routing entry as a "host."
Destination Address	Network/Host address to which information is routed.
Gateway Host Address	Host address of the gateway used for accessing the destination address. If the router is unreachable when this form is configured, it is not used for routing until dynamic routing is reconfigured or the Netra system is restarted.
Hop Count	A value of 0 or greater. 0 means the Netra server is the router; a value greater than 0 means that another system is the router.
Status	Active or Passive. Gateways marked "active" are removed from the routing information if they become inaccessible. Gateways marked "passive" are part of the routing information until explicitly removed. Routes to passive gateways are also not broadcast to the other systems on the network.
Dynamic Routing Information over Point-to-Point Links	Enables or disables RIP over PPP links. Choices: Yes or No.

4. **Click OK.**

▼ To Modify a Dynamic Router

1. **From the Main Administration page, under "Network Connection Administration," click Routing.**

   The Routing Administration page is displayed.

2. **Click Modify dynamic router.**

3. **Complete the form using the information in** TABLE 7-6**.**

Static Router

A *static router* relies on the manual addition of routes. Routing information is not exchanged with other routers.

Static routers are typically used in very stable, simple networks. An example of such a network would be a single LAN connected to the Internet or to another network over a PPP link.

If machines on the LAN require a static router, it must be specified as a default router.

▼ To Configure the Netra System as a Static Router

Note – Before using static routing over PPP links, configure a PPP connection to the remote host using "Modem Administration" on page 127, and add a static route to the remote host's host address (IP address).

---

1. **From the Main Administration page, under "Network Connection Administration," click Routing.**

   The Routing Administration page is displayed.

2. **Click Configure static router.**

   The Static Router Administration page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 7-7 Static Router Administration

Option	Description
Default Router Host Address	Host address of the default router for the network.
Host/Net	Specify whether a destination address is a Network or a Host. If a value of "net" is entered incorrectly, the system attempts to add the routing entry as a "host."

TABLE 7-7 Static Router Administration

Option	Description
Destination Address	Network/Host address to which information is routed.
Router Host Address	Host address of the router used for accessing the destination address.
Hop Count	A value of 0 or greater. 0 means the Netra server is the router; a value greater than 0 means that another system is the router.

Note – If a host address is unreachable at the time of configuration, it is accepted with a warning that the route cannot be accessed. To activate the route once it can be accessed, restart the Netra System, or reconfigure he static router.

▼ To Modify a Static Router

1. **From the Main Administration page, under "Network Connection Administration," click Routing.**

   The Routing Administration page is displayed.

2. **Click Modify static router.**

3. **Complete the form using the information in** TABLE 7-7**.**

Setting a Default Route Over a PPP Link

If you require a default route over a PPP link, choose one of the following options:

- If both local and remote host addresses are statically assigned, you can use either of them as the default route.
- If the remote host address is dynamically assigned, use the local host address as the default route.
- If the local host address is dynamically assigned, use the remote host address as the default route.

If both the local and the remote host addresses are dynamically assigned, you cannot use a default route over a PPP link.

Not a Router

A non-gateway system need not be a router in networks that already have dynamic routers. The Netra server listens for dynamic routers to broadcast route information using the RIP and the ICMP router discovery protocols.

▼ To Configure the Netra System as Not a Router

Note – Once the Netra server is already configured as "not a router," this option is not displayed.

1. **From the Main Administration page, under "Network Connection Administration," click Routing.**

   The Routing Administration page is displayed.

2. **Click Turn off routing, then confirm the operation.**

ATM Administration

This section describes how to set up a connection to an asynchronous transfer mode (ATM) network.

Note – This option is displayed on the Main Administration page only if the relevant hardware and software has been installed. (See system's hardware installation manual for instructions on adding network interface hardware. See *Netra System Administration* for software installation instructions.)

ATM Requirements

ATM is a connection-oriented network protocol. To use this protocol, two communicating entities must establish a connection before data transfer can begin. The Transport Control Protocol/Interface Program (TCP/IP), on the other hand, is inherently connectionless.

The SunATM™ 2.1 software supports two protocols that reconcile the differences between the ATM and TCP/IP paradigms:

- Classical Internet Protocol (IP) interface
- LAN Emulation interface

Both these protocols enable TCP/IP to run transparently over an ATM interface by resolving an IP address to an ATM address and establishing the connection to the host to which a message is addressed.

The Netra ATM administration module supports SunATM version 2.1 software and SunATM-155 version 2.1 hardware. (The SunATM-155/Mfiber SBus Adapter 2.1 and SunATM-155/UTP5 SBus Adapter 2.1 are single-wide SBus adapters that conform to the specifications of the ATM Forum.)

Classical Internet Protocol Interface

Classical IP supports the TCP/IP and the User Datagram Protocol/Interface Program (UDP/IP) protocols in an ATM environment. An ATM address resolution protocol (ATM ARP) server replaces the traditional ARP protocol by resolving IP addresses to ATM addresses. It is accessible to all hosts on a subnet. Each host must register with the ARP server when the ATM interface is brought up.

Classical IP has the following limitations because it does not support broadcast and multicast messaging.

- Running NIS or NIS+ over Classical IP requires configuration beyond the scope of the ATM module and is not supported.
- The Routing Information Protocol (RIP) and the Router Discovery Protocol are not supported. Thus, to route over an ATM network using a Classical IP interface, the Netra server must be configured as a static router. Routes to the routers in the ATM subnet must be explicitly added.

Each ATM port (SBus card) on the Netra server supports only one Classical IP interface.

LAN Emulation Interface

LAN Emulation, which provides mechanisms to send broadcast messages, is another way of supporting the TCP/IP and UDP/IP protocols over an ATM network. A series of LAN Emulation services (such as the LAN Emulation Configuration Server -LECS-, the LAN Emulation Server -LES-, and the Broadcast and Unknown Server -BUS-) provide address resolution information. When a LAN Emulation interface is brought up, it joins the LAN by registering with these services. The LAN Emulation protocol provides a broadcast service to the upper layer protocols. Therefore, a LAN Emulation interface is not affected by the multicast and RIP limitations of Classical IP.

Each ATM port on the Netra server currently supports only one LAN Emulation interface.

Configuring ATM Interfaces

To configure ATM interfaces on the Netra server, you must perform the following general tasks:

1. Set the type of framing interface.

ATM switches use either the Synchronous Digital Hierarchy (SDH) or the Synchronous Optical NETwork (SONET) framing interface. (The framing interface used by the ATM switch should be in the switch product information.) Set the framing interface type using the Change Framing Interface option, as described on page 139.

2. Set the User Network Interface (UNI) version for each ATM port.

Each ATM port must be configured with a User Network Interface version. This version applies to all Classical IP and LAN Emulation interfaces configured on that port. Each port can be configured with a different version. Set the UNI version using the Change User Network Interface Version option, as described on page 140.

3. Configure a Classical IP and/or a LAN Emulation interface for each ATM port.

Use the Configure a Classical IP Interface and Configure a LAN Emulation Interface options described on page 140 and page 142.

Framing Interface

▼ To Set the Framing Interface

1. **On the Main Administration page, under “Network Connection Administration,” click ATM.**

   The ATM Administration page is displayed with the current switch and port configuration information.

2. **Click Change Framing Interface.**

3. **Choose the type of framing interface. See the following table.**

   Choose either SONET, or SDH. The Netra default is SONET.

4. **On the Main Administration page, under “System Administration,” click Restart and Shutdown to restart the Netra server.**

User Network Interface

▼ To Set the User Network Interface Version

1. **On the Main Administration page, under “Network Connection Administration,” click ATM.**

   The ATM Administration page is displayed with configuration information for each port.

2. **Click Change User Network Interface for the required ATM port.**

3. **Choose the version number.**

   Specify the version (either 3.0 or 3.1) of the User Network Interface (UNI) used for signaling. The default is 3.0.

4. **Restart the Netra server on the Main Administration page, under “System Administration,” click Restart and Shutdown.**

Classical IP Interface

▼ To Configure a Classical IP Interface

1. **On the Main Administration page, under “Network Connection Administration,” click ATM.**

   The ATM Administration page is displayed with configuration information for each port.

2. **Click Configure a Classical IP interface for the required ATM port.**

   An administration page for the chosen interface is displayed.

3. **Complete the form using the information in the following table.**

TABLE 7-8 Information for ATM Classical IP Interface

ARP Configuration	The server or client ARP configuration. Choose either Server, Client, or Standalone. Standalone enables a back-to-back configuration.
ARP Server Prefix	The 13-byte prefix of the ARP server switch. If the ARP server is on the same switch as the Netra server, no entry is required. If there is no entry in this field, the local switch prefix is used. This field is required only when the ARP Configuration field is set to Client.
ARP Server Address	The 7-byte local portion of the ATM address of the ARP server. If no server is specified, the default local server is used. (There are also 256 addresses reserved by Sun: SUNMACSEL0-255.) This field must remain blank if the ARP Configuration field is set to Standalone.
Remote Host Address	The remote host address for the machine to which the Netra server is connected. The remote host address and the host address must be on the same subnet. This field is required only when the ARP Configuration field is set to Standalone.
Host Address	The host address for the network interface. This address should be unique on the system.
Netmask	The netmask address that determines the network with which the host address is associated. Example: 255.255.255.0

If no remote host configurations are defined in the ATM module, the following message may be displayed on the console when the Netra server is restarted.

```
cannot find atmconfig file in /etc; exiting S60sunatm
```

This message can be ignored.

4. **On the Main Administration page, under “System Administration,” click Restart and Shutdown to restart the Netra server.**

▼ To Modify or Unconfigure a Classical IP Interface

1. **On the Main Administration page, under "Network Connection Administration," click ATM.**

   The ATM Administration page is displayed with configuration information for each port.

2. **Choose one of the following.**
   - To modify a Classical IP interface, choose Modify for the required interface, and make the changes in the form using TABLE 7-8.
   - To unconfigure a Classical IP interface, choose Unconfigure for the interface to be removed; then confirm the operation.

3. **On the Main Administration page, under "System Administration," click Restart and Shutdown to restart the Netra server.**

Configuring a LAN Emulation Interface

▼ To Configure a LAN Emulation Interface

1. **On the Main Administration page, under "Network Connection Administration," click ATM.**

   The ATM Administration page is displayed with configuration information for each port.

2. **Click Configure a LAN Emulation Interface.**

   An administration page for the chosen interface is displayed.

3. **Complete the form using the information in the following table.**

TABLE 7-9 Information for ATM LAN Emulation Interface

LAN Name	The name of an emulation LAN to join.
Host Address	The host address for the network interface. This address should be unique on the system.
Netmask	The netmask address that determines the network with which the host address is associated. Example: 255.255.255.0

4. **On the Main Administration page, under "System Administration," click Restart and Shutdown to restart the Netra server.**

▼ To Modify or Unconfigure a LAN Emulation Interface

1. **On the Main Administration page, under "Network Connection Administration," click ATM.**

   The ATM Administration page, with configuration information for each port, is displayed.

2. **Choose one of the following.**
   - To modify a LAN emulation interface, choose Modify for the required interface, and make the changes in the form using TABLE 7-9.
   - To unconfigure a LAN emulation interface, choose Unconfigure for the interface to be removed; then confirm the operation.

3. **On the Main Administration page, under "System Administration," click Restart and Shutdown to restart the Netra server.**

High-Speed Serial Interface

Note – This option is available only if the relevant hardware and software has been installed. (See the system's hardware installation manual for instructions on adding network interface hardware.)

▼ To Configure a Port for PPP

1. **On the Main Administration page, under "Network Connection Administration," click High-Speed Serial Interface.**

   The High-Speed Serial Interface page, with configuration information for each port, is displayed.

2. **Click Configure for PPP for the required port.**

   The High-Speed Serial Interface Administration page for the chosen port is displayed.

3. **Complete the form using the information in the following table.**

TABLE 7-10 Information for the High-Speed Serial Interface

Option	Definition
Local Host Address	The host address of the HSI interface, provided by the Internet Service Provider.
Local Netmask	Netmask of the LAN
Remote Host Address	The host address of your Internet Service Provider.
Line Speed	The line speed of the modem or CSU/DSU. This value must match that of the modem or CSU/DSU. For example, 1536000
Clocking	Selecting external clocking specifies that the incoming transmit clock is used. Selecting internal clocking specifies that Netra server's internal clock is used.

4. **On the Main Administration page, under "System Administration," click Restart and Shutdown to restart the Netra server.**

▼ To Modify or Unconfigure a Port for PPP

1. **On the Main Administration page, under "Network Connection Administration," click High-Speed Serial Interface.**

   The High-Speed Serial Interface page, with configuration information for each port, is displayed.

2. **Choose one of the following.**

   - To modify a high-speed serial interface, choose Modify for the required port, and make the changes in the form using TABLE 7-10.
   - To unconfigure a high-speed serial interface, choose Unconfigure for the port to be unconfigured; then confirm the operation.

3. **On the Main Administration page, under "System Administration," click Restart and Shutdown to restart the Netra server.**

ISDN Administration

Note – This option is available only if the relevant hardware and software has been installed. (See the system's hardware installation manual for instructions on adding network interface hardware.)

▼ To Add a Remote Host Connection

1. **On the Main Administration page, under "Network Connection Administration," click ISDN.**

   The ISDN page is displayed.

2. **Click Add a remote host connection.**

   The Add Remote Host Connection page is displayed

3. **Enter the information in the form using the following table.**

TABLE 7-11 Information for Remote Host Connection

Option	Description
Remote Host Address	The host address of the peer side of the ISDN point-to-point link.
Local Host Address	The host address of the local side of the ISDN point-to-point link. Setting this field to the keyword "dynamic" turns on the negotiate address feature
Netmask	The number that masks the host component of a host address and thus shows how to divide the network component of the host address into subnetworks.
Inactivity Timeout	The number of minutes an ISDN connection is allowed to idle before it is disconnected.
Host Setup Timeout	The number of minutes allowed before an ISDN connection request ceases its attempt to connect to the remote system.
Default Route	The route entry that allows connections to unspecified hosts to go through this connection. The default route is created when the connection is made with the remote system; it is deleted when that connection is terminated or timed out. Choose On, or Off.

TABLE 7-11 Information for Remote Host Connection *(Continued)*

Option	Description
Bandwidth Controller	The side of the connection that is controlling the number of ISDN links used on the connection. Only one side can be on at a time. Choose On, or Off.
Encapsulation	The encapsulation protocol used in data transfers. For multilink PPP (MP), the control protocol may or may not be encapsulated. Ascend boxes require control encapsulation, others typically do not. Choose PPP, MP-Ascend, or MP-Other.
Data Compression	Turn data compression on. Note: Encapsulation must be set to one of the MP options.
Local Authentication	The authentication mechanism used by the Netra to authenticate incoming calls. Chap Authentication Protocol (CHAP) uses encryption-based password control. Password Authentication (PAP) is similar to CHAP. Choose chap, pap, or off.
Remote Authentication	The authentication protocol that is used with remote systems. Choose chap, pap, or both.
ID String	The login string used by the authentication protocol.
Password	The password string used by the authentication protocol.
Caller ID	If the incoming call presents its caller ID number, this number is used to find an isdn_path for the incoming call. Choose On, or Off.
Channel Baud Rate	The B-channel baud rate. Choose data56, or data64.
Hunt Mode	Sequentially dial through the phone numbers listed for a remote host, until a connection is made or until the list is exhausted.
Phone Number 1	The phone number to dial to reach the system at the other end of the ISDN connection. Example 17005554141.
Phone Number 2	An alternate phone number to dial to reach the system at the other end of the ISDN connection. This phone number need only be entered if supplied by the remote system.

▼ To Configure a Local Port

1. **On the Main Administration page, under “Network Connection Administration,” click ISDN.**

   The ISDN page is displayed.

2. **Click Configure for the required port.**

   The Configure ISDN Port page is displayed

3. **Complete the form using the information in the following table.**

TABLE 7-12 Information for ISDN

Option	Description
Switch Type	Specifies the type of switch to which your ISDN line is connected. This information is available from your phone company or Internet Service Provider (ISP). Choices: • au1 (Australia) • vn3, vn6 (France) • 1tr6 (Germany) • ntt (Japan) • bt2 (United Kingdom) • dms, 5ess, ni2 (North America) • etsi (Europe) • swd-etsi (Sweden) • htk (Hong Kong)
Force 56kb	Forces the ISDN line to a 56Kb transfer rate regardless of how the incoming call identifies itself. This is mainly used to solve incompatibility problems between switches.
Calling Line Identify	Enables or disables exchange service (if available) where the exchange verifies that the local calling number is the phone number of the calling system.
ISDN Number	Your ISDN phone number. This information is used for outgoing calls and specifies the calling number to the remote host.
ISDN Subaddress	If more than one ISDN device is using the same ISDN line, sub-addressing can be used to address each device. This is an advanced feature; consult the ISDN documentation for details.
SPID	The service profile identifier. It is used in North America as an additional identifier and in conjunction with the calling number, to identify the local number to the local switch.
Local Number	Use to "filter" incoming calls. If the calling number of an incoming call does not match this number, the call is rejected. When used, this number should be your ISDN number.
Local Subaddress	This is an advanced feature and is normally not needed.

Note – Profile B should be used only within the USA.

▼ To Modify or Unconfigure a Local Port

1. **On the Main Administration page, under “Network Connection Administration,” click ISDN.**

   The ISDN page is displayed.

2. **Choose one of the following.**

   - To modify a port, choose Modify for the required port, and make the changes in the form using TABLE 7-12.
   - To unconfigure a port, choose Unconfigure for the port to be unconfigured; then confirm the operation.

▼ To View or Clear a Remote Host Connection Log

1. **On the Main Administration page, under “Network Connection Administration,” click ISDN.**

   The ISDN page is displayed.

2. **Choose one of the following.**

   - To view a log file, click View log file; the log is displayed.
   - To clear a log file, choose, click Clear log file; then confirm the operation.

CHAPTER 8

Using Security Administration

This chapter describes the Security Administration modules:

- Administration Web Server
- Network Service Access Administration

Administration Web Server

The Administration Web Server serves the administration pages through which the Netra administration modules are configured. To protect access to the administration web server from unauthorized users, access to the web server is protected through a password (mandatory), and an access list (optional). If an access list is specified, connections from machines that are not on the list are refused. Connections from machines on the list are permitted access, provided the user knows the password.

▼ To Change the Administration Password

1. **From the Main Administration page, under “Security Administration,” click Administration Web Server.**

   The Administration Web Server Administration page is displayed.

2. **Click Change Administration Password.**

   The Administration Password page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 8-1 Web Server Password Administration

Option	Description
Current Administration Password	Type existing administration password. The administration password for an unconfigured Netra system is `setup`. A password can be a combination of any characters.
New Administration Password	Type a new password to access your Netra server. The password is not echoed as you type it. If you change the existing password, you must re-authenticate the browser connection using the new password you provide.
Re-enter New Administration Password	Type the new administration password. Because the password is not echoed as you type it the first time, you must verify it by typing it a second time.

▼ To Modify Host Access Control

The Host Access Control enables you to set the hosts that can access the administration web server. There are two possible access modes: Administration access can be granted to all hosts, or access can be restricted to a specified list of hosts and networks (an access control list). The Netra system is always allowed administration access, even when it is not specified in the access control list. If security is important, set restrictions, particularly when the Netra system is connected to the Internet.

1. **From the Main Administration page, under "Security Administration," click Administration Web Server.**

   The Administration Web Server Administration page is displayed.

2. **Click Modify Host Access Control.**

   The Host Access Administration page is displayed.

3. **Complete the form using the following table for reference.**

TABLE 8-2 Host Access Control Administration

Option	Description
All hosts	Access to the administration web server is permitted to all hosts. Any specified host or network addresses are ignored.
Specified host and network addresses	The host and network addresses that are allowed access to the administration modules.

Note – If you do not specify any hosts, all hosts are allowed access.

UDP-based services, which are not connection-oriented, may linger after the client has disconnected. Reboot the Netra j server after modifying the access control to these services.

Network Service Access Administration

The Netra server provides a number of generic network services that do not have administration modules associated with them. These services enable users to access information and facilities on the server. You can restrict access to any or all of these services using the Network Service Access module. Restricting access to all services helps ensure the security of your network.

Each network service has three access modes:

- The service can be denied to all hosts.
- The service can be made available to a specified list of hosts and networks (using a control list).
- The service can be made available to all hosts.

All services using the control list access mode share one access control list.

The following network services are available on your Netra server:

- *File Transfer Protocol* (`FTP`) – Enables an authorized user to transfer files between a remote machine and the Netra server.
- *TELNET Protocol* (`telnet`) – Enables an authorized remote user to log in to the Netra server and interact as a normal user.
- *Remote User Information* (`finger`) – Enables network users to display information about users logged in to the Netra server.
- *Remote Shell* (`rsh`) – Enables an authorized remote user to open a command-line interpreter (shell) on the Netra server and run commands there.
- *Remote Login* (`rlogin`) – Enables an authorized remote user to log in to the Netra server and interact as a normal user.
- *Remote Execution* (`rexec`) – Enables a library routine to be run on a remote machine and return streams to the local machine.
- *Remote System Statistics* (`rstat`) – Enables a remote user to get performance data from the Netra server.
- *Mail Notification* (`comsat`) – Enables the Netra server to detect incoming mail and notify local users logged into the Netra server.

