

# **Omni-Series**

## User's Manual

Copyright © 1991-2002 XLink Technology, Inc.

***XLink Technology, Inc.***

1546 Centre Pointe Dr.

Milpitas, CA 95035

U.S.A

Phone: (408) 263-8201

Fax: (408) 263-8203

Sales e-mail: sales@xlink.com

Support e-mail: support@xlink.com

Copyright Notice

All rights reserved. Reproduction or use of editorial or pictorial content in any manner without expressed permission is prohibited. Use, copy, and disclosure are restricted by license agreement.

Trademarks

Omni-NFS, Omni-NFS/X, Omni-NFS Enterprise, Omni-NFS/X Enterprise, Omni-VT420, Omni-Tar, Omni-NFS Gateway, Omni-NFS Dual Gateway, Omni-Print, Omni-Lite ,and Omni-Series related products are registered trademarks of XLink Technology, Inc..

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other trademarks or registered trademarks of respective holders are acknowledged.

# Table of Contents

---

<b>CHAPTER 1 HOW TO USE THIS MANUAL.....</b>	<b>1</b>
INTRODUCTION TO OMNI-SERIES SOFTWARE .....	1
ABOUT OMNI-SERIES .....	1
OMNI-SERIES PACKAGES.....	2
ADDITIONAL INFORMATION .....	2
CONVENTIONS USED IN THIS USER'S GUIDE.....	3
<b>CHAPTER 2 NFS GATEWAY.....</b>	<b>5</b>
INTRODUCTION.....	5
STARTING NFS GATEWAY .....	5
DEFINE AN GATEWAY DRIVE .....	6
BROWSE EXPORTED NFS DRIVE.....	7
SET NFS DRIVE OPTIONS.....	9
SET USER PERMISSION .....	11
USE GATEWAY MOUNT WIZARD.....	11
WHAT IS AN DEFAULT USER ACCOUNT.....	12
USER ACCOUNT MAPPING.....	13
<b>CHAPTER 3 NFS DUAL GATEWAY.....</b>	<b>17</b>
INTRODUCTION.....	17
STARTING NFS DUAL GATEWAY .....	18
<b>CHAPTER 4 NFS CLIENT .....</b>	<b>19</b>
INTRODUCTION.....	19
SETUP NFS CLIENT CONNECTION.....	19
SETTING NFS DRIVE OPTION.....	24
NFS AUTHENTICATION.....	26
MOUNT WIZARD .....	27
AUTO-MOUNTING NFS DRIVES .....	28
OTHER UTILITY FOR NFS CLIENT .....	28
SYMBOLIC LINK SUPPORT .....	28

NFS CLIENT TROUBLESHOOTING.....	30
<b>CHAPTER 5 NFS SERVER.....</b>	<b>31</b>
INTRODUCTION.....	31
FEATURES.....	31
SETUP NFS SERVER.....	32
SECURITY MAPPING.....	34
SETUP NFS PRINTER.....	39
OPTIONS FOR NFS SERVER.....	39
UTILITY FOR NFS SERVER.....	40
AUTO START NFS SERVER SERVICE.....	41
HOW TO EXPORT NETWORK DRIVES (NT ONLY).....	41
TROUBLESHOOTING.....	43
<b>CHAPTER 6 HOST EDITOR.....</b>	<b>45</b>
INTRODUCTION.....	45
SETUP HOST EDITOR.....	45
NIS SETUP.....	48
TROUBLESHOOTING.....	49
<b>CHAPTER 7 LPD SERVER.....</b>	<b>51</b>
INTRODUCTION.....	51
CONFIGURING THE LPD APPLICATION.....	51
HOW TO SET UP LPR ON REMOTE UNIX SYSTEMS.....	53
LPD TROUBLESHOOTING.....	54
<b>CHAPTER 8 LPR HOSTS.....</b>	<b>55</b>
INTRODUCTION.....	55
STARTING LPR HOSTS.....	55
<b>CHAPTER 9 ADDING NETWORK PRINTERS.....</b>	<b>57</b>
INTRODUCTION.....	57
SETTING UP AND USING NFS PRINTER.....	57
SETTING UP AND USING LPR PRINTER.....	58
TROUBLESHOOTING.....	59

<b>CHAPTER 10</b>	<b>FTP SERVER</b>	<b>61</b>
	INTRODUCTION	61
	STARTING FTP SERVER	61
	TROUBLESHOOTING	63
<b>CHAPTER 11</b>	<b>FTP CLIENT</b>	<b>65</b>
	INTRODUCTION	65
	USING FTP CLIENT	65
	FTP CLIENT TROUBLESHOOTING	70
<b>CHAPTER 12</b>	<b>VT420(TELNET)</b>	<b>71</b>
	INTRODUCTION	71
	USING VT420 TERMINAL EMULATION	71
	MULTIPLE SESSION CAPABILITY	71
	STARTING AND TERMINATING VT420	72
	GENERAL SETUP	72
	DISPLAY SETUP	75
	KEYBOARD SETUP	77
	AUTO LOGIN	78
	PRINTER SETUP	79
	KEYMAP	79
	COLOR MAPPING SETUP	81
	TROUBLESHOOTING	82
<b>CHAPTER 13</b>	<b>RSH (REMOTE SHELL)</b>	<b>83</b>
	INTRODUCTION	83
	USING RSH	83
<b>APPENDIX A</b>	<b>NETWORK LOCK MANAGER</b>	
	<b>(NLM FILE LOCKING)</b>	<b>85</b>
	FILE LOCKING	85
	NO LOCKING	85
	READ ONLY	86