- *Talk Program* (`talk`) – Enables users on remote systems to enter lines of text on one machine and display them on the terminal of someone logged into the Netra server. (Remote users can thus “chat” with users on the Netra server.)
- *Distributed System Admin* (`sadmind`) – Enables remote users to perform distributed system administration operations on the Netra server.
- *Network File System Quota* (`quotad`) – Enables for notification if users use more than an allocated amount of disk space on the Netra server.
- *User Info* (`rusers`) – Enables a remote user to check which users are logged into the Netra server.
- *Diagnostic Packet Tester* (`spray`) – Enables a remote user to send a one-way stream of packets to the Netra server to see how many are received and at what rate.
- *Broadcast Messages* (`rwall`) – Enables a single message from a remote user to be sent to all users logged into the Netra server.
- *UNIX-to-UNIX Copy* (`uucp`) – Enables remote copy exchanges between a remote machine and the Netra server.
- *Trivial Name Server* (`tnamed`) – A server that supports the DARPA trivial name server protocol.
- *Calendar Manager* (`cmsd`) – Enables remote users to check the Calendar Manager entries of a user with an account on the Netra server.

▼ To Control Access to Network Services

1. **From the Main Administration page, under “Security Administration,” click Network Service Access.**

   The Network Service Access Administration page is displayed with a list of the server’s network services and corresponding access levels.

2. **Choose the access mode for each network service using the information in the following table.**

TABLE 8-3 Security Levels for Network Services

Option	Description
None	Denies access to all hosts for this service.
Control List	Permits access by hosts and networks specified in the `Control List Host and Network Addresses` field.
All	Allows access to all hosts.
Control List Host and Network Addresses	The host or network addresses of the hosts and networks of hosts that are allowed access to the services. This field is required for services using the Control List access mode.

CHAPTER 9

Using System Administration

This chapter describes the system administration modules:

- "External Disks" on page 153
- "File System Backup and Restore" on page 156
- "Host Name" on page 161
- "Log Files" on page 161
- "Netra Ready Applications" on page 162
- "Restart and Shutdown" on page 162
- "Save and Restore Configuration" on page 163
- "Software Management" on page 166
- "System Defaults" on page 169
- "User Accounts" on page 169

External Disks

Note – The Netra software does not display the External Disks module if you do not have external disks attached to the Netra server. If you add a new external disk to a Netra server that is already configured, restart the server with the "Check for new devices during restart" option so that it recognizes the new disk drive.

Use the External Disks module to create mount points for external disks or to erase any unmounted disks. You must provide the mount point for a disk drive.

The External Disk module presents a graphic overview of the external disks attached to the system. Each disk is presented as a colored icon, and the icon color represents its state. The legend correlates the icon color to states described in the following table.

TABLE 9-1 External Disk State Color Code

Color	State	Comment
Green	Unused	Disk is available for formatting and mounting.
Red	System	Disk contains the Solaris operating environment.
Yellow	Erased	Disk has been formatted.
Aqua	Mounted	Disk is accessible through the file system hierarchy.
Orange	Not a Netra disk	Disk is not a Netra disk, but partially or totally mounted.
Purple	Meta	Disk which all or part is in use by a metadevice.
(blank)	Empty	No disk.

Above each disk icon is the disk name. If this name is a link, then by clicking the link, a list of valid operations for that disk is displayed. Only unused disks or disks that have already been erased/mounted by the Netra system show up as links.

Caution – When you erase a disk, you lose all the data on it.

▼ To Mount an External Disk

Note – If an external disk is attached to the Netra server but is not in the expected Netra format, you do not see the mount option. Erase the disk first. The mount option is then displayed.

1. **From the Main Administration page, under “System Administration,” click External Disks.**

   The External Disk Administration page is displayed.

2. **Complete the form using the information in the following table.**

TABLE 9-2 External Disk Mountpoint Information

Option	Description
Mount point	The directory on which to mount the disk. If the directory does not exist, it is created before the disk is mounted.

Note – A mounted disk cannot be erased through the External Disks Administration module.

▼ To Unmount an External Disk

1. **From the Main Administration page, under "System Administration," click External Disks.**

   The Unmount External Disk Administration page is displayed.

2. **Click OK to confirm the operation.**

▼ To Erase an External Disk

1. **From the Main Administration page, under "System Administration," click External Disks.**
2. **Under "External Disk Administration," click disk link, then click Erase External Disk.**

   The Erase External Disk Administration page is displayed.

Caution – When a disk is erased, all the data on it is lost forever.

3. **Click OK only if you want to erase the disk, otherwise click on the Home icon.**

File System Backup and Restore

Note – The Netra software does not display the File System Backup and Restore module if a tape drive is not attached to the Netra server. If you add a new tape drive to a preconfigured Netra server, restart the server with the “Check for new devices during restart” option so that it recognizes the new drive.

Use the File System Backup and Restore module to make a copy of the user data file system and save it to tape. You can also use it to restore directories from the tape backup copy if a disk fails or if a file is accidentally deleted.

Backup Options

You can back up any or all of the following directories in the user data file system: `Mail`, `HTML documents`, `Anonymous FTP`, `Users’ homes,` and Netra configuration files. When the backup is complete, the module reports all the directories and files that have been saved via an emailed report to the system administrator (root) user.

Note – The users' home directory option does not back up the system administrator's home directory. For user-specified directories and files, there is an upper limit on the number of characters in the file descriptor: for the path name, the maximum length is 155 characters; for the file name, 100 characters.

The following backup options are available:

- *Set backup options* – Enables you to schedule days of the week and times for regular backups.
- *Immediate backup* – Enables you to back up the file system at any time. This does not affect the scheduled backup.

Note – Only a single-tape backup is supported, and the tape is rewound after the backup process is completed.

Restore Options

When a directory is restored, all files and directories in that directory are copied from the backup tape to the Netra file system. For example, if you restore the `Users' homes` directory, all files in all users' directories are copied to the file system.

The following restore options are available:

- *Change restore device* – A default tape drive is displayed as the device that contains the backup tape from which a file system is restored. This option enables you to specify a different tape drive, if necessary.
- *Easy restore* – Enables you to restore selected directories from the backup tape in the current restore device. You can restore any of the following directories: `Mail`, `HTML documents`, `Anonymous FTP`, and `Users' homes`.
- *Selective restore* – Enables you to restore only the directories you need from a backup tape.

▼ To Set Backup Options for a Scheduled Backup

1. **From the Main Administration page, under "System Administration," click File System Backup and Restore.**

   The File System Backup and Restore page is displayed.

2. **Under "Backup," click Set backup options.**

   The File System Backup Options page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 9-3 Backup Options

Option	Description
Backup Device	The tape drive used for the backup procedure. If an attached tape drive is not displayed in the list, restart the server with the “Check for new devices during restart option” in the Restart and Shutdown module.
Eject Tape	Ejects the tape from the drive after the backup is completed. Choose Yes or No.
Directories	The directories to be backed up. You must choose at least one of the following directories: Mail (`/export/mail`), HTML documents (`/export/htdocs`), Anonymous FTP (`/export/ftp`), Users’ homes (`/export/home`), Netra configuration, or other. If the Web server’s `document root` is not `/export/htdocs`, specify the full path name of the `document root` in the empty text box. • The maximum length for a path name prefix is 155 characters. • The maximum length for a file name is 100 characters. • The maximum length for a full path name is 255 characters. Any file names exceeding these limits are not backed up.

Note – The other directories text field can be used to specify another top-level directory to be saved in the backup. It also must be used to specify an alternate web server document root (other than `/export/htdocs`) if HTML documents are saved in the backup.

▼ To Back Up the File System Immediately

1. **From the Main Administration page, under “System Administration,” click File System Backup and Restore.**

   The File System Backup and Restore page is displayed.

2. **Under “Back up,” click Immediate backup.**

   The Immediate File System Backup page is displayed.

3. **Complete the form using the information described in the Backup Device, Eject Tape, and Directories fields in** TABLE 9-3**.**

   The directories you specified are backed up immediately.

▼ To Change the Restore Device

1. **From the Main Administration page, under "System Administration," click File System Backup and Restore.**

   The File System Backup and Restore page is displayed.

2. **Under "Restore," click Change restore device.**

   The Change Restore Device page is displayed.

3. **Choose the tape drive you want to use to restore the file system.**

TABLE 9-4 Restore Device Administration

Option	Description
Restore Device	The tape drive that contains the backup tape used to restore the file system. If an attached tape drive is not displayed in the list, restart the server with the Check for new devices during restart option in the Restart and Shutdown module.

▼ To Restore Groups of Directories

Note – Before you begin, make sure the tape is in the drive.

1. **From the Main Administration page, under "System Administration," click File System Backup and Restore.**

   The File System Backup and Restore page is displayed.

2. **Under "Restore," click Easy restore.**

   The Easy File System Restore page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 9-5 Easy Restore Administration

Option	Description
Directories	The directories to be restored from the backup tape to the Netra server. You must select at least one directory. Choose `Mail` (`/export/mail`), `HTML documents` (`/export/htdocs`), `Anonymous FTP` (`/export/ftp`), or `Users' homes` (`/export/home`). If the Web server's document root is not `/export/htdocs`, then replace the string "Other Directories" in the text box with the full path name of the `document root`.
Restore location	The directory that receives the restored directories. If not chosen, the directories are restored into their default directories.
Eject Tape	Ejects the tape from the drive after the restore operation is completed. Choices: Yes, No.

▼ To Restore Selected Directories

Note – Before you begin, make sure the tape is in the drive.

1. **From the Main Administration page, under "System Administration," click File System Backup and Restore.**

   The File System Backup and Restore page is displayed.

2. **Under "Restore," click Selective Restore.**

   The Selective File System Restore page is displayed. (Note that it takes several minutes for the form to be displayed because the table of contents on the tape must be read first.)

3. **Complete the form using the information in the following table.**

TABLE 9-6 Selective Restore Administration

Option	Description
Directories	The directories to be restored from the backup tape to the Netra server. You must select at least one directory. Directories are restored recursively. (For example, if you select `/export/ftp`, all the files in all the directories in `/export/ftp` are restored.)
Restore location	The directory that receives the restored directories. If not chosen, the directories are restored into their default directories.
Eject Tape	Ejects the tape from the drive after the restore operation is completed. Choose Yes or No.

Host Name

Use the Host Name module to change the name of your Netra server.

▼ To Change the Host Name

1. **From the Main Administration page, under "System Administration," click Host Name.**

   The Host Name Administration page is displayed.

2. **Enter the Netra server name.**
3. **Restart the Netra server so that the new name is used.**

Log Files

Log files should be viewed and cleared periodically. Use the Log Files module to administer the following types of log files:

- *Message log* – Contains status on generic Solaris modules.
- *Netra log* – Contains information posted by Netra administration modules (such as error conditions).
- *Super User Login log* – Records who logs in to the server as root.

- *Administration Web Server Error log* – Records the times that the Administration Web Server was unable to deliver a page.
- *Administration Web Server Access log* – Records all requests to the Administration Web Server.

▼ To View or Clear Log Files

1. **On the Main Administration page, under "System Administration," click Log Files.**

   The Log Administration page is displayed.

2. **Choose one of the following options:**
   - To look at a log file, click View.
   - To remove a log file, click Clear; then confirm the operation.

Netra Ready Applications

Netra™ Ready™ Applications are provided by Independent Software Venders (ISVs) for use with Netra j software.

Restart and Shutdown

Use the Restart and Shutdown module to restart or shut down the Netra server. You may need to restart the Netra server when you add new devices.

All users who are logged in to the Netra server receive a message before these operations are performed.

▼ To Restart or Shut Down the System

1. **From the Main Administration page, under "System Administration," click Restart and Shutdown.**

   The Restart and Shutdown Administration page is displayed.

2. **Complete the form using the information in the following table.**

TABLE 9-7 System Restart/Shutdown Administration

Option	Description
Shut Down	Shuts down and powers off the Netra server.
Restart	Restarts the Netra server.
Check for new devices during restart?	If this option is selected, the operating system regenerates the list of devices attached to the Netra server. Use this option if you add a tape drive, CD-ROM drive, external hard disk, or network interface hardware to your server.
Delay	The number of minutes before the Netra shuts down or restarts.

Save and Restore Configuration

The Save and Restore Configuration module enables you to:

- Save a record of the current configuration of the Netra server to a diskette or to a file.
- Restore the Netra server to a previous configuration using data that was saved to either media.

You should save the system configuration whenever it is changed so you can return to this configuration state if necessary.

Some of the administration information that is entered using the Network Computer Administration Form is not automatically saved as part of the Netra j Save and Restore feature. The relevant system files must be saved manually if you intend to restore these settings after a system crash. The entire directory `/var/dhcp` should be saved to an off-line storage medium such as magnetic tape or diskette. You should back up the contents of this directory at regular intervals, particularly when new NCs have been added, deleted or modified using the Netra j user interface. These files must be restored separately in addition to the default restore procedures required during a crash recovery of a Netra j server.

Save and Restore Options

The following options are available to save and restore your system configuration:

- *Eject diskette* – This option ejects a diskette from the drive. If you save or restore your system configuration to or from a diskette, the diskette is ejected at the end of the operation.

- *Save configuration to diskette* – This option saves your current system configuration to the diskette in the drive. If you use an unformatted diskette, it is formatted as part of the save process.
- *Save configuration to file system* – This option saves your current system configuration to a system hard disk.
- *Restore configuration from diskette* – Either all or selected configurations on the diskette are restored to the Netra system. This option is displayed only if there is a valid Netra system configuration on the diskette.
- *Restore configuration from file system* – Either all or selected configurations on the hard disk are restored to the Netra system. This option is displayed only if there is a valid Netra system configuration on the hard disk.

The following table describes when file system options are displayed on the Netra j 3.0 Main Administration page.

TABLE 9-8 Options Displayed

Option	When the Option Is Displayed on the Main Administration Page
Eject Diskette	The diskette is in the disk drive.
Save Configuration to Diskette	The diskette is in the disk drive.
Restore Configuration from Diskette	The diskette in the disk drive contains valid Netra configuration information.
Restore Configuration from File System	The Netra configuration state has previously been saved to a file on the hard disk.

▼ To Save the System Configuration

1. **If you are saving to diskette, insert the diskette into the drive; otherwise, proceed to Step 2.**

   Make sure the diskette is not write-protected.

2. **From the Main Administration page, under “System Administration,” click Save and Restore Configuration.**

   The Save And Restore Configuration Administration page is displayed.

3. **Click either Save configuration to diskette or Save configuration to file system; then confirm the operation.**

▼ To Restore the System Configuration

1. **If you are restoring the configuration from a diskette, insert a diskette into the drive; otherwise, proceed to Step 2.**
2. **From the Main Administration page, under "System Administration," click Save and Restore Configuration**

   The Save And Restore Configuration Administration page is displayed.
3. **Click either Restore configuration from diskette or Restore configuration from file system.**
4. **Complete the form using the information in the following table.**

TABLE 9-9 Save/Restore Configuration

Option	Description
Restore entire configuration	Restores all configurations from the diskette/disk.
Restore selected configurations	Restores only the selected configurations from the diskette/disk. If you select this option, you must also select at least one configuration; if you select any configurations, you must also select this option.

Note – When restoring selected configurations, if you checked Network Computer Server, the network computer server and the network computer application management configurations are restored. Network computer application management does not have a separate check box.

▼ To Eject a Diskette

1. **From the Main Administration page, under "System Administration," click Save and Restore Configuration**
2. **Click Eject diskette.**

   The Verify page is displayed.
3. **Click OK.**

Software Management

The Software Management module is used to install and remove software on the Netra server. This module recognizes software that is supplied in the Solaris package, patch, or cluster formats. All Sun software and most third-party software can be managed using this module.

The list of packages, patches, and clusters are displayed in a selection box on the browser page. The performance is significantly improved when administered from HotJava.

A *package* is a collection of files and directories required to form a software application.

A *cluster* is a logical grouping of software packages associated with a specific software product.

A *patch* is a collection of files and directories that replace or update existing files and directories that are preventing proper execution of the software. The existing software is derived from a specified package format and can be installed only if the package it fixes is already present.

Note – When installing or removing software associated with specific hardware, ensure that the hardware is already installed and is part of the system device list. For example, before you install the Token Ring Interface software, make sure that the Token Ring Interface card is installed in the Netra server and that the server has regenerated its list of attached devices (see “Restart and Shutdown” on page 162).

Install and Remove Options

The Software Management module offers the following options:

- *Select new installation medium* – Use this option to set the installation medium from which to do future installs. Clusters, packages or patches to be installed on the Netra can be on installation media such as CD-ROM, diskette, or mounted directories. The CD-ROM is the default installation medium.
- *Install clusters, packages, or patches* – Use this option to install clusters, packages, or patches from the selected installation medium. Once the installation is complete, you should restart the Netra server.
- *Remove packages or patches* – Use this option to remove packages or patches that are installed on the Netra server. Once they are removed, you should restart the Netra server.

- *View packages or patches* – Use this option to see what packages or patches (if any) are installed on the Netra server.

▼ To Specify the Installation Medium

1. **From the Main Administration page, under "System Administration," click Software Management.**

   The Software Management Administration page is displayed.

2. **Under "Select Installation Medium," Select new installation medium.**

   The Select Installation Medium page is displayed.

3. **Choose the medium from which to install packages or patches.**

   If you select CD-ROM or Diskette, the medium is automatically mounted onto the system as part of the installation. If you select Directory, enter the path to the directory from which to install the software.

▼ To Install Clusters, Packages, or Patches

1. **From the Main Administration page, under "System Administration," click Software Management.**

   The Software Management Administration page is displayed.

2. **Under "Install," click Clusters, Packages, or Patches.**

3. **Complete the form using the information in the following table.**

TABLE 9-10 Installing Packages or Patches

Option	Description
Install All Clusters/Packages/Patches	Installs all clusters, packages, or patches from the selected installation medium.
Install Selected Clusters/Packages/Patches	Installs only the clusters, packages, or patches you select from the list. If you select this option, you must also select at least one cluster/package/patch; if you select any clusters/packages/patches, you must also select this option.

4. **Click OK.**

   When clicking OK to install software, you see a message stating that the module is currently installing software. If left as it is, the browser periodically reloads the page until the process has completed, after which it displays the result.

   Alternatively, you can perform other administration tasks and then return to the software module. The next time you visit the module, if the installation is incomplete, you see a message stating that the module is currently installing software; if the installation is complete, you see the result of the installation. The result lists all the successfully installed software and any problems.

5. **Restart the Netra server using System Administration: Restart and Shutdown.**

▼ To Remove Packages or Patches

Note – The Software Management module cannot remove a package if there is another package on the system that requires its presence. The module attempts to remove packages in the order in which they are displayed, and since this may not reflect the dependency order, the removal of a core package may fail even if the packages that depend upon it are also removed. If this happens, reselect the packages that failed and remove them again.

---

1. **From the Main Administration page, under "System Administration," click Software Management.**

   The Software Management Administration page is displayed.

2. **Under "Remove," click Packages or Patches.**

3. **Select one or more Packages or Patches (or All patches); click OK.**

4. **Restart the Netra server using System Administration –> Restart and Shutdown.**

▼ To View Installed Packages or Patches

1. **From the Main Administration page, under "System Administration," click Software Management.**

   The Software Management Administration page is displayed.

2. **Under "View," click Installed Packages or Installed patches.**

   The Viewed Installed Packages or Viewed Installed Patches page is displayed.

System Defaults

Use the System Defaults module to change the time zone and locale for your Netra server.

Note – If you change the time zone or locale, restart the Netra server so that the new value takes effect.

▼ To Set System Defaults

1. **From the Main Administration page, under "System Administration," click System Defaults.**

   The System Default Administration page, showing the time zone, and locale, is displayed.

2. **Complete the form using the information in the following table.**

3. **If you change the time zone or locale, restart the Netra server so that the new value takes effect.**

TABLE 9-11 System Defaults

Option	Description
Default System Time Zone	The default time zone used by the Netra server. You can override the default time zone by setting the TZ environment variable.
Default System Locale	The default locale used by the Netra server. You can override this default by setting the LANG or LC* environment variables. Some of the available locales are partial locales. Choosing a partial locale sets up the system to display localized numeric, monetary, and calendar formats, but not localized user interfaces or messaging.

User Accounts

The User Accounts module is used to add new user accounts and to modify or delete existing ones. Creating an account allocates the new user a home directory on the Netra server and enables the user to access the services that are available on it, which can include mail for example. The account can be accessed through standard protocols such as `telnet`, `rlogin`, `ftp` and `rsh`, provided the server is configured to accept them.

For users to be able to login to NCs administered by the Netra server, the server must be configured as the NIS master of the NIS domain that is used by the NCs.

Note – All users added by the User Module are local users on the Netra j host. This is so regardless of the NIS status of the server. If the Netra j server is configured as a NIS master server at any stage, then these users are ALSO pushed to the NIS name space and are referred to as NIS users in the User Administration forms.

The form asks you to specify a default shell for the user, including an option No shell (NC and email only). If this option is chosen, the user is not allowed to log in to the Netra j server, but can use a NC that is administered by the server. They can also receive mail on the server if it is configured as a mail server.

A password must be specified on creating a user account. This password can be used for login to a NC regardless of the shell chosen. However, if a server login shell is enabled, the password acts as an initial password for such server logins. Before a server login is completed, the user must provide and verify a new password.

If no users are defined, only the Add A User option is available. When user accounts have been added, there are also options to Modify or Delete specific users. When a user account is removed, the corresponding home directory is deleted recursively and the users mailbox is removed. The user is no longer able to log into the server.

The user account module can only be used for ordinary users. System users such as `root` and `ftp` or the Netra setup user cannot be administered from the module.

Configuring Users' Home Directories

Each user's home directory is automatically shared thought NFS by the system and the automounter home database is updated to include the directory. This allows the home directory to be automounted by any NC the user logs on to, provided the Netra server is the NIS master for the NIS domain used by that NC.

▼ To Add a User Account

1. **From the Main Administration page, under "System Administration," click User Accounts.**

   The User Accounts Administration page is displayed.

2. **Under “New Users,” click Add A User.**

   The Add A Local User page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 9-12 User Accounts

Option	Description
User Name	The login name of the user to add or modify. For example, `jsmith`. The user name must be unique and must not be among the list reserved for systems users. If such a name is chosen, the User Accounts module asks for another. The reserved user name list is displayed on the help page.
Password	The password the user must provide when logging in to the Netra server for the first time.
Retype Password	As the password is not echoed on the screen, it must be confirmed by re-entering it.
Full Name	The full name of the user you want to add/modify. Example: Jerry Lee Smith
Login Shell	The default shell for the user. Choose C shell (csh), Korn shell (ksh), Bourne shell (sh), or No shell (NC and email only). If you choose No shell (NC and email only), the user gets mail on the Netra server, but cannot log in.
Home Directory Server	Specify the host name where the home directory of each user resides. This information is used to configure the automounter. If the Netra server is a NIS master server, the auto.home map is also updated. If the user’s home directory is on this local system itself, then sharing of the user’ home directory through the Network File System (NFS) is enabled. If the server is remote, the home directory(s) must be created and shared from the remote host that must be reachable on the network.
Base Directory	The full path to a base directory that holds the user’s home directory on the server specified above; for example, if `/export/` home is entered as the base directory and the server specified is the local host, a successful addition of a user called sample creates a home directory: `/export/home/sample` If the server is the local system and the base directory does not exist, then if possible, the base directory is created.If a remote server is specified for the home directory, then the user must have this base directory on the remote server. In the local system files, the user is then configured with `/home/`<*username*> so that the mounted directory can be used. Note1: The root directory is rejected as a base directory. Note2: When the local server is specified above, a mount point cannot be used as the base directory.

▼ To Add Users From a File

1. **From the Main Administration page, under "System Administration," click User Accounts.**

   The User Accounts Administration page is displayed.

2. **Under "New Users," click Add users from a file.**

   The Add users from a file page is displayed.

3. **Complete the form using the information in the following table.**

TABLE 9-13 Adding Users From a File

Option	Description
Input File	The full path to a UNIX file, which must be correctly formatted. No comments, blank lines, or space characters are allowed. For example, if the field separator specified below is a comma, each line entry must be formatted as follows: *username,<UID>,password.* The username and password must be composed of one to eight alphanumeric characters. Each `username` must be unique and must NOT be any of the following system account names; `root, daemon, bin, sys, adm, lp, smtp, uucp, nuucp, listen, nobody, noaccess, nobody4, setup, ftp.` The `UID` must be between 1000 and 59999. The administrator can optionally leave the uid field blank and one is assigned. For security reasons, the input file must be owned by root with all group/other permissions removed.

TABLE 9-13 Adding Users From a File

Option	Description
Field Separator	The character used to delimit each field in the input file.
Home Directory Server	Specify the host name where the home directory of each user resides. This information is used to configure the automounter. If the Netra server is a NIS master server, the auto.home map is also updated. If the user's home directory is on this local system itself, then sharing of the user's home directory through the Network File System (NFS) is enabled. If the server is remote, the home directory(s) must be created and shared from the remote host that must be reachable on the network
Base Directory	The full path to a base directory that holds the user's home directory on the server specified above; for example, if `/export/home` is entered as the base directory and the server specified is the local host, a successful addition of a user called sample creates a home directory: `/export/home/sample` If the server is the local system and the base directory does not exist, then if possible, the base directory is created. If a remote server is specified for the home directory, then the user must have this base directory on the remote server. In the local system files, the user is then configured with /home/<username> so that the mounted directory can be used. Note1: The root directory is rejected as a base directory. Note2: When the local server is specified above, a mount point cannot be used as the base directory.

▼ To Modify or Delete a User Account

1. **From the Main Administration page, under "System Administration," click User Accounts.**

   The User Administration page is displayed, with a Modify or Delete option for each existing account.

2. **Under "Existing Users," click one of the following options**:

   - To modify an existing account, click Modify and make the changes in the form using TABLE 9-12 and the following table.

- To delete a user account, click Delete, and then confirm the operation.

TABLE 9-14 Other User Account Options

Option	Description
Change password?	This option is available only when an existing user account already has a password. Password changes must be confirmed. If checked yes, this option changes the user's password to the string in the "Password" field for the user's next login.
Home Directory Path	Specify the full path name of the user's home directory. For example, `/export/home/`*username*. If a remote server is specified as the host for the home directory, the path name entered must be the path shared from the REMOTE server. The user is then configured with `/home/`*username* as a home directory in the local server files, as this is where the share is mounted for that username.

Note – The root directory is rejected as a user directory.

Note – When the local server is specified above, a mount point cannot be used to include the user directory.

CHAPTER **10**

Using Proxy Cache Services

The Netra j server can be used as a proxy cache for another HTTP (web) server on your network. This chapter explains how to configure, administer, and monitor proxy cache services on the Netra j server.

Proxy Cache Server Features

Netra j implements a full-featured proxy cache server that you can incorporate seamlessly into your organization's internal network. The Netra j proxy cache server includes the following features:

- Compatible with Squid, Harvest, and CERN proxy standards.
- Supports the Inter Cache Protocol (ICP).
- Caches HTTP 1.0, FTP, and Gopher objects. This list includes, among other types, GIF, JPEG, and `.exe`.
- Supports Secure Sockets Layer (SSL) tunneling.
- Supports persistent HTTP connections, commonly referred to as "keep-alives."
- The cache persists across reboots.

- Provides configurable cache-object expiration times. The proxy cache software ages and deletes a cache object based on attributes specified in its uniform resource locator (URL). The product offers a flexible scheme for cache-object expiration.
- Offers a flexible scheme for setting a cache object to non-cacheable, based on its URL.
- Supports dynamic parent failover: If the proxy cache server has multiple parents and is connected to a parent that fails, the server fails over to the next available parent. Furthermore, the proxy cache server detects when the original parent comes back online.
- Supports conditional retrievals; for example, can retrieve an object if it has been modified in the last day. You can modify the time threshold to suit your needs.
- Caching software imposes no limit on the amount of data cached.
- Enables you to build hierarchies of proxy servers. See "Hierarchies" on page 176.
- Offers a number of auditing features, including hit statistics, detailed user access logs, bandwidth usage statistics, and a number of other proxy- and cache-related statistics.
- Ships with an SNMP MIB and agent, so that you can manage a Netra j proxy cache server from an SNMP-conformant management platform, such as Solstice™ Domain Manager™.
- Offers a variety of filtering features, including blocking and redirecting of HTTP requests based on URL, host name, or user.
- Ships with a set of web-based tools for product configuration and monitoring.

Hierarchies

With the Netra j proxy cache server you can create hierarchies of proxy cache servers simply by pointing proxy cache servers to succeeding proxy cache servers as you proceed toward a firewall.

The following figure illustrates a simple hierarchy of proxy cache servers.

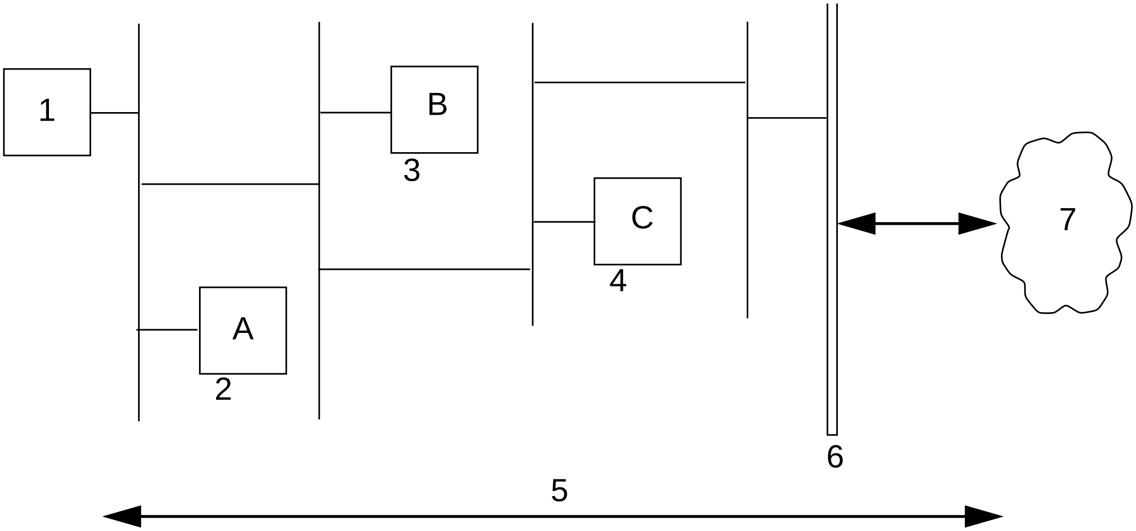


FIGURE 10-1 Simple Hierarchy

Legend:

1. Client browser
2. Netra j proxy cache server A
3. Netra j proxy cache server B
4. Netra j proxy cache server C
5. HTTP Requests/Responses
6. Firewall
7. Internet

Browser (1) points to proxy A. Proxy B is parent to A. Proxy C is parent to B.

In this sample hierarchy, assume the client browser requests a web object that originated somewhere in the Internet and is, at the moment, not in Netra j proxy cache server A's cache. The following sequence ensues:

1. Machine A checks with its parent, machine B.
2. Likewise, B does not have the object in its cache and checks its parent, machine C. If C does not have the object, it goes out through the firewall to the web server to obtain it.

3. Machine C returns the object—obtained from a remote web server or its local cache—to machine B.

4. Machine B returns the object to machine A.

5. Machine A returns the object to the requesting client.

If the object is cacheable, each proxy stores a copy upon receipt. Note that communication between parent proxies is over TCP connections.

Netra j proxy cache software also supports a variation of the preceding scenario. This variation is shown in the following figure.

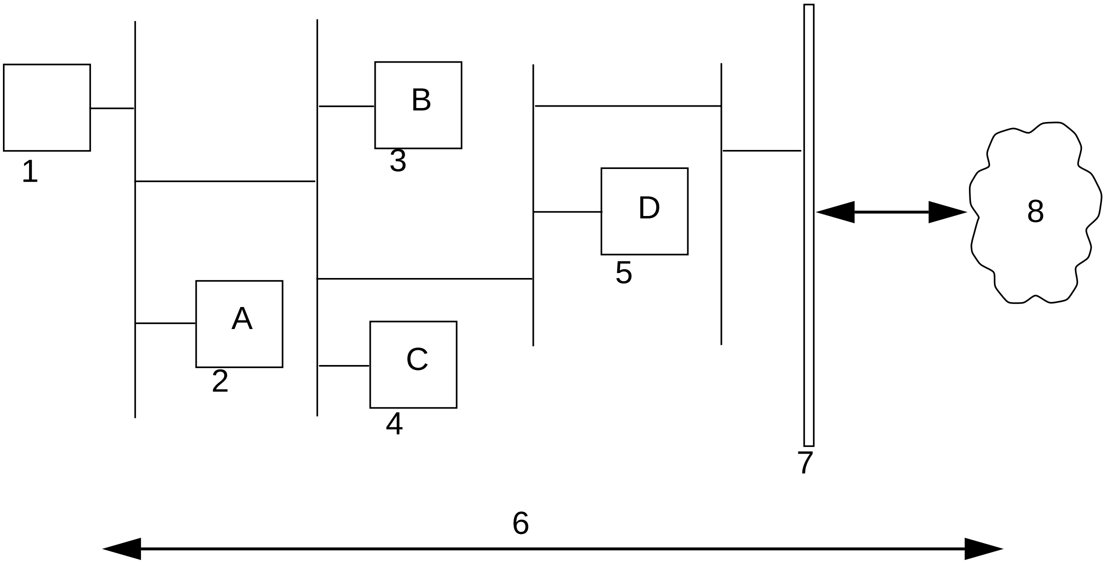


FIGURE 10-2 Multiple Parent Proxies

Legend:

1. Client browser

2. Netra j proxy cache server A

3. Netra j proxy cache server B

4. Netra j proxy cache server C

5. Netra j proxy cache server D

6. HTTP Requests/Responses

7. Firewall

8. Internet

Browser (1) points to A. Proxy B and proxy C are parents to A. Proxy D is parent to B and C.

In this example, if a client requests an object of its proxy server, machine A, that is not in A’s cache, machine A relays the request to its two parents, machines B and C. If one of the parents has the object, it returns the object to A. If neither has the object, machine A forwards the request to the parent that responds faster, assuming that machine to be less loaded and/or have a better network connection.

If you configure multiple parents, the Netra j proxy cache software enables you to give greater weight to one or the other, or to set up one as the default. When no parent (of multiple parents) has a requested object, the “child” proxy always forwards the request to the default parent.

Monitoring and Managing Proxy Services

The Netra j proxy cache server offers three different types of tools for monitoring the state of proxy-caching services:

- You can monitor proxy cache services through web pages. See “Monitoring a Netra j Proxy Cache Server” on page 199 for a description of the monitoring web pages.
- You can monitor proxy cache services through web-based log tracing tools. See “Proxy Cache Log Files” on page 202 for a description of the various types of logs available.
- You can use any SNMP-conformant management platform (such as Solstice Domain Manager) to monitor and manage a Netra j proxy cache server through Management Information Bases (MIBs) included in the Netra j proxy cache software. The software also supports a set of traps that notify you of critical events, ranging from a down server to a failure report on a server component. See “Configuring SNMP Services” on page 197.

Basic Proxy Cache Setup and Shutdown

The Basic Proxy Cache page provides a simple 3-step questionnaire that sets up a fully functional proxy-caching server. If you decide to turn off proxy cache services, you can use the Unconfigure Proxy Cache page.

▼ To Set Up Basic Proxy Cache Services

1. **From the Main Administration page, click Proxy Cache Service.**
2. **In the Proxy Cache Administration page, click Basic proxy cache configuration.**

   The Basic Proxy Cache page is displayed.
3. **Enter the HTTP port number and click the forward arrow icon.**

   Most sites use the default value of 8080 for the HTTP port number. Conventions may differ at your site.
4. **List the domains inside your corporate firewall and click the forward arrow icon.**

   Most corporate intranets are inside a firewall. If you are not inside a firewall, simply proceed to the next step.

   If you are inside a firewall, you have the option of listing domains that are inside the firewall. For URLs containing domains not in this list, the software does not perform a DNS lookup for the host specified in the URL and always fetches the object from a parent cache.
5. **List the parent proxy servers and click the forward arrow icon.**

   The basic setup questionnaire does not require the proxy server to have a parent, but if you are inside a firewall, it probably does have one.

   The Netra j proxy cache server supports multiple parents. For a given transaction, your machine might make requests to all of its parents. It would then use the parent that responded the fastest.
6. **Click the up-arrow icon to return to the Proxy Cache Administration page.**

▼ To Unconfigure the Proxy Cache

1. **In the Proxy Cache Administration page, click Unconfigure proxy cache.**
2. **In the Unconfigure Proxy Cache page, click OK.**

   A confirmation window verifies that proxy services have been unconfigured.

Viewing and Modifying Advanced Configuration Properties

You can view or modify advanced proxy cache configuration properties in pages accessed through the Advanced Proxy Cache Configuration page. This section assumes you have completed the basic setup of your Netra j proxy cache server. See "Basic Proxy Cache Setup and Shutdown" on page 179.

▼ To View or Modify Advanced Proxy Cache Configuration Properties

1. **From the Main Administration page, click Proxy Cache Service.**
2. **In the Advanced Proxy Cache Configuration page, click Advanced proxy cache configuration.**

   The Advanced Proxy Cache Configuration page presents a list of links, each of which corresponds to a category of proxy cache properties. For all categories, you follow the same procedure for viewing or modifying a property.
3. **In the Advanced Proxy Cache Configuration page, click the link for the category in which a property resides.**
4. **In the page for that category, view or make changes to the value of a property.**

   Most properties have editable fields. A few have toggles (either one value or another) or pulldown menus.
5. **At the bottom of the category page, click OK.**

   A page is displayed indicating the success or failure of your change. If a change fails, the page is redisplayed with the error indicated. Correct the error and click OK again. With some errors, a new page containing an error message is displayed. If this occurs, click the Back button on your browser to return to the category page.

   If you click Reset, the values for the properties on a page revert to what they were when you first loaded the page.
6. **After a successful change, click the up arrow icon to return to the Advanced Proxy Cache Configuration page.**

   Alternatively, you can click the home icon to return to the Netra j Main Administration page.

The remainder of this chapter is a description of the advanced proxy cache properties, broken down by the categories reflected in the links on the Advanced Proxy Cache Configuration page.

▼ To View or Modify Primary Configuration Properties

1. **In the Advanced Proxy Cache Configuration page, click Primary Configuration.**

   The Primary Configuration page is displayed.

2. **In the Primary Configuration page, accept or modify values for the following properties.**

TABLE 10-1 Primary Configuration Properties

Property	Description
Proxy Webmaster	An e-mail address of the person or group who is to receive notices of abnormal conditions in the Netra j proxy cache server. The default postmaster is `root`, which means that the recipients you specified for the Netra System Administrator Alias will receive mail bound for the Proxy Webmaster.
Visible Hostname	Error messages generated by the Netra j proxy cache server contain the host name you specify here. The default is the return from the `hostname` command.
Append Domain Name to Unqualified Host Name	If a URL refers to a host name without a . (period) in its name, the domain name you specify for this property is appended to the host name to form a fully qualified domain name.
Port for HTTP Client Requests	The port number at which the Netra j proxy cache server listens for HTTP requests. Most users can accept the default of 8080. Do not use 81; the Netra j proxy cache uses this number for administrative purposes.
Port for Neighboring Cache ICP requests	The number of the port on which the proxy cache server will receive and process ICP (InterCache Protocol) requests by other proxy servers that support the ICP protocol.
Port for Proxy Cache Server Statistics Requests	The TCP or UDP port on which the Netra j proxy cache server provides statistics. The SNMP subagent shipped with the product uses this feature to export the statistics via SNMP. Setting this property to `0` (zero) disables the providing of statistics. The default is 3140. Entering a non-zero value enables proxy cache monitoring, which is described in “Proxy Cache Monitoring” on page 200.

TABLE 10-1 Primary Configuration Properties *(Continued)*

Property	Description
Receive ICP Requests on this Address	If you enter an address, the Netra j proxy cache server accepts ICP requests only at the IP address specified here.
Send ICP Requests from this Address	If you enter an address, the Netra j proxy cache server sends ICP requests from the IP address specified here.
Operation Mode	Choose between Proxy+Cache (the default) and Proxy Only. If you choose Proxy Only, the Netra j proxy cache server does not cache any objects.

▼ To View or Modify Proxy Cascade Properties

1. **In the Advanced Proxy Cache Configuration page, click Proxy Cascade.**

   The Proxy Cascade page is displayed.

2. **In the top portion of the Proxy Cascade page, accept or modify values for the following properties.**

TABLE 10-2 Proxy Cascade Properties

Property	Description
Table of Parent Proxy Caches	When you load the Proxy Cascade page, the table of parents contains the hosts you entered when you last performed basic proxy cache configuration. See "Table of Parent Proxy Caches" on page 185.
Query Parent Cache for Domains	The Netra j proxy cache server contacts parents specified for this property only for matching domain names. An alternative form enables you to specify a host for non-matching domain names. See "Query Parent Cache for Domains" on page 185.
Domains Inside Firewall	When you load the Proxy Cascade page, the Domains Inside Firewall field contains the domains you entered when you last performed basic proxy cache configuration. The Netra j proxy cache server considers domains you list for this property as being inside a firewall. For URLs containing domains *not* in this list, the software does not perform a name service resolution (for example, a DNS lookup) of a host name specified in a URL. Also, for domains not in this list, if the Netra j proxy cache server does not have a requested object in its local cache, it always tries to fetch the object from a parent cache.

3. Scroll down to the remaining properties in the Proxy Cascade page.

TABLE 10-3 Remaining Proxy Cascade Properties

Property	Description
IP Addresses Inside Firewall	The Netra j proxy cache server considers addresses you list for this property as being inside a firewall. When you specify one or more addresses, the Netra j proxy cache server performs a host name resolution (for example, a DNS or NIS lookup) of the address specified in a URL for all requests, to determine whether the address is inside the firewall. For addresses *not* in this list, if the Netra j proxy cache server does not have a requested object in its local cache, it always tries to fetch the object from a parent cache. Note that using this property degrades server response time because of the overhead associated with host name resolutions.
Source Ping	Choose between off (the default) and on. By default, when the Netra j proxy cache server receives a request, it pings (sends ICP requests to) its parents. If Source Ping is on, the software also pings the host specified in the URL of an object it retrieves. This feature can be useful where parents are overloaded and the source web server is not. Note that Source Ping packets are never sent beyond a firewall.
Wais Relay Host	Enter the host name of the proxy server to which WAIS URLs will be relayed.
Wais Relay Port	Enter the port number on the above-named host name to which WAIS URLs are to be relayed.
Max. Relay Object Size (MB)	Enter the maximum size (in MB) of a WAIS object that can be received from the Wais Relay Host. The Netra j proxy cache server does not relay WAIS objects that exceed this limit.
Local Domains Inside the Firewall	When you load the Proxy Cascade page the Local Domains Inside the Firewall contains the domains you entered for the Domains Inside Firewall field when you last performed basic proxy cache configuration. The Netra j proxy cache server retrieves URLs containing the domains you specify here directly from the source and not from a parent. These domains should be the same as or a subset of the domains you specify for Domains Inside Firewall (see description above). Specify here domains to which you have good network connectivity, and from which users request relatively small objects.
Local IP Addresses Inside the Firewall	The Netra j proxy cache server retrieves URLs containing the IP addresses you specify here directly from the source and not from a parent. These addresses should be a subset of the addresses you specify for IP Addresses Inside Firewall (see description above). Specify here addresses to which you have good network connectivity, and from which users request relatively small objects. Note that using this property degrades server response time because of the overhead associated with host name resolutions.