<b><i>APPENDIX B PCNFSD</i></b> .....	<b>87</b>
PCNFSD PROTOCOL DEFINITION.....	<b>87</b>
AUTHENTICATION.....	<b>87</b>
PRINT SPOOLING.....	<b>88</b>
<b><i>APPENDIX C PERFORMANCE TIPS</i></b> .....	<b>89</b>
<b><i>APPENDIX D EXAMPLES ON STARTING NFS</i></b> <b><i>SERVER ON UNIX</i></b> .....	<b>91</b>
<b><i>GLOSSARY</i></b> .....	<b>93</b>
<b><i>INDEX</i></b> .....	<b>99</b>

## CHAPTER 1

---

---

### *How to Use this Manual*

#### Introducing Omni-Series Software

Omni-series software is a set of computer software products that utilize NFS protocol for Windows ⇔ Unix systems connectivity. Following topics are illustrated in this chapter:

- **About Omni-Series Software** – describes the Omni-Series software and lists some of the features.
- **Omni-Series Packages** – lists all the packages available in the Omni-Series software family.
- **Additional Information** – describes where additional information can be found.
- **Conventions used in this User's Guide** – describes the conventions used throughout this Guide along with any other assumptions that should be noted by the Omni-Series software users.

#### About Omni-Series

The Omni-Series software provides you with easy and efficient tools to operate and manage your network environment. A wide variety of applications are designed to make better use of existing resources by implementing file and print sharing within your network.

Omni-Series software works in conjunction with Microsoft's TCP/IP. It is a combination of comprehensive NFS and network related applications, which transform your PC into a fully functional NFS client/server.

## Omni-Series Packages

*For Windows 2000/NT*

<i>Package Name</i>	<i>Related Application Reference</i>
<b><i>Omni-NFS Gateway</i></b>	Chapter 2, 6 -13
<b><i>Omni-NFS Dual Gateway</i></b>	Chapter 2, 3, 5 -13
<b><i>Omni-Lite</i></b>	Chapter 4, 6, 7, 8, 9

*For Windows 2000/NT/98/95/XP/ME*

<i>Package Name</i>	<i>Related Application Reference</i>
<b><i>Omni-NFS Enterprise</i></b>	Chapter 4 -13
<b><i>Omni-NFS/X Enterprise</i></b>	Chapter 4 -13
<b><i>Omni-NFS Server</i></b>	Chapter 5, 6, 7, 10
<b><i>Omni-Print</i></b>	Chapter 6, 7, 8, 9
<b><i>Omni-VT420</i></b>	Chapter 6, 11, 12
<b><i>Omni-X</i></b>	Refer to Omni-X User Manual

*For Windows 98/95/ME*

<i>Package Name</i>	<i>Related Application Reference</i>
<b><i>Omni-NFS</i></b>	Chapter 4 -13
<b><i>Omni-Lite</i></b>	Chapter 4, 6, 7, 8, 9

## Additional Information

The Omni-Series software comes with comprehensive and easy to use online help. Changes and additions to any of the applications will be announced on XLink's web site and are downloadable. Some examples are also provided and accessible from our web FAQ page.

If you have any technical question or problem that needs to be resolved immediately, our support staff can be reached via e-mail or by phone for one-on-one troubleshooting.



Note: The content information in this User Guide may be updated without notice. Addendum may be requested.

You can contact XLink's Technical Support Department, Monday to Friday between 9:00a.m. and 6:00p.m. Pacific standard time (with the exception of holidays) at:

**XLink Technology, Inc.**  
1546 Centre Point Dr.  
Milpitas, CA 95035  
U.S.A.

Phone: 408-263-8201  
Fax: 408-263-8203  
E-mail: support@xlink.com  
WEB: http://www.xlink.com

## Conventions Used In This User's Guide

This guide provides instructional-based information. The following table provides some conventions used throughout this Guide.

<i>If you see...</i>	<i>It means....</i>
<ret>	Press "Enter" key on your keyboard.
<tp> xxxx	Type the subsequent character with your keyboard.
<pc>	Indicates commands on your PC
<ux>	Indicates commands on your UNIX hosts
C:>	DOS command prompt
#	UNIX command prompt
<b>Bold</b>	Any word in bold type indicates important or specific terminology used in Windows or Omni-NFS Series software, or dialog button names.
<b>eg.</b>	Indicates example.
<b>Note:</b>	Side notes or tips.
<Data>	< > indicated information needs to be entered.

#### 4 How to Use this Manual

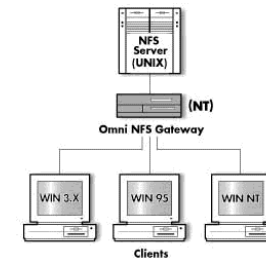
## CHAPTER 2

---

# NFS Gateway

## Introduction

Omni NFS Gateway is a NFS client product with gateway functionalities. Installed on a Windows 2000/NT server system, it allows NFS connections being re-shared to all Windows workstations in the LAN as local drives.



Administrators can now gain centralized network control. It provides **Transparent, Secure, and User-friendly** access for users to NFS resources. Files remain on the NFS host system, so Windows and UNIX users gain access to files without duplicating data. Individual Windows user identities are mapped to NFS accounts as they are passed through the Gateway, ensuring security and restricting file access privileges.

## Starting NFS Gateway

To start **NFS Gateway** :

1. From Windows “Start” menu, select Programs/**Omni-NFS Gateway**
2. Click the **NFS Gateway** icon.
3. The NFS Gateway main screen appears.

Interface Status:

**Drive:**

Indicates available and used drive letters.

## 6 NFS Gateway

The small boxes beside the drive letters show the status of each drive. Green boxes indicate started services and the yellow ones are for unused drives.

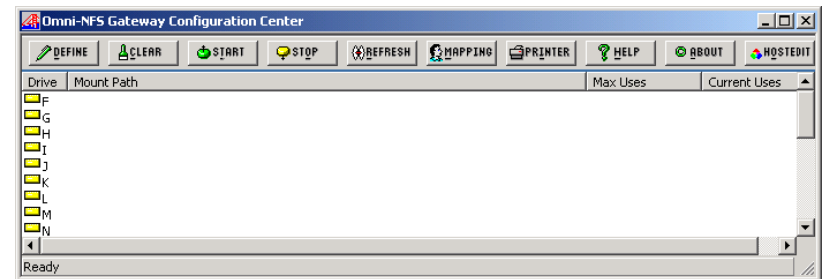
**Max Uses:**

Maximum client seats indicated in the license agreement.

**Current Uses:**

Current number of clients access Gateway mounted drives.

The Gateway interface appears as following:



## Define an Gateway Drive

Step-by-step procedure for defining an NFS drive:

1. Click on the Define button. The NFS Drive Define screen appears.
2. Enter the valid NFS Server name configured in the **Host Editor** program for mounting in the text box.
3. Enter the mount path exported from NFS server in the **Mount Path** box. Mount Path list can be found by click on the **Browse** button, and the **Browse** screen appears for the desired path (please refer to **Browse Exported NFS Drive** section).
4. Options for the NFS drive can be configured by clicking on the **Option** button, and the Drive Option screen appears (see picture in page 9). Here is the place where file attributes, file locking control, file conversion (DOS ↔ Unix), buffer size and cache are set.
5. Click on the **Next** button to the Authentication dialog. Authentication method can be set by choosing PCNFSD, NIS or UID & GID. Enter

- the User Name and Password or UID and GID for the default account to mount the NFS Drive (please refer to the **Default User Account** section for more information).
6. Click on the **Next** button to the Sharing dialog. Enter a share name for the NFS resource. The default name will be the drive letter. If none is specified, the drive will be mounted as a regular NFS drive (sharing can be modified from **Windows Explorer**). Any comments for the sharing directory can be added in the **Comment** text box. If any specific permission should be set for NT access right, click on the **Permission** button for further setting.
  7. Click on the **Next** button to the Summary dialog. Summary dialog allows user to have a final review on the settings before the completion of the NFS drive define.
  8. Click on the **Finish** button to complete definition or **Back** for modification.



*Example:*

*Predefined Host Information in host editor database:*

<i>Host Name</i>	<i>IP Address</i>	<i>Host Type</i>
<i>HP-UX</i>	<i>192.1.2.3</i>	<i>NFS Server</i>
<i>LINUX</i>	<i>192.3.5.6</i>	<i>NFS Server</i>

*Assuming the host information shown above has been created in the Host Editor program.*

<u><i>Drv</i></u>	<u><i>Server Addr.</i></u>	<u><i>Mnt Path</i></u>	<u><i>Auth</i></u>	<u><i>Share Name</i></u>	<u><i>Comment</i></u>	<u><i>User</i></u>	<u><i>Pass</i></u>	<u><i>UID &amp; GID</i></u>
<i>E</i>	<i>HP-UX</i>	<i>/home</i>	<i>PCNFSD</i>	<i>NFS1</i>	<i>NFS Drive</i>	<i>tom</i>	<i>****</i>	<i>-----</i>
<i>F</i>	<i>LINUX</i>	<i>/usr</i>	<i>UID&amp;GID</i>	<i>NFS2</i>	<i>NFS Drive</i>	<i>-----</i>	<i>-----</i>	<i>100, 20</i>

*Once all the configurations are correctly set, starting the Gateway service will mount the NFS resources with the information provided and perform auto-sharing.*

## Browse Exported NFS Drive

User may browse the exported NFS volumes on the remote NFS Server during the drive define process, all the fields in the Browsing dialog are described as following:

### Server Box

Display a list of NFS servers.