Table of Parent Proxy Caches

The table of parent proxy caches contains the hosts you entered when you last performed basic proxy cache configuration. If you have multiple parent proxies that do not support ICP, the proxy cache service contacts those parents in the order you list them here. If you have multiple parents that do support ICP, the proxy cache service determines the “closest” parent by comparing response times to its ICP queries.

The headings in the table of parent caches are as follows:

- *Proxy Name* – Fully qualified host name of the parent proxy cache host. If this host is not in the same domain as the Netra j proxy cache host, you must specify the domain name; for example: `webcache.eng.acme.com`
- *HTTP Port* – The HTTP port number on which the parent listens for HTTP requests.
- *SSL* – A checkbox indicating whether a host supports the tunneling of the Secure Sockets Layer protocol.
- *Persistence* – A checkbox indicating whether a host supports the HTTP persistent connections feature, sometimes referred to as “keep-alive.”

Query Parent Cache for Domains

This property enables you to specify parents the Netra j Proxy Cache Server will contact only for URLs with matching domain names or, alternatively, with non-matching domain names.

Entries have the form *hostname domain_name* or *hostname* !*domain_name*. For example, if you have a parent `wbyeats`, in the same domain as the Netra j proxy cache server, to which you want directed all traffic related to URLs that contain the domain names `sales.acme.com` and `eng.acme.com`, you make an entry:

```
wbyeats sales.acme.com eng.acme.com
```

If you have multiple entries for one host—for example, in addition to the above, if you had: `wbyeats fin.com`—the domains in those entries are combined to form a single list.

You can also have a reverse match on domain names, so that requests related to URLs that contain domain names that do not match the specified domains are directed to the specified host. So, for example, if you want `wbyeats` to field all requests related to domains *other than* the domain names `sales.acme.com`, you make an entry:

```
wbyeats !sales.acme.com
```

Note that with the reverse-match feature, you can specify only one domain name, either as the only domain name in an entry or as the last domain name in an entry. If you want to prevent use of a given parent for multiple domains, specify additional entries. For example:

```
wbyeats !sales.acme.com
wbyeats !eng.acme.com
```

▼ To View or Modify Cache Policy Properties

1. **In the Advanced Proxy Cache Configuration page, click Cache Policy.**

   The Cache Policy page is displayed.

2. **Under the Cache Policy heading, enter or accept values for the properties described below.**

   The properties are divided into groups reflected in the following sections.

HTTP Policy

There are three HTTP Policy properties.

TABLE 10-4 HTTP Policy Properties

Property	Description
Time To Live (min)	The limit on the length of time an HTTP object can remain in the cache. The default is 720 minutes (12 hours).
Max Object Size (MB)	The limit on the size of an HTTP object for caching. The Netra j proxy cache server proxies for, but does not cache, HTTP objects that exceed this limit. The default is 4 MB.

Do not Cache URLs Containing	The Netra j proxy cache server does not cache HTTP URLs containing strings you add to this list. The defaults are:
	`/cgi-bin/`
	`/htbin/`
	`/www-bin/`
	`?`

Gopher Policy

There are three Gopher Policy properties.

TABLE 10-5 Gopher Policy Properties

Property	Description
Time To Live	The limit on the length of time a Gopher object can remain in the cache. The default is 4320 minutes (three days).
Max Object Size	The limit on the size of a Gopher object for caching. The Netra j proxy cache server proxies for, but does not cache, Gopher objects that exceed this limit. The default is 4 MB.
Do not Cache URLs Containing	The Netra j proxy cache server does not cache Gopher URLs containing strings you add to this list. The default is ? (question mark).

FTP Policy

There are three FTP Policy properties.

TABLE 10-6 FTP Policy Properties

Property	Description
Time To Live	The limit on the length of time an FTP object can remain in the cache. The default is 4320 minutes (three days).
Max Object Size	The limit on the size of an FTP object for caching. The Netra j proxy cache server proxies for, but does not cache, FTP objects that exceed this limit. The default is 4 MB.
Do not Cache URLs Containing	The Netra j proxy cache server does not cache FTP URLs containing strings you add to this list. There are no defaults.

URL Policy

There are two URL Policy properties.

TABLE 10-7 URL Policy Properties

Property	Description
Do not Query Neighbors for URLS Containing	For URLs containing strings you add to this list, the Netra j proxy cache server looks in its own cache and does not query parent caches.
TTL Selection Based on URL	The Netra j proxy cache server enables you to set the Time To Live for URLs containing strings that you specify (see below).

Setting the TTL for URLs

You can specify a URL's Time To Live in either of two ways: as an absolute value or as a percentage of an object's age. Entries have the following form:

```
reg_expression  absolute_TTL  percentage  maximum_TTL
```

where:

- *reg_expression* is a regular expression that is matched against a URL. See "Rules for Pattern Matching for TTL Selection Property" on page 219 for rules for the regular expression.

- *absolute_TTL* is the TTL (in minutes) used by the Netra j proxy cache server if the percentage method is not used.
- *percentage* is the percentage of the duration between an object's last-modified timestamp and the current time.
- *maximum_TTL* is the upper limit (in minutes) on the TTL.

The proxy cache uses the percentage method of determining the TTL if a matched object has a last-modified timestamp. If an object does not have such a timestamp, the absolute TTL is used instead. You can specify a negative value for *absolute_TTL* thereby forcing the percentage method to be used. If a matched object then does not have the required timestamp, the TTL is set from a value set under Cache Policy (see Step 2 in To View or Modify Cache Policy Properties).

If neither the absolute TTL nor percentage methods result in a TTL for a matched object, the TTL is determined from the values set in the Cache Policy properties.

The Netra j proxy cache server checks all patterns in the list and uses the *last* match.

The following is an example of a TTL-selection entry:

```
^http:// 1440 20 43200
```

The preceding example matches URLs that start with `http://`. If a URL contains a last-modified timestamp, the TTL for that URL is set to 20% of the difference between the timestamp and the current time. If the URL does not have such a timestamp, the TTL is set to 1440 minutes. In any event, the URL will not stay in the cache longer than 43200 minutes.

Other

Two properties are outside the scope of the previous categories.

TABLE 10-8 Other Properties

Property	Description
Max Request Size	The maximum size of a request, in KB. The default is 100. This value should be large enough to accommodate users who use the `POST` method to upload files.
Quick Abort	By default, the Netra j proxy cache server completes the retrieval of an object even when the request for that object is aborted. This is potentially a benefit because the cache will then have the object should it be requested subsequently and the machine resources and bandwidth consumed to the point of the aborting of the request are not wasted. However, this feature can be a detriment where you have slow links or very busy caches. This feature also allows for the possibility of impatient users tying up a URL by repeatedly aborting and re-requesting non-cachable objects. You have the option of turning this "quick abort" feature on (meaning that object retrieval ceases if the request is aborted). The default is off.

▼ To View or Modify Access Control Properties

1. **In the Advanced Proxy Cache Configuration page, click Access Control.**

   The Access Control page is displayed.

2. **Under the Access Control heading, enter or accept values for the properties listed below.**

   Enter access control definitions one to a line. To edit an entry, click the entry in the table, and then make any changes you want.

TABLE 10-9 Access Control Properties

Property	Description
Access List Definition	Access lists enable you to control access to the functions of the Netra j proxy cache server based on characteristics of a request. See "Access List Definition" on page 192.

Client Access Control	This and the following properties are used in conjunction with the access lists you create. For a given access list, you can allow or deny access to the HTTP port on the Netra j proxy cache server.
	The Client Access Control property takes an entry of the form:
	`allow` (*or* `deny`) *access_list* . . .
	The default values for Client Access Control are:
	`deny CONNECT !SSL_ports`
	`allow all`

Access to Cache Via ICP	An entry of the form: `allow` (*or* `deny`) *access_list* . . . The default for Access to Cache via ICP is to allow all accesses.
ACLs for the Cache Host	An entry of the form: *cache_server access_list* . . . Enables you to limit the ICP queries sent to a given host (such as ICP-capable parent proxy), based on the contents of an access list. If you specify multiple access lists, the Netra j proxy cache server applies the first list that matches for a given URL.

URL Redirection	An entry of the form:
	access_list . . . : `HOST` *hostname* `PATH` *path*
	Enables you to redirect a URL to a specified host and path. The access lists must be of types domain, service, or pattern. For example, the entry:
	`games : HOST restricted.acme.com PATH /restricted.html`
	redirects a URL that matches the `games` access list to:
	`http://restricted.acme.com/restricted.html`
	To create a URL Redirection entry, enter:
	• The name of one or more access lists, followed by a colon
	• The word `HOST` and a fully-qualified host name
	• The word `PATH` and an absolute path name

Access List Definition

Access lists enable you to control access to the functions of the Netra j proxy cache server based on characteristics of a request. To create an access list, you create a name (an arbitrary string), specify the type of access list (types are described below), and specify an argument that is used to match against the request. After creating an access list, you can specify that list for the following properties:

- Client Access Control
- Access to Cache via ICP
- ACLs for Cache Host
- URL Redirection

These properties are described below.

Access list definitions have the following form:

```
name type argument
```

Access list types are as follows:

- `src`
  Matches on the source address in a request. It takes an argument of the form: *ip_address*`/`*netmask*. You can specify multiple pairings of IP address and netmask.
- `domain`
  Matches on the domain specified in a URL. It takes an argument of the form: `.`*domain_name*. You can specify multiple domain names.
- `time`
  Matches on a time period specified in a URL. It takes an argument of the form: *day_of_the_week start_time*`-`*end_time*. The variable *day_of_the_week* is expressed as one of the following abbreviations:

TABLE 10-10 Day-of-Week Abbreviations

S	Sunday
M	Monday
T	Tuesday
W	Wednesday
H	Thursday
F	Friday
A	Saturday

The *start_time*-*end_time* variables are expressed as *hour*:*minutes*, using a 24-hour clock. For example, to express a period in the mid-afternoon, you specify `14:15-16:30`, meaning from 2:15 p.m. to 4:30 p.m.

- `pattern`
  Matches on a pattern specified in a URL. It takes an argument of the form: *pattern_to_be_matched*. You can specify multiple patterns.
- `port`
  Matches on a port number specified in a URL. It takes an argument of the form: *port_number*. You can specify multiple port numbers.
- `proto`
  Matches on a protocol specified in a URL. It takes an argument of the form: *protocol* (HTTP, FTP, Gopher, or WAIS). You can specify multiple protocols.
- `method`
  Matches on a method (`CONNECT`, `HEAD`, `POST`, or `GET`) specified in a URL. It takes an argument of the form: *method_name*. You can specify multiple methods.
- `service`
  Matches on the service specified in a request. It takes an argument of the form: *ip_address*/*netmask*. "Service," in this context, is an instance of a service on a Netra j proxy cache host, as identified by a service address and netmask.

Note – If you have multiple access lists of the same type, the Netra j proxy cache server, when determining which list a URL is in, works from top to bottom and stops after the first match.

The following is an example of an access list:

```
games domain game.com
```

This example creates an access list named `games` of type `domain`. This list includes all URLs containing a destination domain of `game.com`. In the HTTP Access property (described in TABLE 10-9 on page 191), you can, for example, deny access to the `games` list.

▼ To View or Modify Storage Management Properties

1. **In the Advance Proxy Cache Configuration page, click Storage Management.**

   The Storage Management page is displayed.

2. **Under “Storage Management,” enter or accept values for the following properties.**

TABLE 10-11 Storage Management Properties

Property	Description
High-water mark for Memory (%)	Removing of the least recently used objects in memory begins when the high-water mark is reached and ends when enough objects are removed so that the low-water mark (see following property) is reached. Note that objects removed from memory remain on disk. Enter a percentage. The default is 90%.
Low-water mark for Memory (%)	See the description of the high-water mark, above. Enter a percentage. The default is 75%.
High-water mark for Disk Cache (%)	Replacement of the least recently used objects in the disk cache begins when the high-water mark is reached and ends when enough objects are removed so that the low-water mark (see following property) is reached. Enter a percentage. The default is 90%.
Low-water mark for Disk Cache (%)	See the description of the high-water mark, above. Enter a percentage. The default is 75%.
Garbage Collection (GC) Rate (min)	Specifies how often, in minutes, the Netra j proxy cache server runs a full garbage collection. Garbage collection involves checking the expiration time of every object in the cache. In the course of normal operation, the Netra j proxy cache server removes expired objects so that explicit garbage collection is not necessary. This feature can be helpful if you have a frequent need to reclaim disk space. Note that the server does not process client requests during garbage collection. Enter a number of minutes if you want to use this feature, or leave the field blank to disable garbage collection.
Time of Day for GC (HH:MM:SS)	Enables you to schedule garbage collection at an off-peak time. Time is expressed on a 24-hour clock. For example, if you want garbage collection to occur at 3:30 a.m., enter `03:30:00`.

▼ To View or Modify Timeouts

1. **In the Advanced Proxy Cache Configuration page, click Timeouts.**

   The Timeouts page is displayed.

2. Under “Timeouts,” enter or accept values for the following properties.

TABLE 10-12 Timeout Properties

Property	Description
ICP Neighbor Timeout	The period of time after which ICP (InterCache Protocol) requests made to parent proxies will time out. The default is two seconds.
Timeout for Server Connections (sec)	The maximum duration, in seconds, the server waits for a connection to be established. The default is two minutes. See “Proxy Cache Connect Timeout and Parent Failover” on page 218 for a discussion of the relationship of this property to the operating system’s TCP connect timeout.
Read Timeout (min)	The duration beyond which the Netra j proxy cache server disconnects a connection on which no activity is occurring. The default value is 15 minutes.
Client Lifetime (min)	The maximum duration a client (browser) is allowed to remain connected to the cache process. This timeout prevents clients that go away without shutting down from consuming software resources. The default is 200 minutes (3 hours, 20 minutes). If you have high-speed client connectivity or occasionally run out of file descriptors, you might want to reduce the default number.
TTL for Negative Caching of Objects (min)	The server caches the fact that a cache request failed (for example, the object identified by a specified URL cannot be found). This negative caching lasts for the number of minutes specified for this property. The default is five minutes.
TTL for Successful DNS Lookups (min)	The server caches the result of a successful host name lookup for the duration specified for this property. The default is six hours. Note that the proxy cache service does not observe the TTL specified in a DNS record.
TTL for failed DNS Lookups (min)	The server can cache the fact that a host name lookup failed. The default is zero minutes, which means that, by default, the server does not perform this type of negative caching.

▼ To View or Modify Log File Options

- **In the Advanced Proxy Cache Configuration page, click Log File Management.**

  The Log File Management page is displayed. For instructions on using this page, see “Administering Proxy Cache Service Log Files” on page 204.

▼ To View or Modify Web Server Accelerator Options

1. **In the Advanced Proxy Cache Configuration page, click Web Server Accelerator Options.**

   The Web Server Accelerator Options page is displayed.

2. **Under "Web Server Accelerator Options," enter or accept values for the following properties.**

TABLE 10-13 Web Server Accelerator Properties

Property	Description
Host for Real HTTP Server	The Netra j proxy cache server can act as a front end for an HTTP server. This function is sometimes referred to as an *HTTP accelerator*. This feature can be useful under the following conditions: • If the Netra j proxy cache server is more powerful or more highly available than the HTTP server. • If the HTTP server is connected to a slow network, while clients have relatively fast connectivity to the Netra j proxy cache server. The Netra j proxy cache server hides the effects of the slow link. • If the HTTP server is vulnerable to attack. The Netra j proxy cache intercepts all requests. Also, you can set up an access list to limit the effect of an attack. A potential disadvantage of this feature is that the HTTP server does not have available the source IP address of clients. Enter the fully-qualified hostname of the server for which the Netra j proxy cache server is acting as a front end.
Port for Real HTTP Server	The HTTP port on the server for which the Netra j proxy cache server is acting as a front end. (See the preceding property.)
% Main Memory for Caching Objects	The percentage of memory used for keeping a number of web objects. If you are using the Netra j proxy cache server as a front end for an HTTP server, use a value of 12.5 (percent).
Enable Proxy Mode Also	This property determines whether a Netra j proxy cache server is acting as a front end, caching only the URLs of the HTTP server being "accelerated" or caches URLs from all web servers. Accept the default value of off, or select on to enable caching of URLs from all servers.

▼ To View or Modify External Program Options

1. **In the Advanced Proxy Cache Configuration page, click External Program Options.**

   The External Program Options page is displayed.

2. **Under the External Program Options heading, enter or accept values for the following properties.**

TABLE 10-14 External Program Properties

Property	Description
FTP User	The string supplied as the login password for anonymous `ftp`. This enables you to supply an informative address, if you want.
Options for 'ftpget'	The arguments supplied to the `ftpget` command. The `ftpget` command retrieves FTP data for the cache. HTTP and Gopher protocol support are built into the proxy cache software. To view a list of valid `ftpget` arguments, invoke `/opt/SUNWcache/lib/ftpget`, with no arguments.
No. of Processes for DNS Lookups	The number of processes spawned by the Netra j proxy cache server to service DNS name lookups. This number indicates the maximum number of concurrent DNS lookups. On heavily loaded caches, you might want to increase this value from the default of 5 to 10. The maximum is 32.

Configuring SNMP Services

The SNMP Configuration page enables you to set up user groups with permissions for performing the following SNMP actions:

- Reading variables from the Netra j proxy cache server Management Information Base (MIB)
- Changing the settings of variables from that MIB
- Receiving traps generated by the Netra j proxy cache server agent

▼ To Configure SNMP Services

1. **In the Proxy Cache Administration page, click SNMP configuration.**

   The SNMP Configuration page is displayed.

2. **Under the SNMP Configuration Parameters heading, enter or accept values for the following properties.**

TABLE 10-15 SNMP Configuration Parameters

Parameter	Description
SNMP Manager	SNMP Managers are hostnames of machines that will receive SNMP traps from the Netra j proxy cache server agent. This should be the same set of machines that is running your SNMP management platform.
SNMP Read Community	The name of a user group with permission for reading variables from the Netra j proxy cache server MIB.
SNMP Write Community	The name of a user group with permission for changing the settings of variables read from the Netra j proxy cache server MIB.
SNMP Trap Community	The name of a user group with permission for receiving traps generated by the Netra j proxy cache server agent.

Backing Up and Restoring the Proxy Cache Service Configuration

This section describes the procedures for backing up and restoring the Netra j proxy cache configuration.

Backing Up Your Configuration

You can back up your proxy server configuration by using the Save/Restore link in the Netra j Main Administration page.

▼ To Back Up a Proxy Cache Configuration

1. **Insert your backup diskette in the diskette drive of the host being restored.**
2. **In the Netra Main Administration page, click Save/Restore.**
3. **In the Save/Restore page, click Save configuration to diskette.**

Restoring Your Configuration

Assuming you have backed up your configuration to diskette (see the preceding section), you can subsequently restore that configuration to your server. Use the Save/Restore link in the Netra j Main Administration page (see the preceding procedure).

Monitoring a Netra j Proxy Cache Server

This section explains how to monitor a Netra j proxy cache server through the Netra Administration web pages. You can also monitor the server through log traces or through an SNMP-conformant management platform. See "Proxy Cache Log Files" on page 202 and "Configuring SNMP Services" on page 197.

▼ To Load the Host Status or Proxy Cache Monitoring Pages

- **In the Proxy Cache Administration page, click Host Status to monitor the server, or Proxy Cache Monitoring to view statistics related to the operation of the proxy cache service.**

Host Status

When you click the Host Status link in the Proxy Cache Administration page, the Host Status page is displayed.

When you load the Host Status page, a snapshot of current host activity is displayed. To obtain the latest statement of host activity, click on your browser's Reload button to refresh the latest host activity statistics.

There is a single table in the Host Status page.

TABLE 10-16 Table on Host Status Page

Table	Description
Test Objects	A test object is a software object that runs on a host to test a specific component of that host, such as the integrity of an interface or the existence of a process. A test object returns OK (yes) or not-OK (no) for the object it tests. There is a man page for each test object.

Proxy Cache Monitoring

When you click the Proxy Cache Monitoring link in the Proxy Cache Administration page, the Proxy Cache Monitoring page is displayed. This page presents a snapshot of current proxy cache statistics. Click on your browser's Reload button to refresh the latest proxy cache statistics.

The tables in the Proxy Cache Monitoring for Host page are listed below.

TABLE 10-17 Tables on the Proxy Cache Monitoring for Host Page

Table	Description
Proxy Cache URL Statistics	Provides statistics on the rate of URL requests and the extent to which requests are serviced from the local cache.
Proxy Cache Connection Statistics	Provides statistics on HTTP and SSL connections.
Cached Object Statistics	Provides statistics on the number of objects cached, for each type of object.

The headings for these tables are described in the following tables.