## 8 NFS Gateway

### Exported Path Box

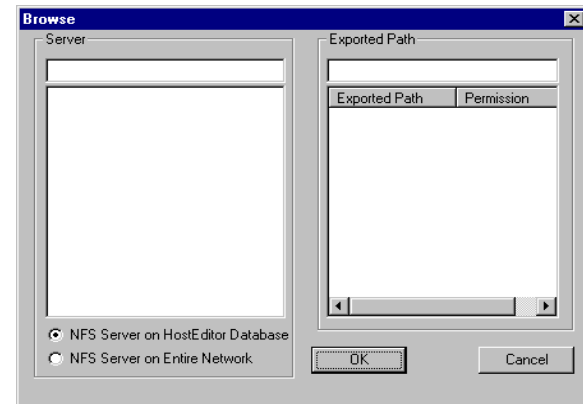
Display a list of directories exported by specified NFS server.

### NFS Server on HostEdit Database

By clicking on this radio button, a list of NFS Servers will be retrieved from the **Host Editor** program database.

### NFS Server on Entire Network

By clicking on this radio button Gateway will search for all existing NFS Servers on the entire network.



*Note: If none of the exported file systems is listed for the selected server, the followings may be the cause:*

- 2000/NT Gateway Server information is not in the UNIX host database
- Incorrect host information entered in the Host Editor ( eg. IP )
- Corresponding daemons for NFS mounting are not initialized
- The default user account used to mount NFS resources does not have permission to the exported drive
- Desired NFS resources are not being exported to NFS clients
- Incorrect Network Configuration on the local 2000/NT Server

## Set NFS Drive Options

The screenshot shows the 'Gateway Drive Options' dialog box in the 'Omni NFS Client' application. The dialog is organized into several sections:

- Buffer Size:** A dropdown menu is set to 'Default'. To its right is a checkbox labeled 'Cache Off'.
- Auto DOS to UNIX File Conversion:** A checkbox that is currently unchecked.
- Disable NFS 3.0:** A checkbox that is currently unchecked.
- File Conversion:** Two radio buttons are present: 'All Files' (selected) and 'Selected Extension'. A 'Set Extension...' button is located to the right of the 'Selected Extension' radio button.
- Locking Method:** Three radio buttons are present: 'NT File Locking only' (selected), 'With UNIX NLM', and 'Read Only'.
- File Attributes:** This section contains three columns of checkboxes: 'Owner', 'Group', and 'Other'. Each column has three checkboxes for 'R', 'W', and 'X' permissions. In the 'Owner' column, all three are checked. In the 'Group' column, 'R' and 'W' are checked, while 'X' is unchecked. In the 'Other' column, all three are unchecked.
- Directory Attributes:** This section also contains three columns of checkboxes for 'Owner', 'Group', and 'Other' permissions. The 'Owner' column has all three checked. The 'Group' column has 'R' and 'W' checked, and 'X' unchecked. The 'Other' column has all three unchecked.

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Advanced NFS drive options are available during the drive define process and they are described as following:

### Cache Off

If this option is checked, the data from NFS drive will be retrieved directly from NFS server. If it is unchecked, data will be stored in local cache memory.

### Example:

*Assuming the Cache Off option is not checked ( cache on).*

*When "Tom" has the NFS drive mounted on his system, any changes made by "Marry" from any client stations or console terminal with the same NFS resources will not be updated immediately.*

## 10 NFS Gateway

### Auto DOS to UNIX Conversion

By checking on this option, you can activate the DOS to UNIX bi-directional text file conversion. This option will remove the CR character and transform the text file to UNIX format. It is not recommended to turn this option on which might cause corruption with non-ASCII files. If not all files with different file extensions are wanted for file conversion, the “Set Extension” button will allow you to select desired files by their extensions.

### Disable NFS 3.0

By checking on this option, you can enable the use of NFS 2.0 instead of NFS 3.0.

### Buffer Size

Buffer size is initially set to default, and its value is automatically adjusted for each operating system. You can adjust different buffer sizes for the mounted drive.

*Note: Gateway Services can be optimized by adjusting buffer to the appropriate size. If an unstable Gateway Service is observed, please reduce the buffer size or disable NFS 3.0 for better performance.*

### NLM File LockingBox

Enable user to select file-locking option.

#### ***NT File Locking***

Uses NT File locking mechanism.

#### ***With UNIX NLM***

Applies UNIX file locking along with 2000/NT standard file locking method.

#### ***Read Only***

This option will set all the resources under the mounted drive to read-only.

*Note: This is an advantage for the administrator to prevent any accidental modification to the NFS resources.*

### File and Directory Attributes


Set the default file attribute for any new file/directory created through Gateway Service.

The file/directory format under the **File Attributes/Directory Attribute** is defined according to standard UNIX file format.