In the Proxy Cache URL Statistics table, under *Totals (since start)*:

TABLE 10-18 Proxy Cache URL Totals

Total	Description
# URLs accessed	The number of requests for a URL fielded by the Netra j proxy cache server.
# Hits	The number of URL requests for which the Netra j proxy cache server was able to return an object from its own cache.
% Hits	The number of URLs accessed divided by the number of hits. This number tells you the extent to which the Netra j proxy cache server is able to respond to URL requests from the local cache.

Under *Delta (since reset counter)*:

TABLE 10-19 Proxy Cache URL Deltas

Delta	Description
URLs/sec	The rate at which URL requests are being fielded by the Netra j proxy cache server since the reset counter was last set to zero.
Hits/sec	The rate at which the Netra j proxy cache server was able to find requested objects in a local cache, since the reset counter was last set to zero.
% Hits	The number of URLs accessed divided by the number of hits, since the reset counter was last set to zero.

In the Proxy Cache Connections Statistics table:

TABLE 10-20 Proxy Cache Connections Statistics

Statistic	Description
Connection Type	Has rows for HTTP and SSL connections and for established connections.
Totals (since start)	The total number of connections for each connection type, HTTP and SSL, since the last reboot of the host.
Current	The number of current connections for each connection type, HTTP and SSL, and the number of current established connections.

In the Cached Object Statistics table:

TABLE 10-21 Cached Object Statistics

Statistic	Description
Connection Type	HTTP, FTP, WAIS, or Gopher.
Size (KB) Cached	The size of all objects cached for a given object type.

Under *Number of Objects Cached*:

TABLE 10-22 Statistics on Number of Objects Cached

Statistic	Description
Total Cached Disk & Main Memory	The total number of objects cached on a host for a given object type.
Cached in Main Memory	The number of objects cached in main memory.

Proxy Cache Log Files

This section explains how to view and manage the proxy cache service log files. These log files are distinct from the log files accessed through the Log Files link on the Netra j Main Administration page. The log files described in this section relate only to the activity of the proxy cache service.

▼ To Load the Proxy Cache Log Administration Page

1. **In the Proxy Cache Administration page, click Log Files.**

   A page of administration options is displayed.

   You can view or clear each type of log file listed. If you choose to clear a log file, you are prompted to confirm the operation.

2. **Click OK to confirm.**

Note – Clearing a log file truncates the log file.

The log file types are described in the following table:

TABLE 10-23 Log File Types

Log File	Description
Proxy Cache Server log	Lists status messages related to the activity of the proxy cache service. By default, this log is turned on.
Proxy Cache Access log	Lists records of all client accesses to the Netra j proxy cache server. By default, this log is turned on.
Proxy Cache Hierarchy log	Contains information about which parent satisfied each request. By default, this log is turned off. See "To Enable Hierarchy and Store Logging" on page 203.
Proxy Cache Store log	A log of items stored in and removed from the cache, with type (protocol), size, and timestamp. By default, this log is turned off. See "To Enable Hierarchy and Store Logging" on page 203.
Configuration Installation Error Log	A log of errors or exceptional events that occurred when new configuration details were supplied to the proxy cache service via the Netra user interface.
Administration Client Error log	A log of errors that occur when the `cgi-bin` programs run from the administration web pages. This log can be useful when you encounter an unexpected and inexplicable failure when interacting with the web pages.
Administration Server log	A log of the daemon that maintains the configuration database.
Administration Server Error and Exception log	Records the `stdout` and `stderr` of the daemon referred to in the preceding item. Of use primarily to trained technical personnel.

▼ To Enable Hierarchy and Store Logging

1. **In a text editor, open the file `proxycache.conf`, stored in `/etc/opt/SUNWoam/config/proxy`.**

2. **Uncomment the line corresponding to the log file you want to enable.**

   For example, to enable both types of logging, uncomment the lines for `cache_hierarchy_log` and `cache_store_log`.

3. **In the uncommented lines, replace the word** `none` **with the location of the proxy cache service log files.**

   In the preceding example, the edited lines display as follows:

   ```
   cache_store_log /var/opt/SUNWcache/cachelogs/store.log
   cache_hierarchy_log /var/opt/SUNWcache/cachelogs/hierarchy.log
   ```

Administering Proxy Cache Service Log Files

From the Log File Management page, you can set up automatic rotation and backup of the following proxy cache service log files (each log type is shown in parentheses):

- Proxy Cache Server log (log type: `cache`)
- Proxy Cache Access log (log type: `access`)
- Proxy Cache Hierarchy log (log type: `hierarchy`)
- Proxy Cache Store log (log type: `store`)

At the time of day you specify, log files are rotated so that the current log file, *type*`.log`, becomes *type*`.log.0`; *type*`.log.0` becomes *type*`.log.1`; *type*`.log.1` becomes *type*`.log.2`; and so on. The highest-numbered (and oldest) file, *type*`.log.9`, is overwritten by *type*`.log.8`.

The log files are then stored locally or on a remote server, according to your settings.

▼ To Administer Proxy Cache Service Log Files

1. **In the Proxy Cache Log Administration page, click Administer Proxy Cache Server, Access, Hierarchy, and Store Logs.**

2. **In the Log File Management page, set file location and time of day options.**

TABLE 10-24 File Location and Time of Day Options

Option	Description
Maintain available space	Specifies that log files are stored in the local directory `/var/opt/SUNWcache/cachelogs`. This option enforces a minimum disk space allowance (the default value is 10 MB). If necessary, log files are deleted (starting with the oldest) until the specified amount of space is reached.
Transfer logs via FTP	Specifies that log files are transferred after rotation to a specified directory on a remote server via FTP.
Time of day	The time of day at which you want the log files to be rotated.

3. **Set parameters for local file maintenance or FTP delivery.**

- If Maintain available space is selected and you click Set Parameters, the following option is displayed.

TABLE 10-25 Maintain Available Space Option

Option	Description
Set Minimum Available Space To	The minimum amount of disk space that must be available in `/var/opt/SUNWcache/cachelogs` in addition to the log files.

- If Transfer logs via FTP is selected and you click Set Parameters, the following options are displayed.

TABLE 10-26 FTP Options

Option	Description
Logs To Transfer	The log file types (described earlier in this section) that will be transferred to the remote server.
Transfer Method	The mode (binary or ASCII) in which the FTP service will transfer the log files.
Hostname	The hostname of the remote system to which log files will be transferred.
Username	The username for the FTP account to be used for the transfer.

TABLE 10-26 FTP Options *(Continued)*

Option	Description
Password	The password for the FTP account to be used for the transfer.
Remote Directory	The remote directory to which log files will be transferred.
Log Filename Extension	An extension to be added to all log file names.

4. **Click Set log file options, and enter or accept values for the following properties:**

TABLE 10-27

Option	Description
Emulate HTTPD Log	By default, the server emulates the log file format used by many HTTP servers. Accept the default of on or select off to turn this feature off.
No. of Logfile Rotations	Specifies the number of log file rotations the server performs. With the default of 10, the software creates log files with extensions from `0` through `9`. Set this property to `0` to turn off log file rotation.
Log Directory	You do not have the option to change the default log-storage directory, `/var/opt/SUNWcache/cachelogs`, in the current release.

APPENDIX **A**

Network Computer Configuration Form

This form lists the information you need to set up and configure network computers (NCs) in a Netra j 3.0 network environment. Refer to the Netra j 3.0 *Administrator's Guide* for instructions configuring the Netra j 3.0 server for NCs.

Enter the information recorded on this form into the Name Service administration pages and Network Computer Server administration pages of the Netra j 3.0 administration interface.

TABLE A-1

Page Name	Field Name	Description	Your System Information
Ethernet TCP/IP Interface	Host Name/ Address	The host address or host name for this interface.	________
	Netmask	The netmask for this interface.	
Web Server Document Root	Select Web Server	Select the default web server, which is the web server running on this system at port 80.	________
	Full Path Name of the Document Root	Enter the absolute path name of the default web server's document root.	
Global Parameters	Boot Server Address	The host address of the NC boot server on the local network. The boot server provides DHCP, TFTP, and NFS services.	________
	Time Server Address	The IP address of a server supporting the NTP protocol.	________
	DNS Domain Name	The DNS domain where the NCs reside.	________
	DNS Server Address(es)	The host address of the DNS server for the NCs.	

TABLE A-1

Page Name	Field Name	Description	Your System Information
	NIS Domain Name (optional)	The NIS domain in which the NCs reside.	
	NIS Server Address(es) (optional)	The host address(es) of the NIS servers for the NCs.	
	Router Address(es) (optional)	The host address(es) of the routers to be used by the NCs. If not specified, the JavaOS™ software on each NC will broadcast looking for a router.	
	Lease Time (in days)	The duration (in days) of an IP address lease. IP addresses are leased to NCs, not assigned permanently. For more information, refer to the Netra j 3.0 *Administrator's Guide.*	
	Lease Negotiation	A yes or no value that specifies whether the boot server renews the IP address leases of clients requesting lease renewal.	
	Network Interfaces	A list of the network interfaces accessible to the Netra j 3.0 system. Each interface is associated with a physical device. However, a physical device can have multiple network interfaces.	
	Time Zone	The time zone in which the NCs are located.	
Add A Network Computer	Host Name	The host name of the NC.	
	MAC Address	The MAC address of the NC. This address is a unique assigned number built into the hardware of the computer and displayed at boot time.	
	Host Address	The host address of the NC.	
	Enter Lease Time	The duration (in days) of an IP address lease. IP addresses are leased to NCs, not assigned permanently. For more information, refer to the Netra j 3.0 *Administrator's Guide.*	
	Default Application	Select the application to be run on this NC.	
	Select NC locale	Select the language to be used at this NC.	

TABLE A-1

Page Name	Field Name	Description	Your System Information
	Select Keyboard	Select the native keyboard to be used at this NC.	
	Vendor Specific Options (optional)	Vendor specific options, (JavaOS properties) to be delivered to this NC during boot-up.	
Add Multiple Network Computers	Host Name Prefix	The common prefix of a group of automatically generated host names.	
	Starting IP address	The starting IP address when sequential addresses are generated for the NCs.	
	Number of NCs	The number of network computers for which addresses are generated.	
	Enter Lease Time	The duration (in days) of an IP address lease. IP addresses are leased to NCs, not assigned permanently. For more information, refer to the Netra j 3.0 *Administrator's Guide.*	
	Default Application	Select the application to be run on the NCs.	
	Select NC locale	Select the language to be used at the NCs.	
	Select Keyboard	Select the native keyboard to be used at the NCs.	
	Vendor Specific Options (optional)	Vendor specific options, (JavaOS properties) to be delivered to the NCs during boot-up.	
DNS Client Administration	DNS Domain Name	The DNS domain that will be used to resolve partially-qualified host names. Usually, this is the local domain name.	
	Name Server 1 Address	The host address of the DNS server that will be tried first for all DNS queries.	
	Name Server 2 Address (optional)	The host address of the DNS server to use, if the first name server is unreachable.	
	Name Server 3 Address (optional)	The host address of the DNS server to use, if the first two name servers are unreachable.	

TABLE A-1

Page Name	Field Name	Description	Your System Information
Basic DNS Server Configuration	DNS domain name	Enter the name of the DNS domain in which the Netra server resides (or will reside on completion of the DNS configuration).	
	DNS administrator's user name	Enter the name or alias of the local user (e.g. root) who is responsible for DNS.	
	Root Name Server/ IP Address	The fully-qualified host names and host addresses of a set of DNS servers that can be contacted to resolve name queries.	
Add DNS Primary Domain	Host Names/Host Addresses	The host names and corresponding host addresses of the hosts in the domain.	
	Host Aliases/Host Names	Enter alias names for hosts in the domain followed by a known name of the host.	
	Mail Addresses/ Preferences/Mail Servers	Use this field if people are expected to send mail to the domain rather than directly to the mail server.The preference value (an integer) determines which mail server to use if the domain has more than one: the lower the value, the higher the priority of the corresponding mail server.	
	Domains/DNS Servers	Enter records for other DNS servers. Each record should consist of the name of the domain which the server is responsible for followed by the name of the server.	

TABLE A-1

Page Name	Field Name	Description	Your System Information
Advanced Global Parameters, Localization Properties (optional)	Input Method Server (optional)	A server with a language engine to interpret the keyboard input method (for Korean, Chinese, and Japanese languages only). This server must be running a localized version of Solaris.	
	Input Method Port (optional)	The port where the input method server's language engine is accessible.	
	Fonts Server (optional)	The host address or host name of the fonts server for the NCs. A fonts server is required for Asian locales and if alternate fonts will be used by the NCs. For more information, refer to the Netra j 3.0 *Administrator's Guide.*	
	Fonts Directory (optional)	The directory location of the fonts on the font server for the NCs.	
	Localized Resources Server (optional)	The host address or host name of the localized resources server for the NCs. Localized resources, such as keyboard mapping tables, support NC operation in different languages. For more information, refer to the Netra j 3.0 *Administrator's Guide.*	
	Localized Resources Directory (optional)	The directory location of the localized resources for theNCs.	
	Login Locales List (optional)	The list of locales presented as choices to the user logging on to an NC.	

APPENDIX **B**

Proxy Cache Reference

This chapter contains reference information and advanced procedures for the Netra j proxy cache service.

Advanced Proxy Cache Configuration Examples

This section describes >..the following advanced configuration scenarios:

- Domains Inside Firewall and Local Domains Inside the Firewall
- Limiting Access to the Server

Domains Inside Firewall and Local Domains Inside the Firewall

See "To View or Modify Proxy Cascade Properties" on page 183 for a description of the properties described in this section.

If you have a hierarchy of proxy cache servers, you can use the Netra j proxy cache software's "local domain" features, illustrated in the following figure.

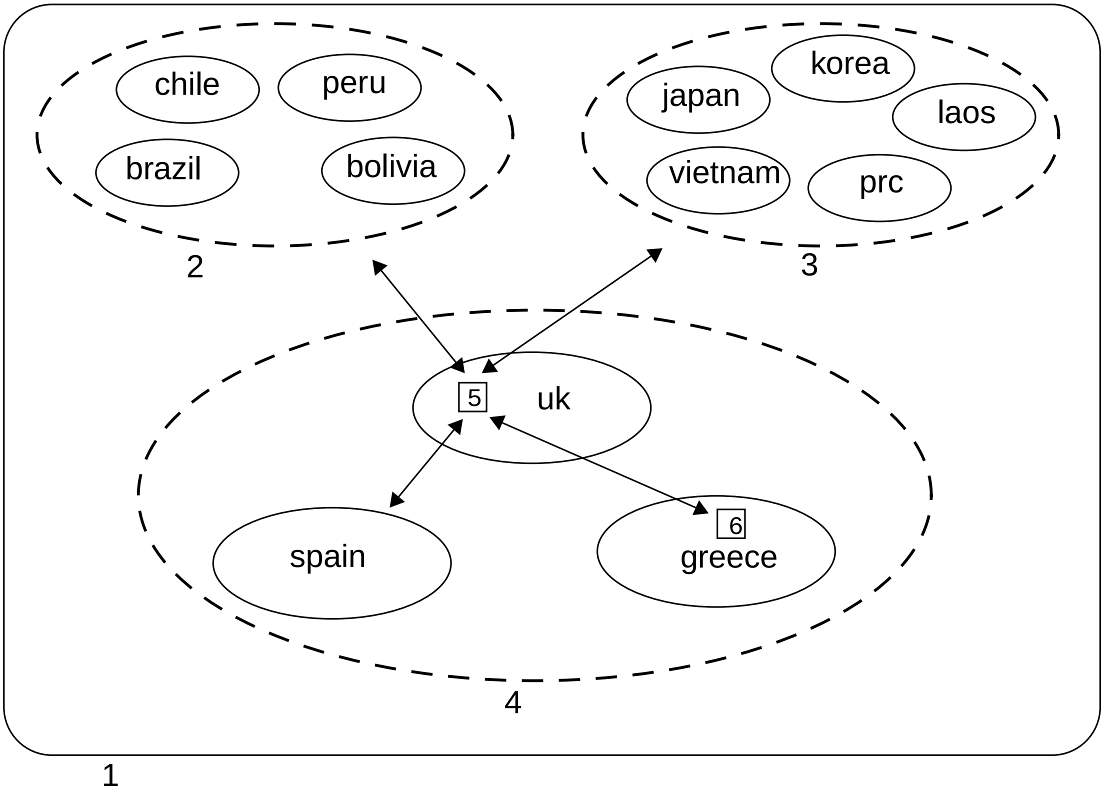


FIGURE B-1 Example of Use of Local Domain Property

Legend:

1. DNS domain `acme.com`
2. The following DNS domains are in the geographic region of South America:
   a. `chile`
   b. `peru`
   c. `brazil`
   d. `bolivia`
3. The following DNS domains are in the geographic region of Asia:
   a. `japan`
   b. `korea`

c. laos

d. prc

e. vietnam

4. The following DNS domains are in the geographic region of Europe:

a. uk

b. greece

c. spain

5. Netra j proxy cache server netra_cache.uk

6. Netra j proxy cache server netra_cache.greece

In this example, the configuration for the Netra j proxy cache server netra_cache.greece (6) is as follows:

- Parent proxy/cache: netra_cache.uk
- Inside-the-firewall domain: acme.com
- Local domain inside the firewall: greece.acme.com, spain.acme.com, uk.acme.com

The effect of these configuration options for the machine netra_cache.greece is that, in general, HTTP requests containing acme.com are retrieved from the parent, netra_cache.uk. However, requests for the local domain, greece, are retrieved directly from the local web server.

Limiting Access to the Server

See "To View or Modify Access Control Properties" on page 190 for a description of the properties you use to limit access to the Netra j proxy cache server.

To limit access to the server, you define a filter in the Access List Definition property, then specify one or more filters for the following properties:

- Client Access Control
- Access to Cache via ICP
- ACLs for Cache Host
- URL Redirection

When you specify multiple entries for any of the preceding properties, list the lines in the order from the most exclusive (smallest set) toward the most inclusive (largest set). In processing multiple entries, the proxy cache service evaluates entries from top to bottom, stopping at the first entry that matches a URL request.

When you specify multiple access lists for a given property, those lists are ANDed.

Limiting by Source Address

The following are example access lists:

Under Access List Definition:

```
eng src 129.144.118.0/255.255.255.0
sales src 129.144.130.0/255.255.255.0
division src 129.144.0.0/255.255.0.0
```

The preceding access lists might be used as follows:

Under Client Access Control:

```
allow eng sales
deny division
```

The preceding entries specify that machines on the subnets 129.144.118.0 and 129.144.130.0 are allowed HTTP access to the Netra j proxy cache server, while machines in the `division` list are excluded.

You might want to restrict Inter Cache Protocol (ICP) access to a server to only those machines. This is illustrated in the following example:

Under Access List Definition:

```
arrayhosts src 129.144.107.1/255.255.255.255 129.144.107.2/255.255.255.255 \
129.144.107.3/255.255.255.255 127.0.0.1/255.255.255.255
all src 0.0.0.0/0.0.0.0
```

Limiting by Time

The following are example access lists:

Under Access List Definition:

```
nights time M-F 17:01-07:59
weekends time A-S 00:00-24:00
worktime time M-F 08:00-1700
```

The preceding access lists might be used as follows:

Under Client Access Control:

```
deny nights weekends
allow worktime
```

Note that A is the abbreviation for Saturday and S for Sunday.

Limiting by Domain in Request

The following are example access lists:

Under Access List Definition:

```
poets domain .poetry .rhyme
sports domain .espn .cnnsi
cooks domain .culinary .gourmet
```

The preceding access lists might be used as follows:

Under Client Access Control:

```
deny poets sports cooks
```

You might want to allow users access to the cache for non-work-hours web access. The following example uses time-based access lists defined in the preceding subsection.

Under Client Access Control:

```
deny worktime poets sports cooks
allow nights weekends poets sports cooks
```

Redirecting Requests

The following are example access lists:

Under Access List Definition:

```
politics domain .rightwing .leftwing
pop_culture domain .disney .twarner
```

The preceding access lists might be used as follows:

Under URL Redirection:

```
politics : HOST www.vatican.net PATH /index.html
pop_culture : HOST lcweb.loc.gov PATH /homepage/lchp.html
```

The effect of the preceding lines is that URL requests that match the `politics` filter are redirected to `http://www.vatican.net/index.html`. Requests that match `pop_culture` are redirected to `http://lcweb.loc.gov/homepage/lchp.html`.

Technical Information

This section describes the following technical information about the proxy cache software.

- System Administrator and Proxy Webmaster Aliases
- Proxy Cache Connect Timeout and Parent Failover
- Rules for Pattern Matching for TTL Selection Property

System Administrator and Proxy Webmaster Aliases

Netra j proxy cache software enables you to establish email recipients for mail that is addressed to `root@`*netra_host_name* or `Postmaster@`*netra_host_name*. When entering email addresses, make sure you specify addresses in a form compatible with your `sendmail` configuration. For example, if your mail system expects an address of a form *login@nis_domain_name*, mail sent to *login@host_name* is undeliverable.

Proxy Cache Connect Timeout and Parent Failover

The Netra j proxy cache server supports parent failover, in which, if the server's parent fails, the server switches to the next parent on its list. (See "To View or Modify Proxy Cascade Properties" on page 183 for a description of the table of parent proxies.) Failover occurs if the Netra j proxy cache server's TCP connect call fails, not if the proxy cache service's connect timeout (2 minutes, by default) is exceeded. (See "To View or Modify Timeouts" on page 194 for a description of the Timeout for Server Connections property.)