Each group has three boxes representing:



**R** – Read, **W** – Write and **X** – Execute

 *Example:*

*Assuming the file attribute is set to be:*

<i>Owner</i>	<i>Group</i>	<i>Others</i>
<i>R,W</i>	<i>R</i>	<i>-----</i>

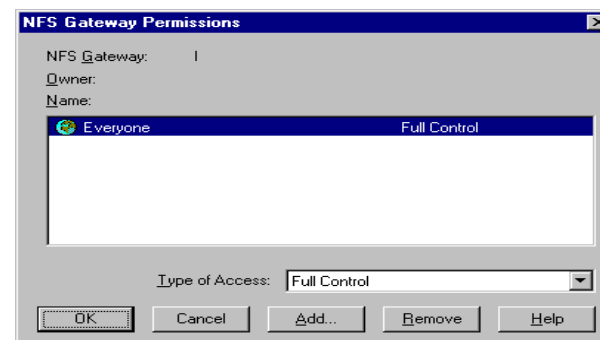
*Any file created in the mounted drive by “Tom” can be read/write by “Tom”, read by anyone in the same group and no access to others.*

File attribute can also be modified after the drive is being mapped. Please refer to **NFS Drive Property** for more information.

*Note: File name case setting can be modified after the drive is mounted from the property tab of the drive in the Windows Explorer.*

## Set User Permission

Administrator can configure user access permissions to the re-shared NFS drives in addition to the standard NFS permission. Administrator can add, remove, or set specific restrictions and access permissions to the selected drives using standard Microsoft security feature. This configuration is available during the drive define process and in the properties of the ready-mounted drive.



## Use Gateway Mount Wizard


Step-by-step procedure for defining an NFS drive:

## 12 NFS Gateway

1. Click on the **Define** button. The NFS Drive Define screen appears (figure 3).
2. Enter the valid NFS Server name configured in the **Host Editor** program for mounting in the text box.
3. Enter the mount path exported from NFS server in the **Mount Path** box. Mount Path list can be found by click on the **Browse** button, and the **Browse** screen appears for the desired path (figure 7).
4. Options for the NFS drive can be configured by clicking on the **Option** button, and the Drive Option screen appears (figure 8).
5. Click on the **Next** button to the Authentication dialog (finger 4). Authentication method can be set by choosing PCNFSD, NIS or UID & GID. Enter the User Name and Password or UID and GID for the default account to mount the NFS Drive ( please refer to the **Default User Account** section for more information ).
6. Click on the **Next** button to the Sharing dialog (finger 5). Enter a share name for the NFS resource. The default name will be the drive letter. If none is specified, the drive will be mounted as a regular NFS drive (sharing can be modified from **Windows Explorer**). Any comments for the sharing directory can be added in the **Comment** text box. If any specific permission should be set for 2000/NT access right, click on the **Permission** button for further setting.
7. Click on the **Next** button to the Summary dialog (finger 6). Summary dialog allows user to have a final review on the settings before the completion of the NFS drive define.
8. Click on the **Finish** button to complete definition and mount the NFS drive or **Back** for modification.

### ***What is an Default User Account***

The user account used to mount the NFS drive on the NFS Gateway will be referred to as the default user account. Any user accessing NFS based files or data through Gateway 2000/NT Server without proper user identification mapping will have the default user access right. This is an advantage for administrators to better manage unknown or unauthorized user access to the NFS resources. It is advisable to use a low privilege default user account.

 *Example:*

**Exported File System from UNIX: /home***Directory Tree of /home*

```

Home -----|-----|-----|-----|
             Steven  Bob    Marry  Guest
             uid:100  uid:102 uid:101 uid:300
             gid:100  gid:100 gid:100 gid:200

```

*Access Control in NFS Server:*

<i>Access Granted Users</i>	<i>UID</i>	<i>GID</i>
<i>Steven</i>	<i>100</i>	<i>100</i>
<i>Marry</i>	<i>101</i>	<i>100</i>
<i>Bob</i>	<i>102</i>	<i>200</i>

*Gateway Mounted NFS Drive Default User Information:**User Name: Guest**Password: xxxxxx (UID 300, GID 200)*

*If Steven accesses the NFS based 2000/NT Server drive, he will be given access right to **/home/john**. It applies to all the users that are granted with the relative UID & GID.*

*If Katy, who has no UID & GID, accesses the NFS based 2000/NT Server drive, she will be connected to **/home/Guest** with restricted privileges defined for the Guest account.*

**User Account Mapping**

Administrators can now map each user with a unique UID & GID to be used when a user tries to access any Gateway mounted drives. The mapping utility can be found on the NFS Gateway interface. The following information describes the function of each field on the mapping dialog.

**Microsoft Domain**

Lists all the domains that are within the network of the 2000/NT Gateway Server.

**Microsoft Host**

Lists all the 2000/NT hosts that are under the selected Microsoft Domain.

## 14 NFS Gateway

### Microsoft Account

Lists all the login names (users), local and Global Groups and general information for the selected Microsoft Host.

### UNIX Server's Name

Allows one-to-one dedicated UNIX server UID & GID mapping.