A TCP connect call might fail because the operating system's timeout (3 minutes, by default) is exceeded or from some other cause. If the proxy cache service's timeout is shorter than the operating system's (as is true for the default case), the connect attempt is terminated before an error is returned, with the result that parent failover does not occur.

If your server experiences frequent connection timeouts when attempting to connect to a parent, you can set the proxy cache service's connect timeout to be at least 10 seconds greater than the operating system's TCP connect timeout. Alternatively, (if you have a serial connection to your server) you can reduce the operating system's timeout. To change the operating system's timeout, use the `ndd` command, which takes arguments in milliseconds. For example:

```
# ndd -set /dev/tcp tcp_ip_abort_cinterval 30000
```

The preceding command sets the TCP connect timeout to 30 seconds. To view the current TCP connect timeout, enter:

```
# ndd /dev/tcp tcp_ip_abort_cinterval
```

Rules for Pattern Matching for TTL Selection Property

Listed below are the rules for pattern matching used for the *reg_expression* component of the TTL Selection Based on URL property, described in "URL Policy" on page 188. These rules are taken from Section 3C of the Solaris `regexec` man page.

1. If subexpression `i` in a regular expression is not contained within another subexpression, and it participated in the match several times, then the byte offsets in `pmatch[i]` will delimit the last such match.

2. If subexpression `i` is not contained within another subexpression, and it did not participate in an otherwise successful match, the byte offsets in `pmatch[i]` will be -1. A subexpression does not participate in the match when:

- `*` or `\{ \}` appears immediately after the subexpression in a basic regular expression, or `*`, `?`, or `{}` appears immediately after the subexpression in an extended regular expression, and the subexpression did not match (matched zero times) or

- | is used in an extended regular expression to select this subexpression or another, and the other subexpression matched.

3. If subexpression i is contained within another subexpression j, and i is not contained within any other subexpression that is contained within j, and a match of subexpression j is reported in pmatch[j], then the match or non-match of subexpression i reported in pmatch[i] will be as described in 1. and 2. above, but within the substring reported in pmatch[j] rather than the whole string.

4. If subexpression i is contained in subexpression j, and the byte offsets in pmatch[j] are -1, then the pointers in pmatch[i] also will be -1.

5. If subexpression i matched a zero-length string, then both byte offsets in pmatch[i] will be the byte offset of the character or NULL terminator immediately following the zero-length string.

Adding a SCSI Disk

Depending on the hit rate experienced by your server, the size of cached objects, and client usage patterns, adding disk space can improve the performance of your server. Such an improvement would be manifested in reduced response time for users and decreased network traffic between the proxy server and its parents.

Adding a SCSI Disk includes three procedures:

- Installing the new SCSI disk
- Formatting the disk
- Configuring new file systems

For these procedures, you must have a serial connection to the Netra j proxy cache server.

▼ To Install a SCSI Disk

In the procedure specified below, for purposes of this example, assume the following:

- You are adding a six-disk Sun StorEdge™ MultiPack enclosure to the existing SCSI controller (controller 0, or c0).
- You will use all of the space on all of the disks in the enclosure for caching.
- You will use slice (partition) 0 for all of the available space on a disk.
- The disks in the MultiPack enclosure are formatted at the factory.

1. **Set the address switch on the back of the MultiPack enclosure to 9–14.**

   The two internal disks are `c0t0` and `c0t1`. For controller 0, you can use target numbers other than 0, 1, and 6, which is used by the CD-ROM drive.

2. **Halt your machine.**

   In the Netra j Main Administration page, click Restart and Shutdown. In the Restart and Shutdown Administration page, click the Shutdown and power off operation and leave the check box for “Check for new devices upon restart” set to Yes. Click OK.

3. **Ensure that the server is powered off (after about 90 seconds).**

   The green indicator light on the front of your machine is off when the machine is powered off.

4. **Connect the MultiPack enclosure to the SCSI port on the back of the server.**

5. **Power on the enclosure.**

▼ To Format the New Disk

1. **Power on the Netra j machine and log in as root.**

2. **Invoke `format`:**

```
# format
```

3. **In the available-disk menu, select `2`, for the first available disk after the two internal disks.**

   In this menu, there are eight disks: 0 and 1 for the internal disks and 2 through 7 for the disks in the MultiPack enclosure.

4. **If the disk is new, you are asked whether to label the disk. Enter `y` to label the disk now.**

5. **In the `format` menu, enter `p` for partition.**

6. **In the partition menu, enter `m` to modify a partition table.**

7. **In response to the Select partitioning base menu, enter the number to select “modify the current partition table.”**

   The current partition table is displayed.

8. **In the displayed partition table, make a note of the number of cylinders for slice (partition) 2.**

9. **Press Return to indicate that, yes, you want to create a new partition table.**

10. **Press Return to accept the default partition number (for example,** 6**) for the free hog partition.**

11. **Enter the number of cylinders noted in Step 8 for the size of partition 0.**

    For example, `4101c`, to indicate 4101 cylinders.

12. **Except for the partition number for the free hog partition, enter a size of 0 for the remaining partitions. For the free hog partition, press Return to accept the default.**

    After making or accepting an entry for each partition, the partition table is displayed.

13. **Press Return to OK the current partition table or enter** `n` **to make changes.**

14. **After confirming your partition table, you are prompted to enter a table name. Enter a name enclosed in quotes.**

    For example, `"added_cache1"`, for the first disk in a MultiPack enclosure.

15. **If the disk is not a new disk, you are asked whether you are ready to label the disk. Enter** `y` **to label the disk.**

16. **Enter** `q` **at the** `partition>` **prompt.**

17. **Enter** `disk` **at the** `format>` **prompt, to return to the available-disk menu.**

18. **Repeat Step 3 through Step 16 for each disk in the MultiPack enclosure.**

    For Step 3, enter the number that corresponds to the disk whose partition map you are modifying.

19. **After you modify the partition map for the last disk in your MultiPack enclosure, enter** `q` **at the** `format>` **prompt (see Step 17), to exit** `format`**.**

▼ To Configure New File Systems

1. **For each disk in the MultiPack enclosure, enter a** `newfs` **command of the following form:**

```
# newfs /dev/rdsk/c0tnumd0s0
```

where *num* is, in succession, 9, 10, 11, 12, 13, and 14.

Each instance of the `newfs` command takes a few minutes.

2. **Edit `/etc/vfstab` to add the new partitions.**

   The original `vfstab` contains:

```
# cat /etc/vfstab.orig
#device         device          mount           FS      fsck    mount   mount
#to mount       to fsck         point           type    pass    at boot options
#
#/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr          ufs     1       yes     -
fd      -       /dev/fd fd      -       no      -
/proc   -       /proc   proc    -       no      -
/dev/dsk/c0t0d0s1       -       -       swap    -       no      -
/dev/dsk/c0t1d0s1       -       -       swap    -       no      -
/dev/dsk/c0t0d0s0      /dev/rdsk/c0t0d0s0      /       ufs     1       no      -
/dev/dsk/c0t1d0s0      /dev/rdsk/c0t1d0s0      /var    ufs     1       no      -
this line continued from previous line ufs     2       yes     -
this line continued from previous line ufs     2       yes     -
swap    -       /tmp    tmpfs   -       yes     -
```

Using the disks in our example MultiPack enclosure, add lines such as the following to `vfstab`:

```
# The following disks were added to extend the cache
/dev/dsk/c0t9d0s0       /dev/rdsk/c0t9d0s0      /var/opt/SUNWcache/cache3
this line continued from previous line ufs     2       yes     -
/dev/dsk/c0t10d0s0       /dev/rdsk/c0t10d0s0      /var/opt/SUNWcache/cache4
this line continued from previous line ufs     2       yes     -
/dev/dsk/c0t11d0s0       /dev/rdsk/c0t11d0s0      /var/opt/SUNWcache/cache5
this line continued from previous line ufs     2       yes     -
/dev/dsk/c0t12d0s0       /dev/rdsk/c0t12d0s0      /var/opt/SUNWcache/cache6
this line continued from previous line ufs     2       yes     -
/dev/dsk/c0t13d0s0       /dev/rdsk/c0t13d0s0      /var/opt/SUNWcache/cache7
this line continued from previous line ufs     2       yes     -
/dev/dsk/c0t14d0s0       /dev/rdsk/c0t14d0s0      /var/opt/SUNWcache/cache8
this line continued from previous line ufs     2       yes     -
```

Note that the mount points, `/var/opt/SUNWcache/cache`*num*, are present in the Netra j proxy cache software distribution.

3. **Reboot.**

   In the Netra j Main Administration page, click Restart and Shutdown. In the Restart and Shutdown Administration page, click the Restart operation and leave the check box for “Check for new devices upon restart” set to Yes. Click OK.

   Upon rebooting, in the console window, you receive output such as the following:

```
Disk configuration has changed.
New filesystem detected: /var/opt/SUNWcache/cache3
New filesystem detected: /var/opt/SUNWcache/cache4
New filesystem detected: /var/opt/SUNWcache/cache5
New filesystem detected: /var/opt/SUNWcache/cache6
New filesystem detected: /var/opt/SUNWcache/cache7
New filesystem detected: /var/opt/SUNWcache/cache8
Disk configuration has changed.
Reconfiguring the cache. Please wait.
This operation should take no more than 5 minutes.
Current time is: Fri Dec  5 11:06:04 PST 1997

0          1           2          3           4          5 (min)
|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|
                                                            DONE
The cache has been reconfigured.

oamserver in stop state
The system is ready.

host_name console login:
```

   At this point, the proxy cache service can begin to use the additional disks for caching web objects.

APPENDIX **C**

Netra j Package Information

This appendix describes the packages included in the Netra j 3.0 software.

- "Netra j 3.0 Administration Interface" on page 225
- "Network Computer Software" on page 226
- "Solaris 2.5.1 Add-ons" on page 226
- "OpenConnect System Software" on page 228
- "Additional Software" on page 228

Netra j 3.0 Administration Interface

The Netra j 3.0 administration interface is the web-based graphical user interface (GUI) you use to set up and configure the servers and clients needed in your network environment. The Netra j 3.0 administration interface comprises the following packages:

TABLE C-1 Netra j 3.0 Software Packages

Package Name	Package ID
HTTP server root package	`SUNWhttpr`
HTTP server user package	`SUNWhttpu`
HTTP server var package	`SUNWhttpv`
Netra Java Server Administration	`SUNWjsA`
Netra j HotJava Browser for Solaris	`SUNWnhjb`
Netra Required Functionality	`SUNWntr`
Netra j Server Administration	`SUNWntrj`
Netra Server Administration	`SUNWntrjs`

TABLE C-1 Netra j 3.0 Software Packages *(Continued)*

Package Name	Package ID
SSL 1.0 Software (Library Global Version)	SUNWssl
Sun Internet Mail Server	SUNWimap
Solstice Internet Mail POP3 server	SUNWipop

Network Computer Software

These software packages provide the operating system, boot image, and client applications for the NCs.

TABLE C-2 Network Computer Software Packages

Package Name	Package ID
JavaOS 1.1, inetboot images	SUNWjsos
HotJava Views 1.1.3	SUNWjdt
HotJava Views Documentation	SUNWjdtdc
HotJava Views Demo Support	SUNWjdtd
HotJava Browser 1.1.4	SUNWjshjb

Solaris 2.5.1 Add-ons

Netra j 3.0 also includes Solaris 2.5.1 add-on software. The following software is required for systems running the Solaris 2.5.1 operating environment. If these packages are not already installed on the system, then Netra j adds them to the server.

TABLE C-3 Solaris 2.5.1 Add-ons

Package Name	Package ID
PPP/IP Asynchronous PPP daemon	SUNWapppr
PPP/IP Asynchronous PPP daemon	SUNWapppu
Networking UUCP Utilities	SUNWbnur

TABLE C-3 Solaris 2.5.1 Add-ons

Package Name	Package ID
Networking UUCP Utilities	SUNWbnuu
System Localization	SUNWloc
PPP/IP and IP dialup	SUNWpppk
X Windows optional fonts	SUNWxwoft
NIS Kit 1.2	SUNWnsktr, SUNWnsktu, and SUNWnskta (AnswerBook Documentation)
Dynamic Host Configuration Protocol (DHCP)	• Federated Naming System – SUNWfns • BOOTP/DHCP server services (root) SUNWdhcsr • BOOTP/DHCP server services (usr) – SUNWdhcs
Other packages	SUNWdhcsu,SUNWsprot,SUNWmibii,SUNsacom, SUNWsadmi,SUNWsasnm,SUNWjvrt,SUNWjvjit

Solaris 2.6 Add-ons

If the following packages are not already installed on Solaris 2.6 system, then Netra j adds them to the server.

TABLE C-4 Solaris 2.6 Add-ons

Package ID	
SUNWbtool	SUNWapppu
SUNWscplp	SUNWbnur
SUNWsprot	SUNWbnuu
SUNWdhcsr	SUNWloc
SUNWdhcsu	SUNWypu
SUNWpppk	SUNWypr
SUNWapppr	SUNWxwoft

OpenConnect System Software

The OC://WebConnect and OpenVista software enables clients that use Java technology to access data and applications on IBM mainframes and on midrange computers from many vendors. OC://WebConnect is a Java applet that provides 3270, 5250, and VT220 terminal emulation with any web browse that can use Java technology.

TABLE C-5 OpenConnect System Software

Package Name	Package ID
OpenVista	`OCSvista`
OC://WebConnect	`OCSwcd`

Additional Software

Sun WebServer software enables companies to publish and distribute information and deploy web-based applications across any network environment.

TABLE C-6 Sun WebServer Packages

Package Name	Package ID
Sun WebServer SKI 1.0 Software (User Package)	`SUNWski`
Sun WebServer SKI 1.0 Software (CA Package)	`SUNWskica`
Sun WebServer SKI 1.0 Software (Licensing Package for CA)	`SUNWskicw`
Sun WebServer SKI 1.0 Software (CA Manual Page Package)	`SUNWskimc`
Sun WebServer SKI 1.0 Software (User Manual Page Package)	`SUNWskimu`

GO-Joe is a thin-client X server that provides access to all UNIX and X Window applications, including browsers such as HotJava Browser.

TABLE C-7 GO-Joe Packages

Package Name	Package ID
GO-Joe Virtual X Server 2.0	`SUNWgjvxs`
GO-Joe Virtual X Viewer 2.0	`SUNWgjvxv`

Solaris 2.6 customers can also view the *Netra j collection* online documentation, which includes the *Netra j 3.0 Installation Guide* and *Netra j 3.0 Administrator's Guide*. Refer to the *Information Library for Solaris 2.6 (SPARC Platform Edition)* included with the Solaris 2.6 CD for installation procedures.

TABLE C-8 Netra j Collection for Solaris 2.6

Package Name	Package ID
Netra j 3.0 Collection	`SUNWnjdoc`

Packages Removed During Install

Netra j removes the following packages if they exist. These packages were part of previous netra products. There are NO Solaris packages or non-netra packages.

TABLE C-9 Packages Removed During Install

Package ID		
SUNWjsA	SUNWaftpA	SUNdntri
SUNWnrwA	SUNWntrA	SUNWintri
SUNWappA	SUNWntriP	SUNWsntri
SUNWenntr	SUNWntrnA	SUNWentri
SUNWntrjP	SUNWntrnp	SUNWcntri
SUNWtcpwp	SUNWntrpg	SUNWkntri
SUNWuserA	SUNWpkgA	SUNWhntri
SUNWswA	SUNWsbhtp	SUNWfrntr
SUNWnsA	SUNWswapA	SUNWdentr
SUNWmailA	SUNWtaskA	SUNWitntr
SUNWisdnA	SUNWdocsA	SUNWsvntr
SUNWhsiA	SUNWpop	SUNWesntr
SUNWdiskA	SUNWprxyA	SUNWcntr
SUNWbkupA	SUNWjantr	SUNWkontr
SUNWatmA	SUNWjntri	SUNWhntr
SUNWapppA	SUNfntri	

Other Packages Added

If any of the following packages do not exist on the server then we install them. If the same version or a later version of the package is already installed, then Netra j does not install these packages. Netra j replaces older packages with the newer ones.

TABLE C-10 Other Added Packages

Package ID
SUNWimap
SUNWipop
SUNWgjvxv
SUNWntr
SUNWntrjs
SUNWntrj
SUNWnhjb
SUNWdocc
SUNWjsos
SUNWjsosl
SUNWjshjb
SUNWjdt
SUNWjdtgl
SUNWjdtd
SUNWhttpr
SUNWhttpu
SUNWhttpv
SUNWski
SUNWskica
SUNWskicw
SUNWskimc
SUNWskimu
SUNWssl
SUNWcache
SUNWscalr
SUNWoam
SUNWcaoam
SUNWscsnm
SUNWcasnm
OCSvista
OCSwcd

APPENDIX **D**

Troubleshooting

This appendix provides troubleshooting procedures and is organized as follows:

Starting the Administration Interface

▼ To Prepare For Configuration

1. **Make sure the Netra j software is installed according to procedures. Refer to the** *Netra j 3.0 Installation Guide* **for instructions.**

2. **Complete the Network Computer Configuration Checklist (Appendix A).**

3. **Make sure the administrative web server daemon is running:**

```
% ps -ef | grep httpd
```

The output should contain the following line:

```
root pid 1 0 date 0:03 /usr/lib/httpd -config /etc/opt/netra/
SUNWnetra/conf/httpd.conf
```

If it is not running, start it by using the following:

```
% /etc/initid/ahttpd start
```

4. **Find the path name of the web server document root. This is the root directory of the web server running on `port 80` on your system.**

Updating `javaos` binary

After updating a new `javaos` binary to flash memory, the server automatically reboots the JavaStation and may display the following warning:

```
Can’t open device.
Keyboard not present. Using ttya for input and output.
```

This warning is displayed when the JavaOS software is first installed or when the end-user elects to update the operating system on reboot.

This warning is from the Open Boot Prom (OBP) and has no impact on how JavaOS functions.

Web Proxy

On networks with both a Netra j server and a separate Web proxy server, you must modify NC HotJava Views and HotJava Browser preferences to allow *no proxy for* the Netra j server. Otherwise, the NC client always contacts the Web proxy for all its services, which could lead to potential connectivity problems.

Viewing Network Activity

You can view network activity to help facilitate how to troubleshoot problems with the operating system.

You can also change the console key from PrintScreen to another key by setting a JavaOS property. See *JavaStation Client Software Guide* for details.

▼ Using the JavaOS Console

- **To open the JavaOS console window from the network computer client, wait until the star-field screen is displayed, then press the print screen key.**

  The JavaOS console window displays the network activity.

Boot Problems

The following table describes how to update the flash-prom (programmable read-only memory) with the JavaOS operating system by changing the `javaos.alwaysUpdate` property.

TABLE D-1 Updating the Flash-prom with JavaOS

If	then
If not set	then the default behavior occurs: if the DHCP-supplied checksum is present and is not zero and does not match the checksum stored in flash, then an Update Flash dialog is displayed. The default value is null.
If set to `true`	then if the above conditions hold, no dialog is displayed and flash is updated.
If set to any value other than `true`	then regardless of checksum presence/value, flash is not updated. Note, that if the DHCP checksum is not present or is zero, the flash is not updated.

Note – See *JavaStation Client Software Guide* for additional information.

Name Services

The following table describes name services error messages.

TABLE D-2 Name Services Error Messages

Message	Action
DNS domain name is empty Host name field is empty	Specify a DNS domain name or host name
Invalid DNS server IP address Invalid IP address Invalid subnet mask Invalid router IP address	IP addresses must be in the form *x.x.x.x* where *x* is a number between 0 and 255. Type `man inet` for more information. Hex values are also acceptable.
Host name already exists IP address already exists Ethernet address already exists	Each client must have a unique host name, Ethernet address, and IP address. Enter a different value.
Invalid Ethernet address	Ethernet addresses must be in the form *xx:xx:xx:xx:xx:xx*, where *xx* is a hexadecimal number separated by colons.

HotJava Views

This section lists some of the known problems with the HotJava Views software.

General

- HotJava Views 1.1 requires a minimum of 32 Mbytes of memory to run on an NC.
- There may be intermittent problems when running against a loaded NC HTTP server.
- The selector desktop configuration file (`selector.desktop`) has changed. Applications are now in the `selector.apps` file. The `selector.desktop` file now refers only to the name of applications that are defined in `selector.apps`.

MailView

- On NC systems, the right mouse button does not currently generate events to applets and applications. For this reason, MailView functionality in pop-up menus activated by the right mouse button are not available. This primarily affects folder management in the tree display in the upper-left corner and in attachments.
- Make sure that when the NC clients are installed, there are proper entries in DNS for each client system. If the NC client is not in the DNS maps, the user may not be able to send mail.
- Temporary file space in `/var/tmp` can become full, causing append commands to fail. This can occur when large mail messages are sent, and the user gets an "Unable to send" error notice. More space is required in `/var/tmp` to resolve this issue.

HotJava Views Administration

Use of the HotJava Views Administration facility requires a browser that is compliant with JDK 1.1. Both HotJava Views and HotJava Browser are compliant with JDK 1.1, but other browsers may not yet be fully compliant.

The administration facility is applicable only when configuring HotJava Views installed on the HTTP server that is used to deliver Views applets and configuration files.