### UNIX Account

For assigning an unique UID and GID for the selected user.

### Mapped UID & GID

Shows the current UID & GID mapping for a selected user.

### GIDs & Secondary GID

For assigning and displaying any other GIDs for a selected user.

### Add Mapping

Adds user mapping information to the mapping list

### Mapping List

Shows all users mapping information and allows removal of mapping list.

The screenshot shows the "NT to Unix Account Mapping" dialog box. It is divided into two main sections: "Select NT Account" and "Select UNIX Account".

**Select NT Account:**

- Microsoft Domain: WORKGROUP
- Microsoft Host: TERMINAL
- Microsoft Account:  Show user list,  Show group list
- A list box showing user information with columns "Login Name" and "Full Name". The list contains: Administrator, eric, Guest, and a partially visible "j...".

**Select UNIX Account:**

- Browse UNIX Account Information via NIS
- UNIX Server: [For All UNIX]
- UID: [ ] GID: [ ]
- Secondary GID: [ ] with + and - buttons
- Secondary GIDs List: [ ]
- Buttons: Add Mapping, Mapped UID: [ ], Mapped GID: [ ], Mapping List, Close

### ***How To Map A User with a Unique UID & GID?***

All users who needs to will have the access to the NFS resources will need to have exact login names created in the local 2000/NT Gateway Server.

Perform the following steps to map UID & GID for a user:

1. Select a login name from the Microsoft Account List. You must select a Microsoft domain and a Microsoft host before you can select a login name from the list.
2. If your network has NIS set up, check on **Browse UNIX Account Information via NIS** to browse the existing UID & GID in the UNIX system, then select one account for mapping. Otherwise, select a specific UNIX server (default is set to **For All UNIXs**) manually enter the UID and GID in the blank text box.
3. If a secondary or more GIDs are desired for a selected user, please enter the GID in the text box under **GIDs** then click **Add**. To remove the secondary mapping, click on **Remove**. (Secondary GIDs can only be modified if there is no mapping defined for the selected user.)
4. Click on **Add Mapping** to map the UID & GID. To remove mapping, click on **Remove Mapping**. The mapped UID and GID should appear in the **Mapped UID** and **Mapped GID** text box.
5. Once the mapping is complete, click on the close button for the Gateway Service to update the mapping information.

**Note:**

*The mapping is based on one-to-one mapping for a single user name. If a user has different UID & GIDs for different UNIX Servers, specific UID & GID mapping can be performed by selecting specific UNIX Server (defined in Host Table) from the drop down box. This enables user to connect to different NFS resources with predefined UID & GIDs. All users belonging to Administrators group will have only the mapping of administrator account, not individual account. However, users with same user login name will use only one set of configuration to access the resources.*



Example: John can access HP with UID & GID of 100 and 200,

and access SPARC with UID & GID of 300 and 600.

 **Example:** *John from 2000/NT1 has the same access right as John from 2000/NT2*

Since browsing only searches the 2000/NT platform, Windows 95 and 98 clients will need to have login names created in the 2000/NT Gateway Server.

### ***How to do Group Account Mapping***

The NFS Gateway allows Group Account Mapping. To map a group of users in selected Microsoft Host, you will need to bring up the Mapping Dialog. You can view the group lists on a selected host by clicking on the **Show group list** radio button (to map the entire group with a unique UID & GID, you need to highlight a group from the list then assign UID & GID by manually type in or from NIS list). Accounts mapped for all users can be viewed by clicking on the **View Mapped Log** button.

## CHAPTER 3

---

# NFS Dual Gateway

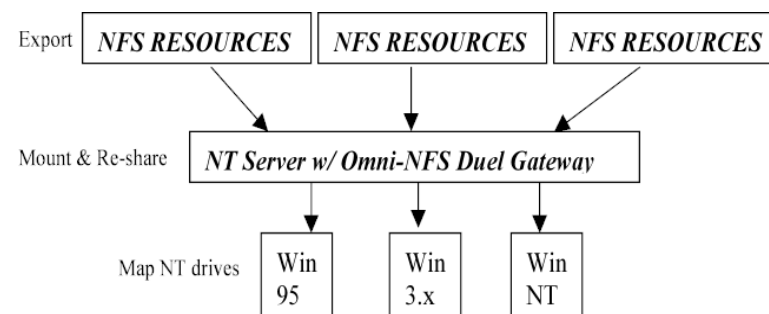
## Introduction

Omni NFS Dual Gateway is an extended package from Omni NFS Gateway. By including a NFS server in the product, Omni NFS Dual Gateway allows file sharing for both directions.

It provides **Transparent, Secure, and User-friendly** access for users to NFS resources. Files remain on the NFS host system, so Windows and UNIX users gain access to files without duplicating data. Individual Windows user identities are mapped to NFS accounts as they are passed through the Gateway, ensuring security and restricting file access privileges.