Tips

General Tips for Using HJV Administration

- Use a web browser to verify all URLs specified in `/var/dhcp/dhcptab` and in the JavaOS properties text file.
- Run `snoop(1M)` and watch the packets to and from the NC.
- Early access versions of Views improperly saved properties into `~/.jdt`.
- See the `README` files in `/opt/SUNWjdt/doc` for each component.
- Refer to the following Solaris man pages: `dhcp(4)`, `dhcp_network(4)`, `dhcpconfig(1M)`, `dhcptab(4)`, `dhtadm(4)`, `pntadm(4)`, `in.dhcpd(1M)`, `snoop(1M)`
- To update the “About” button, you must edit the `lib/html/welcome/welcomeAbout.html` file.

- To change the alias associated with the “Feedback” button, you must update the `selector.props` property for each group configuration.

CalendarView

- CalendarView works best with the Common Desktop Environment (CDE) calendar server. The feature of storing mail messages with appointments is available only for calendars in the data version 4 format. This format is supported by the CDE calendar server. The OpenWindows^{TM} calendar server does not support the data version 4 format.
- To find out whether the CDE calendar server is running on a particular machine, as superuser, type:

```
# /usr/dt/bin/sdtcm_admin -l -h name-of-machine-to-check
```

If the `sdtcm_admin` command returns a list of calendar names, the CDE calendar server is running on that machine. Otherwise, the command returns the following message:

```
# /usr/dt/bin/sdtcm_admin: Could not list calendars because:
Service is unavailable.
```

The CDE calendar server is available in the `SUNWdtdmn` package.

- When an appointment is scheduled through MailView, the mail message containing the appointment is saved in the login user's calendar mailbox and a reference to the saved mail message is stored with the appointment. This feature is not available for calendars in the OpenWindows calendar format, data version 3 or less. This is a limitation of the data version 3 (or less) format.

You can use the `/usr/dt/bin/sdtcm_convert` calendar conversion utility to convert data from version 3 calendars to data version 4 format. Refer to the `sdtcm_convert` man page for details.

- The Additional Permissions list within the Properties dialog may contain login IDs instead of complete names (for example, joes may be displayed instead of Joe Smith). This can occur if the user's calendar is in the OpenWindows data format or if the entry was added using calendar clients other than CalendarView. If the calendar is in the OpenWindows data format, use the `/usr/dt/bin/sdtcm_convert` utility to convert it to data version 4 format. Refer to the `sdtcm_convert` man page. Otherwise, use only CalendarView to add editors.

- For editable calendars, clicking within an empty time slot creates a new 1-hour appointment in that time slot. There may be a significant delay in refreshing the view. If you did not intend to create a new appointment, delete it by clicking the Delete button in the CalendarView detail area.
- To demonstrate automatic update, you need two calendar clients (two CalendarView clients or CalendarView and dtcm).

NameView

- It may be useful to capture output from the Namesvc proxy to a file. This can be enabled by editing /opt/SUNWjdt/cgi-bin/namesvc. Comment the line:

```
# $JAVA_HOME/bin/java sunw.jdt.dex.server.Namesvc
```

And uncomment the line:

```
# $JAVA_HOME/bin/java sunw.jdt.dex.server.Namesvc | tee /tmp
dex.last
```

If you perform a search and this file doesn't get created or updated, then the httpd server is having problems launching the cgi-bin script. If the output in the file indicates some type of error:

```
Content-type: text/plain
<DBError>:6
```

then the database probably couldn't be found or the permissions on the file are not set correctly. Make sure the database files have read access for world.

- If you have enabled capturing output to /tmp/dex.last and this file isn't being updated, then check the httpd server error log file. This may indicate that there was some sort of cgi-bin error. The server may not be configured to run cgi scripts or might not be able to find the namesvc script.
- Make sure the database files you have created have read access set for world (chmod 664).
- The 1.1 back end is not compatible with 1.0 clients. If you need to support both 1.1 and 1.0 clients, you have several choices. The easiest solution is to install the 1.1 back end on a different server than the 1.0 back end. In this configuration you simply follow the steps that have already been outlined above. If you want to support 1.1 and 1.0 clients from the same server, follow these instructions:

1. Install 1.1 on the server, but do not install it on top of your 1.0 installation. Put 1.1 under `/opt/SUNWjdt1.1` or something similar.
2. In your web server `cgi-bin` directory create a symbolic link from *webserver*`/cgi-bin/jdt1.1` to `/opt/SUNWjdtd1.1/cgi-bin`.
3. Edit the `namesvc` file in `/opt/SUNWjdtd1.1/cgi-bin`. Change the `JDT_HOME` environment variable from `/opt/SUNWjdt` to `/opt/SUNWjdt1.1`.
4. Edit `/opt/SUNWjdt1.1/lib/props/standard/nameview.props`. Change the value of the `dex.db.cgi.proxy` property to `/cgi-bin/jdt1.1/namesvc.2.0`.
5. Edit `/opt/SUNWjdt1.1/lib/props/namesvc.props` to point to your database.

▼ Enable Error Message Logging

This release of HotJava Views has an error message logging capability that is used most extensively by NameView. If you want to enable this capability, use the following procedure on the system running your web server.

1. **Assuming you have installed HotJava Views in `/opt/SUNWjdt`, create a symbolic link called `jdt` from within your `httpd` server's `cgi-bin` directory (this location varies among servers) to `/opt/SUNWjdt/cgi-bin`.**

   For example, if you are running the Apache server, you can use the following commands:

```
# pwd
# /opt/WWW/Apache/httpd/cgi-bin  Your httpd server's cgi-bin dir
# ln -s /opt/SUNWjdt/cgi-bin ./jdt
# ls jdt
# getidsvc.2.0   jdtlogsvc  namesvc.2.0
```

2. **Some web servers require that you explicitly turn on `cgi-bin` support before `cgi-bin` scripts can be executed. Refer to your `httpd` server's documentation to determine your server's requirements.**

3. **Edit the `/etc/syslog.conf` file and add the following line**:

```
# local0.info/var/opt/SUNWjdt/jdt.log
```

Make sure that you use tabs, *not* spaces, between the values.

4. **Create** `/var/opt/SUNWjdt/jdt.log` **and modify its permissions:**

```
# mkdir /var/opt/SUNWjdt
# touch /var/opt/SUNWjdt/jdt.log
# chmod 666 /var/opt/SUNWjdt/jdt.log
```

5. **Restart the** `syslog` **daemon:**

```
# kill -HUP `cat /etc/syslog.pid
```

HotJava Views uses CGI to send error messages to the `jdtlogsvc` script on your web server. The `jdtlogsvc` script uses `syslog` to log the errors.

HotJava Views Troubleshooting

TABLE D-3 HotJava Views Error Messages and Suggested Actions

Message or Problem	Action
JavaOS 1.1 boots OK, but upon login, the heap viewer applet displays instead of Views.	The alternate main parameters are not getting passed to JavaOS. Make sure you have specified the correct URL in the `-i` option in `/var/dhcp/dhcptab`. Use a web browser to verify the URL. Make sure the j`avaos.mainProgram`, `javaos.mainZip` and `javaos.mainHomeprop` parameters are correctly specified in the `javaosopt.txt` file. Use the `-i` URL indirection. Make sure you have sent a `SIGHUP` to `in.dhcpd` if you have changed the `/var/dhcp/dhcptab` file.
JavaOS 1.1 boots OK, but upon login, a blue screen displays instead of Views.	JavaOS has received the alternate main parameters, but they are incorrect. Make sure `javaos.mainProgram` and `javaos.mainZip` are specified correctly in the `javaosopt.txt` file. Verify the URLs are correct by using a web browser.
`class not found/defined` error	This error is common if you are using the JavaServer™ server. Servers may fail to handle HTTP requests. If this happens when Views is trying to load a class file, you get a *class not found/defined* error. Try using the Apache or Netscape server to correct this problem.
Tables do not parse well in WebView.	The `.jdt/props/selector.props` files may contain invalid entries for class names that handle HTML tags. Check your `selector.props` file for entries that specify classes that start with *sun.hotjava*. If you find such entries, move your`.jdt/props/selector.props` file aside (don't forget to reset your proxies).
After modifying Appointment Reminder properties within the Properties dialog, the appointment reminder types (Post Notice and /or Ring Bell) do not match the property value settings.	Restart Selector for the new property setting to take effect.

TABLE D-3 HotJava Views Error Messages and Suggested Actions *(Continued)*

Message or Problem	**Action**
Several (or many) reminders are posted for a single appointment.	Chances are your calendar file is in an older format, and/or your workstation has a different time than your calendar server. Update your calendar file and sync your workstation clock with the server's clock.
No reminders are displayed for appointments inserted through Month view.	After inserting appointments in Month view, perform an action that reloads your calendar, such as changing the month you're viewing or switching to Day view or Week view.
Closing the Mail Login dialog in Calendarview can cause HotJava Views to lock up.	Don't close the Mail Login dialog using the window menu. Use the Login and Cancel buttons to close the dialog.
HotJava Views complains about not being able to mount my home directory.	JavaOS mounts your home directory when you log in. It gets the location of your home directory from the `passwd` and `auto.home` NIS maps. Make sure these maps are correct and that your home directory is properly exported so the NC can mount it. You can run `snoop(1M)` and watch for the `MOUNT` request that happens after you log into JavaOS.
`snoop(1M)` doesn't show all the packets from the NC.	You may be on a switched network. In this case, packets from the NC may not be visible to the system on which you are running `snoop`. The best way to make sure you see all packets is to plug the NC and your Solaris system into a mini-hub and run `snoop etherid for javastation`.

The following table describes HotJava Views error messages and known problems.

GO-Joe

GO-Joe provides diagnostic tools and outputs to help diagnose problems that may arise due to misconfiguration and other difficulties. Check these if you encounter any problems.

Diagnostic Tools

JavaOS Console Output

On devices that provide it, the JavaOS console output (see “Troubleshooting”) can be highly informative if the applet terminates prematurely. When viewing this output, look for all exceptions that may be listed. Exceptions may occur that cause further exceptions as the program continues to execute, and it is usually the original exception that indicates the true cause of the problem. In addition, the GO-Joe applet prints messages to the status bar, but not all Java environments show this status (or they may overwrite it with their own status messages). These messages are also sent to the Java console, so they may be visible in the console log when they are not visible on the status line.

The `/tmp/Xerr:n` Error File

The GlobalHost loadable ddx module redirects the standard error output for the session to a file called `/tmp/Xerr:n`, where *n* represents the display number of the session. This file contains diagnostic messages from the `GlobalInit` program, from the ddx loadable module itself, and from the X clients that run throughout the session.

Common Problems

The GO-Joe product has been designed to be easy to configure and use, yet is somewhat complex in operation. Some of the more common problems encountered are described here.

HTML References

If the GO-Joe applet fails to load entirely, check the HTML file you are loading and verify that the `APPLET` tag is correctly formed. Check the codebase path and the path and file name to the applet file itself. Finally, investigate the log files for your HTTP server (usually called `access_log` and `error_log`) to see if the applet is being successfully transmitted to the Java environment. It may help to exit your browser or Java environment and restart it to clear any cached files that may be interfering with the applet's execution.

Java Security Manager Exceptions

All Java environments implement a security manager that determines what operations may be dangerous for an applet to perform and can enable or restrict these actions as it sees fit. The biggest restriction that most Security Managers implement with respect to GO-Joe is that an applet is allowed to connect only to the host that served that applet. If you have such a Security Manager, your GO-Joe applet is only able to connect to the `go-login` program running on the server that the applet was loaded from. In addition, the `diagfile` functionality of GO-Joe is similarly restricted.

The JavaStation produces a message as follows:

```
Sunw.hotjava.applet.AppletSecurityException:
checkconnect.networknone
at sunw.hotjava.security.CommonSecurity.checkconnect()
at java.net.InetAddress.getAllByName)()
```

Capturing Log Files

In some cases, if JavaOS fails, it may broadcast an SNMP trap. The trap can be received by any SNMP manager listening on the (sub)net. There is a simple SNMP trap receiver supplied with JavaOS state information in a log file.

▼ To Capture Log Files for JavaOS

- **Run the following command on any machine in the (sub)net:**

```
# /opt/SUNWjsos/bin/snmptrapd -x /opt/SUNWjsos/bin/logdumper&
```

If failures do occur, they are saved in the `/tmp` directory of the server machine with the following unique file name:

```
/tmp/javaos.log.<IP address of failed client>@<time in seconds
since January 1, 1970>
```

You can browse the log file to determine errors that may have caused a failure. You may also want to add the snmptrapd command to the Solaris initialization and booting hierarchy. See the README files in /etc/init.d and /etc/rc2.d for details.

Note – Not all JavaStation client failures result in a log file creation on the server machine.

Additional Error Messages and Known Problems

The following table describes additional error messages and known problems.

TABLE D-4 Miscellaneous Error Messages and Suggested Actions

Message	Action
Cannot read /etc/hosts File not found: /opt/SUNWjshm/bin/jdhostcfg Cannot read /opt/SUNWjshm/lib/Help.txt Cannot write /tmp/.jdcfg	Check to ensure the Solaris operating environment and the SUNWjshm package are installed correctly. Also check file system permissions.

APPENDIX **E**

Page Types and Icons

This appendix shows and describes the various types of screens and icons used in Netra j administration interface.

Page Types

The Netra user interface has five types of pages:

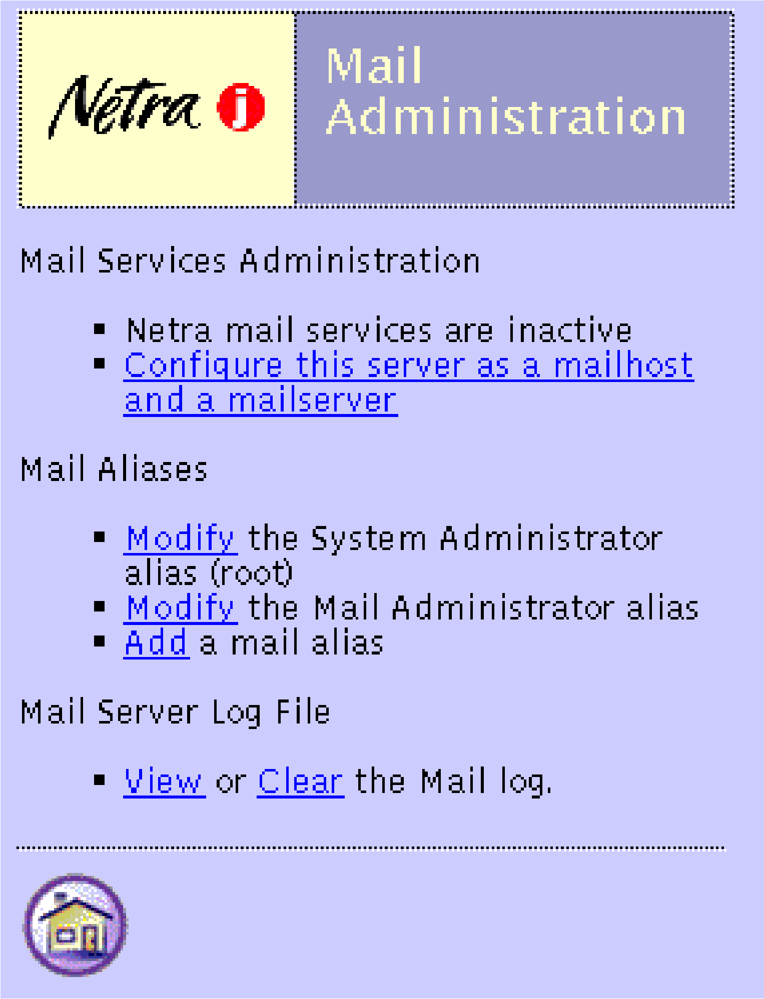
- "Navigation Page" on page 249
- "Task Page" on page 250
- "Help Page" on page 254
- "Glossary Page" on page 256
- "Status Page" on page 256

Navigation Page

A Navigation page is a page that contains only links to other pages. You select a task by clicking on the link, which displays a task page or another Navigation page. When you follow a link, the state of the system does not change.

Some navigation pages are dynamic: they display only the options that are available on your particular Netra system. If you enter information on a task page that changes the available options, these Navigation pages reflect the changes.

The following figure shows a Navigation page for the Mail Administration module. From this page you can add a mail alias or modify an existing administrator by selecting the appropriate links.



Netra j

Mail Administration

Mail Services Administration

- Netra mail services are inactive
- Configure this server as a mailhost and a mailserver

Mail Aliases

- Modify the System Administrator alias (root)
- Modify the Mail Administrator alias
- Add a mail alias

Mail Server Log File

- View or Clear the Mail log.

FIGURE E-1 Navigation Page

Task Page

A task page is also called a *form*. There are two types of forms: regular and special.

Regular Form

Regular forms provide the only way to change the system state. When a form is displayed, the values in the fields are either current or default values. You can enter information in a regular form by typing it into the text boxes or by choosing the radio button options.

Regular forms have an OK button that you must click to activate any changes or to enter new information.

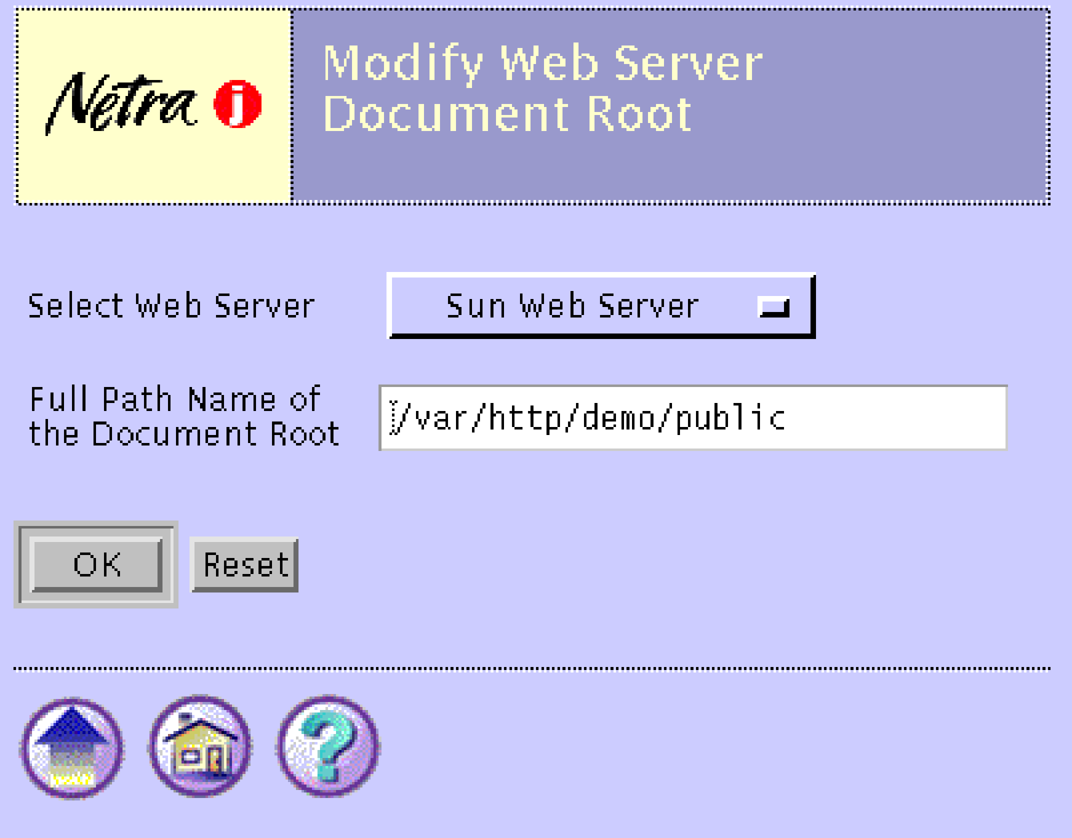
Some regular forms also have a Reset button. If you want to discard your changes before they are activated, use the Reset button to return fields to their previous values.

The fields in a form are described in the following table.

TABLE E-1 User Input Elements

Element	Description
Text box	Accepts one line of text input.
Text area	Accepts multiple lines of text input.
Radio buttons	A group of one or more buttons, only one of which can be selected. You click on a radio button to select it; this deselects any other selected radio button in its group. The only way to deselect a radio button is to select another one.
Check box	Selects an option. Click on the check box to change its state.
Pop-up menu	A list of options displayed in a menu. Only one option can be selected at a time. The selected item is shown. Press the mouse button on the menu to display the list of options. Release over a new option to select it.
Scrolling list	A list of options displayed in a window. Click on an option to select it. You can choose multiple selections in a scrolling list.

The following figure shows an example of a task page (regular form) to Modify Web Server Document Root.