## Client Gateway Service

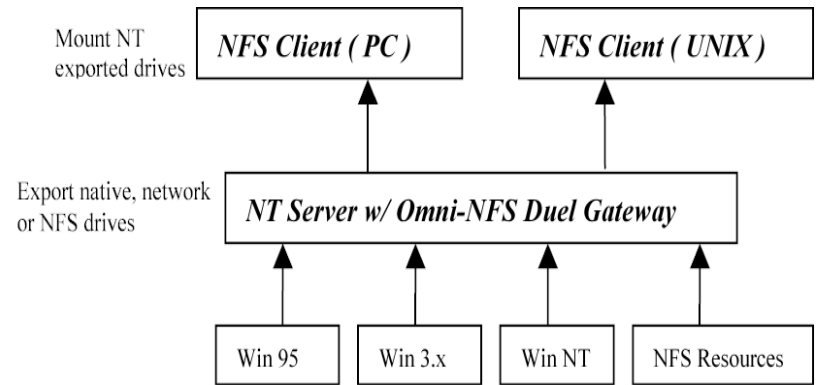
Provides re-sharing services for Windows Clients to access NFS resources from 2000/NT Gateway Server.



## Server Gateway Service

Administrators can also export any 2000/NT drives to the authorized UNIX or PC Clients through NFS using Server Gateway.

## 18 NFS Dual Gateway



### Starting NFS Dual Gateway

Please refer to Chapter 1 (NFS Gateway) for the Client Gateway configuration and Chapter 5 (NFS Server) for the Server Gateway configuration.



## CHAPTER 4

---

# *NFS Client*

### Introduction

NFS Client enables users of Microsoft Windows systems to gain access to the NFS file systems on UNIX networks.

This chapter explains how to access those remote files.

*NFS Client* provides you with the following advantages:

- You can now use all Microsoft Windows operating systems to access data/files located on the UNIX platforms. Windows applications now can directly work with the file while it is still on the UNIX machines. No need to FTP files back and forth.
- You can save hard drive space by keeping the file on the UNIX server.
- Seamless integration with the Windows platform enables users to access UNIX files easily via Windows Explorer, Network Neighborhood, and My Computer.

### Setup NFS Client Connection

NFS Client enables Windows users to gain access to UNIX drives as any typical Windows network drive. This means that there's no need to transfer files residing on the UNIX machines (NFS Server) to the local computer in order to work with them.

Before being able to setup NFS connection, you have to setup the host table on your system. Please refer to Chapter 9 – Host Edit – for detailed instructions.

There are three ways to mount remote UNIX drives:

## 1. Mounting through Network Neighborhood

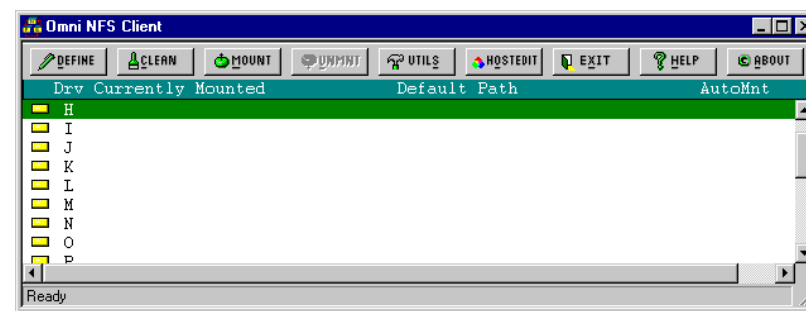
1. Double Click the **Network Neighborhood** icon on the desktop.
2. Double click the **Entire Network/XLink\_NFS** icon (NT Only). This window should list all of the NFS Servers you have entered in the Host Editor application.
3. Double click on the specific NFS server you wish to mount and a list of exported file systems will be displayed. If you do not see the list of exported file systems, please refer to the troubleshooting section.
4. Double Click on the file systems that you wish to mount.
5. Double click the exported file system to bring up the window displaying the contents of that file system.
6. You may also right click on the icon to choose to mount the network resource as a network drive. To configure detailed NFS drive options, please refer to **Setting NFS Drive Option** section.

## 2. Mounting with Windows Explorer

1. Run **Windows Explorer**.
2. Select **Tools** menu.
3. Select **Map Network Drive**
4. Select the drive to be mapped/mounted.
5. Enter the remote path to be mounted or select from the history list.
6. Press the **OK** button.
7. To enable the automount function, the **Reconnect at logon** option needs to be checked.
8. To configure detailed NFS drive options, please refer to **Setting NFS Drive Option** section.

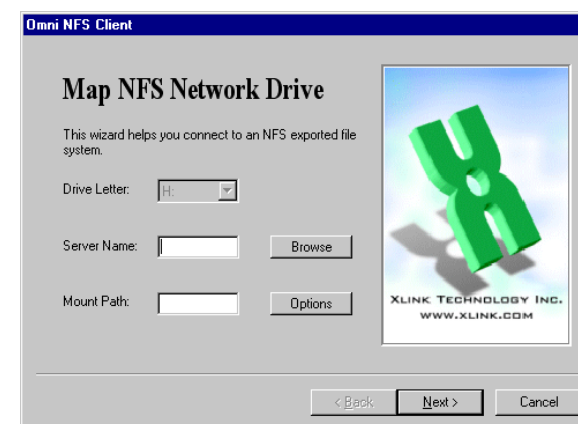
## 3. Mounting with NFS Client GUI / Mount Wizard

The NFS Client Window is used to see the status of drives, define/modify network drive resource definitions, or mount and un-mount drives.