Modify Web Server Document Root

Select Web Server: Sun Web Server

Full Path Name of the Document Root: /var/http/demo/public

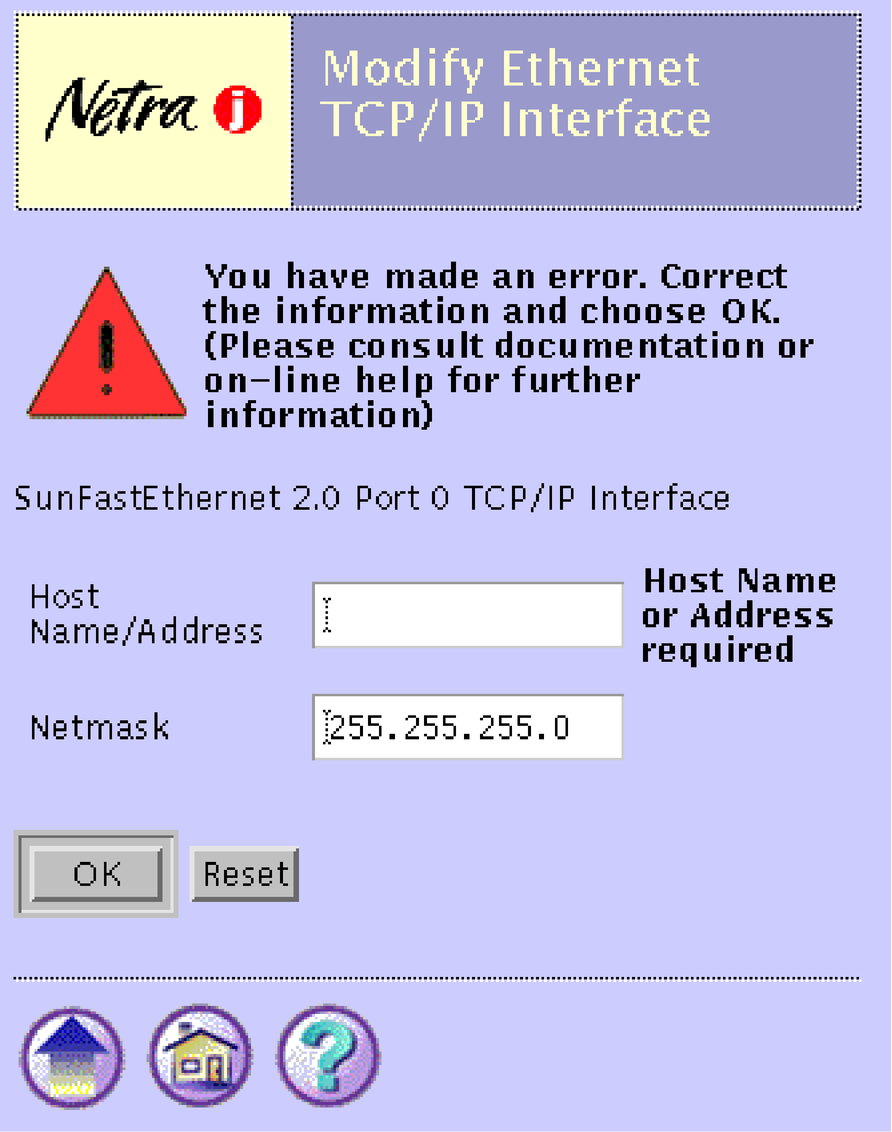
FIGURE E-2 Task Page (Regular Form)

Special Form

Special forms are based on regular forms. Special forms are automatically displayed. There are two types of special forms: Error forms and Verify forms.

- An error form does not change the system state. It displays an error icon, and enables you to correct the error and re-enter information in a regular form. Errors are marked on the form next to the relevant field. The following figure shows an Error form for the Local Area Network module.

Note – If the information you enter in a form produces an error, the system state is not changed. The form is redisplayed with the erroneous data. You must correct the data.



Modify Ethernet TCP/IP Interface

You have made an error. Correct the information and choose OK. (Please consult documentation or on-line help for further information)

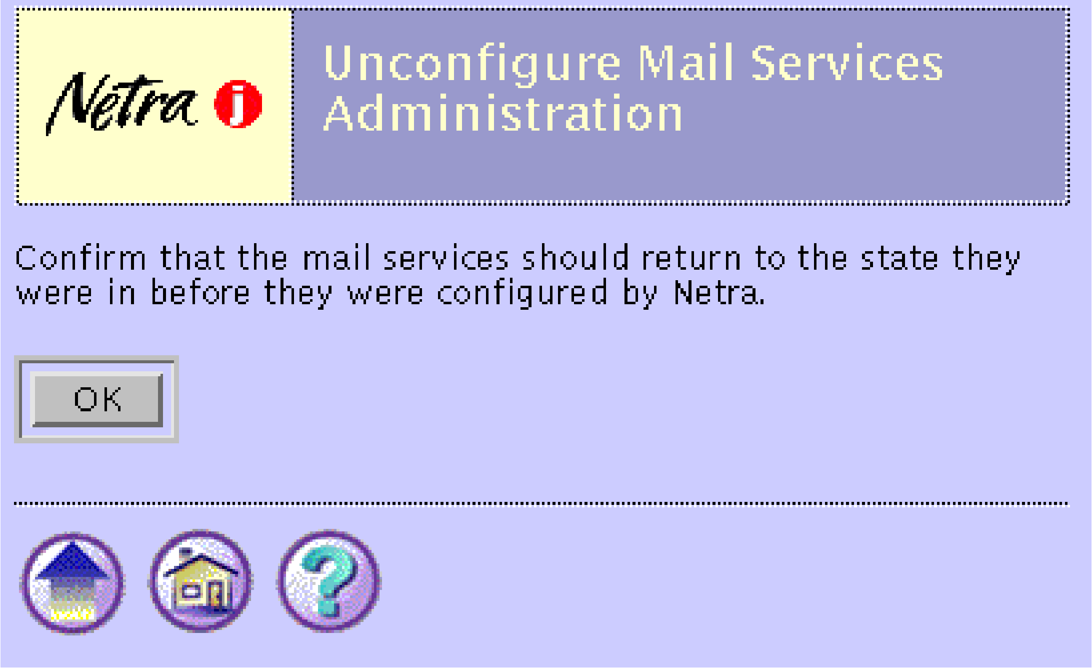
SunFastEthernet 2.0 Port 0 TCP/IP Interface

Host Name/Address		Host Name or Address required
Netmask	255.255.255.0	

FIGURE E-3 Error Form

- A verify form is a prompt to confirm a previous choice.

The following figure shows a Verify form for the Mail Administration module.



Unconfigure Mail Services Administration

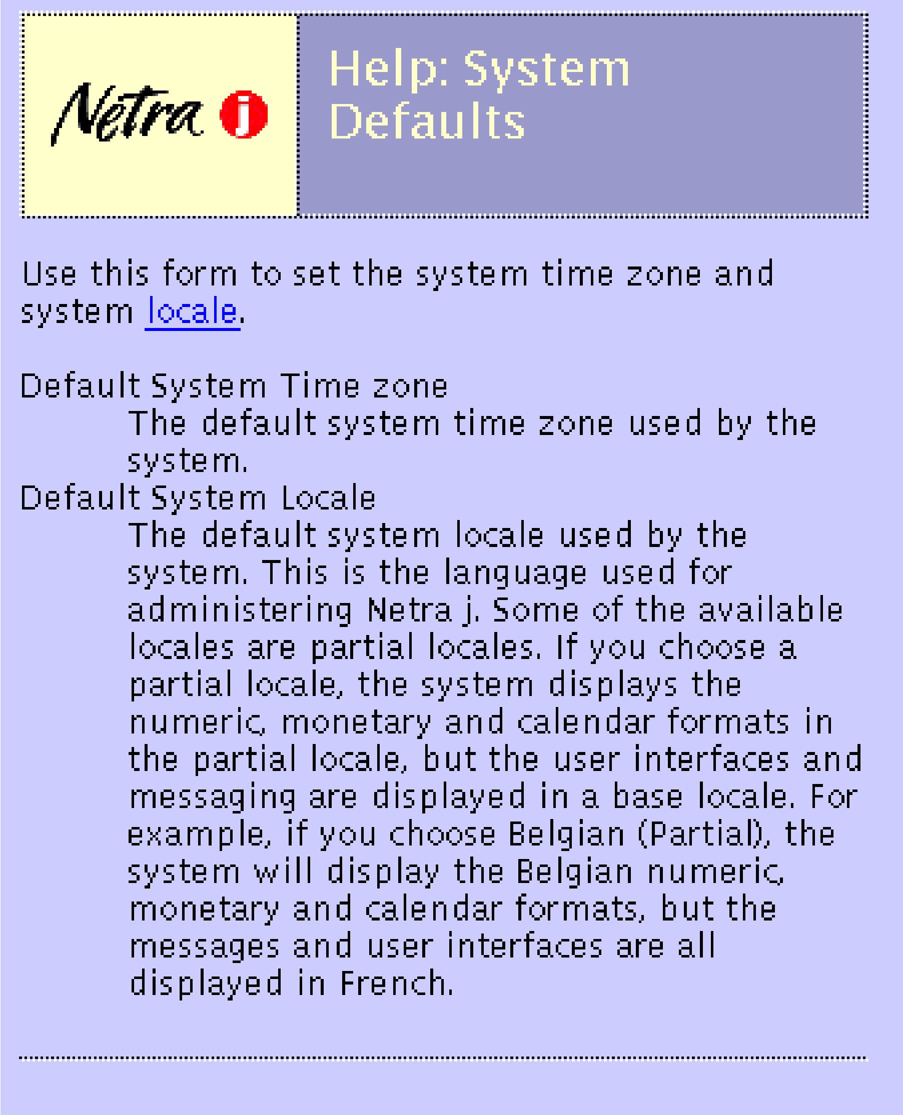
Confirm that the mail services should return to the state they were in before they were configured by Netra.

FIGURE E-4 Verify Form

Help Page

When you click on the Help icon, a separate browser opens to display Help pages. Help pages contain the information you need to fill out a form. All forms have a Help icon in the form of a question mark. Some Help pages use terms that are linked to the glossary.

The following figure shows a Help page for the System Defaults.



Help: System Defaults

Use this form to set the system time zone and system locale.

Default System Time zone

The default system time zone used by the system.

Default System Locale

The default system locale used by the system. This is the language used for administering Netra j. Some of the available locales are partial locales. If you choose a partial locale, the system displays the numeric, monetary and calendar formats in the partial locale, but the user interfaces and messaging are displayed in a base locale. For example, if you choose Belgian (Partial), the system will display the Belgian numeric, monetary and calendar formats, but the messages and user interfaces are all displayed in French.

FIGURE E-5 Help Page

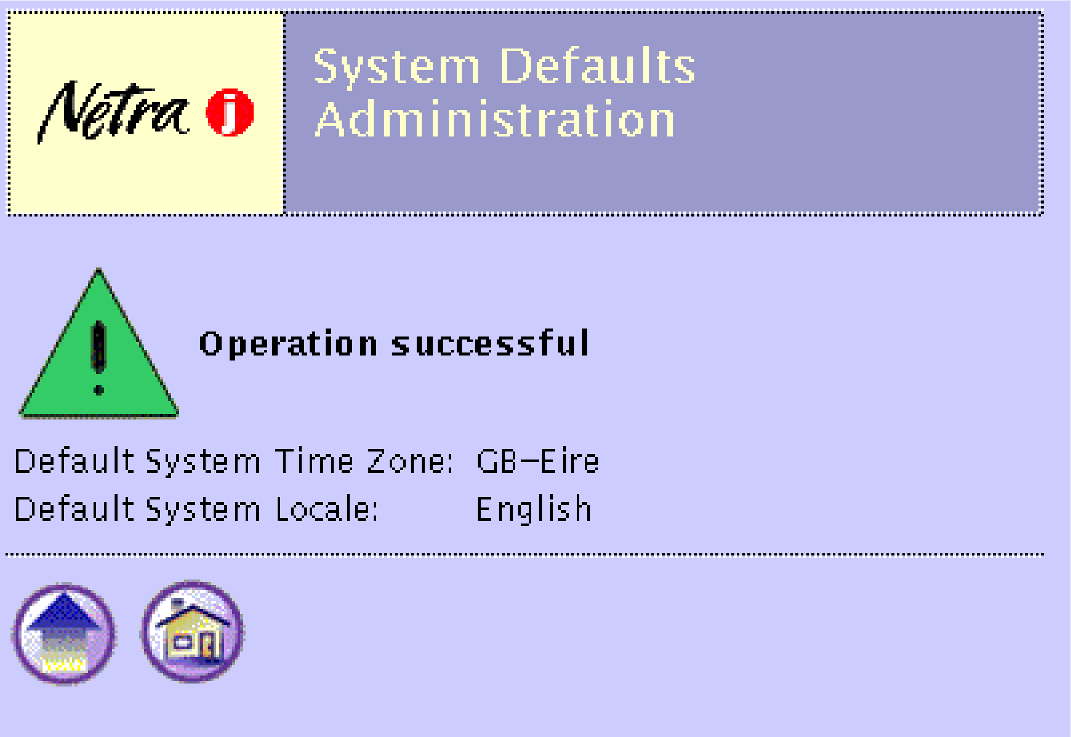
Glossary Page

You can access the glossary page using links from the Help pages. When you select a term that is a link, the term and its explanation are displayed at the top of the glossary page. The glossary page is displayed in a scrolling window. To return to the help page, use the back arrow icon located on the bottom of the glossary or browser back button.

Status Page

A status page is displayed once you have completed all the forms for a task. It contains either a success icon or an information icon. A status page confirms that the system state has changed.

The following figure shows an example success Status page for the System Defaults.



System Defaults Administration

Operation successful

Default System Time Zone: GB–Eire

Default System Locale: English

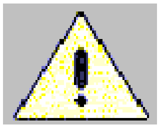
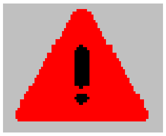
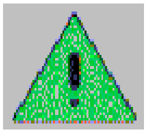
FIGURE E-6 Success Status Page

Icons

Information Icons

The icons shown in the following table may be displayed while a task is being completed.

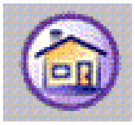
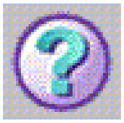
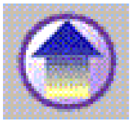
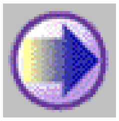
TABLE E-2 Netra Information Icons

Icon	Description
	Information icon. Calls attention to important messages in response to submitting a form. The message indicates the status of the operation. Yellow triangle with exclamation point.
	Error icon. Calls attention to errors in form entries. Red triangle with exclamation point.
	Success icon. Indicates that a task has been completed successfully. Green triangle with exclamation point.

Navigation Icons

Each administration page contains some of the icons shown in the following table.

TABLE E-3 Netra Navigation Icons

Icon	Description
	Home icon. Returns to the Netra Main Administration page. (Clicking on the Netra j banner also does this.)
	Help icon. Contains explanations of fields in the related form.
	Top of Module icon. Returns to a module's top-level page.
	Forward Arrow icon. Continues to the next configuration task.

Glossary

address resolution protocol (ARP) A method for finding a host's Ethernet address from its Internet address. The sender broadcasts an ARP packet containing the Internet address of another host and waits for it (or some other host) to send back its Ethernet address. Each host maintains a cache of address translations to reduce delay and loading. ARP enables the Internet address to be independent of the Ethernet address, but this works only if all hosts support it.

ARP See *address resolution protocol*.

ATM address A 20-byte (the bytes are often referred to as octets) number that uniquely identifies an asynchronous transfer mode (ATM) endpoint. The first 13 bytes are assigned by the switch and are called the switch prefix; the remaining 7 bytes (made up of a 6-byte end system identifier and a 1-byte selector) are assigned by the local host.

DHCP See *dynamic host configuration protocol*.

DNS See *Domain Name System*.

domain name A name that identifies a logical group of computers. It is a text string that can include letters (a–z and A–Z), digits (0–9), and hyphens (-) (for example, `eng`). A fully qualified domain name is composed of the local domain and all of its ancestor domains leading to the root domain, separated by periods and ending in a period (for example, `eng.sun.com.`). A partially qualified domain name is the local domain name and some number of ancestor domains separated by periods (for example, `eng.sun`). When a partial domain name is used, it is assumed to be within the current domain or within one of the ancestor domains of the current domain.

Domain Name System (DNS) A network information service that provides information about hosts within the domain name system. It is mainly used for name resolution, that is, it is used to provide host addresses that correspond to host names. It can also be used to provide other information about hosts such as aliases or mail servers.

Dynamic Host Configuration Protocol (DHCP) A protocol that provides a host with an Internet protocol (IP) address and other Internet configuration parameters without any need for preconfiguration by the user.

dynamic router A router that relies on information broadcast from other routers to update its routes to reflect changes in the network topology. The router also broadcasts this information to other dynamic routers.

email address An electronic mail address, which is composed of three parts: the user name (the name of the person who receives the mail), the host name (the system on which that user has an account) and the domain name (the domain in which the system resides). The user name is separated from the host name by an “at” sign (@). The host name and domain name are separated by a period (for example, *user@host.domain.com*).

Ethernet A network protocol that broadcasts information to all the hosts on the network. The information is accepted by the intended recipients and discarded by the other hosts.

firewall A logical border that protects the local network against intrusion from other networks. A firewall can monitor or prohibit connections to and from specified services or hosts.

file transfer protocol (FTP) A protocol that enables files to be copied between systems connected to a TCP/IP network independent of the operating systems or architectures of the hosts involved in the file transfer.

FTP See *file transfer protocol.*

hexadecimal number A number expressed in base 16. It is composed of the characters 0–9, a–f, and A–F.

host address (IP address) An assigned number that uniquely identifies each computer connected to a TCP/IP network. The address consists of two parts: a network number and a host number. The network number identifies the network to which the computer is connected, and the host number identifies the computer on that network. The host address is composed of four integers separated by periods. The first integer must be in the range 0–223, the second and third integers in the range 0–255, and the fourth integer in the range 1–254 (for example, 129.144.0.1).

host name The name of a computer within the local domain. It is a text string of up to 24 characters composed of letters (a–z and A–Z), digits (0–9), and hyphens (-). The last character cannot be a hyphen.

HTML See *hypertext markup language.*

HTTP See *hypertext transport protocol.*

HTTPD See *hypertext transport protocol daemon*.

hypertext markup language (HTML) A language used to format hypertext documents. Hypertext documents have text that contains links to other documents or to images, sound, graphics, or video files.

hypertext transport protocol (HTTP) A way used to transmit and display hypertext documents. HTTP capitalizes on the fact that navigation information can be embedded directly in the documents. Thus, the protocol does not need to support full navigation features like the FTP protocols do. Because HTTP has low overhead, HTTP servers are commonly used for serving hypertext documents.

hypertext transport protocol daemon (HTTPD) The software component of a Web server. Using the HTTPD, the Netra server makes its administration tools available to clients on the LAN.

ICMP See *internet control message protocol*.

IDE See *integrated development environment*.

integer A whole number composed of the digits 0–9.

Internet A global collection of networks connecting a wide range of computers using a common protocol to communicate and share services.

Internet control message protocol (ICMP) An extension to the Internet protocol (IP). It allows for the generation of error messages, test packets, and informational messages related to IP.

Internet protocol (IP) Internet protocol. The network layer protocol for the Internet protocol suite.

integrated development environment (IDE)

integrated services digital network (ISDN) A set of integrated telecommunications services available over public telecommunication networks.

Internet Service Provider A company that provides an Internet connection by using its own computer system as a conduit to the Internet. The service provider generally has a direct Internet connection; the client typically connects to the service provider with a dial-up connection.

IP See *Internet protocol*.

ISDN See *integrated services digital network*.

local area network A group of computer systems in close proximity that can communicate with one another via some connecting hardware and software.

LAN See *Local Area Network.*

MAC address The unique hardware address assigned to a system or interface board when it is manufactured.

multihomed host A host that has more than one network interface connected to the same network.

netmask A mask used to determine the network address from a host address. A netmask is composed of four integers in the range 0–255 separated by periods. When a netmask is expressed in binary notation, it must be a contiguous sequence of "ones" followed by a contiguous sequence of "zeroes" (for example, 255.255.128.0).

network address A number that identifies the network in which a computer resides. A network address is composed of four integers separated by periods. The first integer must be in the range 0–223, the second and third integers must be in the range 0–255, and the fourth integer must be in the range 0–254 (for example, 129.144.0.0).

network interface An access point to a system on a network. Each interface is associated with a physical device. However, a physical device can have multiple network interfaces.

Network Information Service (NIS) A network information service containing key information about the systems and the users on the network.

network time protocol (NTP) A protocol built on top of TCP/IP that ensures accurate local timekeeping with reference to radio, atomic or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NFS Network File System. This Remote Procedure Call (RPC) service that enables machines to share files across the network. It permits the user to access remote files and hierarchies transparently as if they were local to the user's machine.

NIS See *Network Information Service.*

NTP See *network time protocol.*

point-to-point protocol (PPP) This protocol enables two computers to be connected over a two-way communications link, such as a telephone line. The connection is established as needed.

PPP See *point-to-point protocol.*

RARP See *reverse address resolution protocol.*

Remote Procedure Call (RPC)

reverse address resolution protocol (RARP) Thus protocol provides the reverse function of address resolution protocol (ARP). RARP maps a hardware address to an Internet address. It is used primarily by diskless nodes when they first initialize to find their Internet address.

route A route specifies the next router on a message's path to its destination. A default route does not contain a specific destination; it has a general destination used for any destinations not specified in other routes.

router A computer or other dedicated hardware that connects two or more networks and routes data between them.

static router A router that relies on manual addition of routes. Routing information is not exchanged with other routers.

software package A collection of files and directories required for a software product. A complete software product can be made up of several packages. A collection of packages required for a software product is called a software cluster.

software patch A collection of files and directories that fix a set of problems associated with a software product. A patch can be installed on a system only if the software product being fixed is also installed.

TCP/IP Transport Control Protocol/Interface Program. The protocol suite originally developed for the Internet. It is also called the Internet protocol suite.

uniform resource locator (URL) The addressing system used by clients to request web documents from servers. The format of a URL is *protocol*://*system*:*port*/*document* (for example, `http://www.sun.com/`).

URL See *uniform resource locator.*

user name The name that the computer uses to identify a particular user. It is a text string of up to eight characters that can include letters (a–z and A–Z), digits (0–9), hyphens (-), and underscores (_). The first character must be a letter.

Web A collection of systems on the Internet that contain hypertext documents that are accessible using HTTP and are displayed as web pages by web servers.