Before you can mount an NFS drive, you must first define the NFS server systems you want to connect to in HOST EDITOR. (see Chapter 6 for details)

Highlight the drive letter you wish to use for NFS connection, then click on the **DEFINE** button to bring up the Mount Wizard.



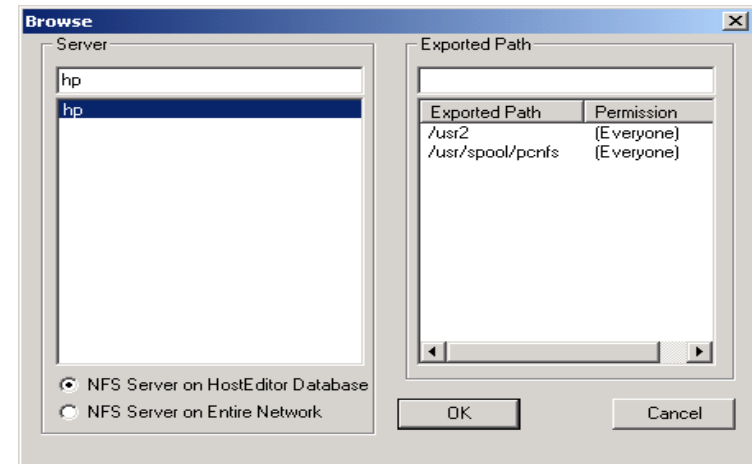
From this dialog box, you can define (NFS) server name and mount path. You can either type in the information or simply click on button BROWSE and let Omni NFS client program do the work for you.

If you decide to type, the Server Name can be either the name of the NFS server system or its IP address. Server Name can be up to 260 characters.

When entering the path, use the syntax native to the server on which the resource resides. For example, if you are entering a UNIX path name, begin the path name with a slash (/) and separate each successive directory name with a slash. The path can be a maximum of 260 characters.

## 22 NFS Client

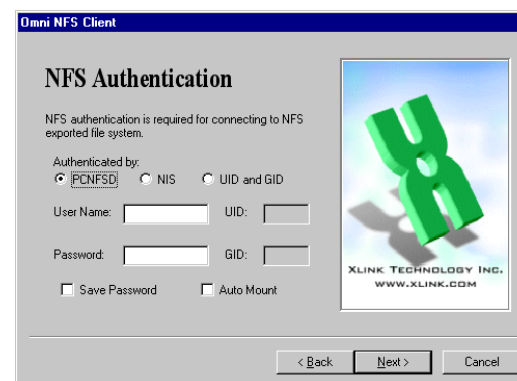
If you click on BROWSE, you will open up the dialog box looks like the one following:



In this example, the Server Name is “hp” which has two directories exported with permission to everyone. You can select the directory you want to connect to and click “OK” to go back to the NFS client GUI. Here you can either click on OPTIONS to modify system settings, or leaving the settings as default and move on to setup NFS connection.

Click on the **Option** button to modify system settings. For details, please see following section (Setting NFS Options).

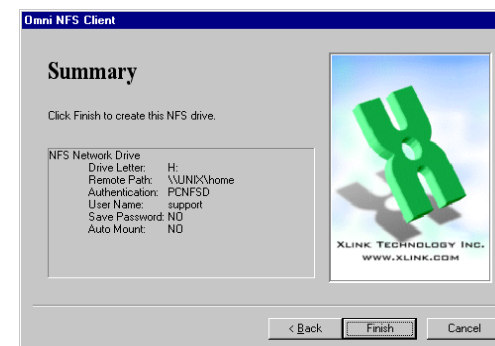
Click on the **Next** button to the authentication dialog. Type the user name and password and select either **PCNFSD** or **NIS** as the authentication method (see **NFS Authentication** section). You may also check **Save Password** box if you do not want to enter password each time **NFS Client** restarts (only for **PCNFSD** and **NIS** authentication). Select the **AutoMount** check box if you want the drive to be mounted automatically every time you run the XLink NFS Client application (see **Auto Mounting NFS Drives** section).



**Note:** The **AutoMount** check box is active only when **Save Password** check box is selected.

The next screen will bring you the summary of your definition. If the settings are correct, click on **Finish** to complete the drive definition.

Now, you are back to the NFS client GUI again. To establish the NFS connection, you click on **MOUNT** button. The “LED” on the drive icon will turn green if the drive is mounted successfully; otherwise, the light turns red. Any drive definition can be deleted by highlighting the defined entry then click the **CLEAR** button.



To unmount a network drive, you simply highlight the defined entry then click the **UNMNT** button. The “LED” will turn yellow.

Repeat the above procedures to define more drives or to modify existing drives which have already been defined.

## Setting NFS Drive Option

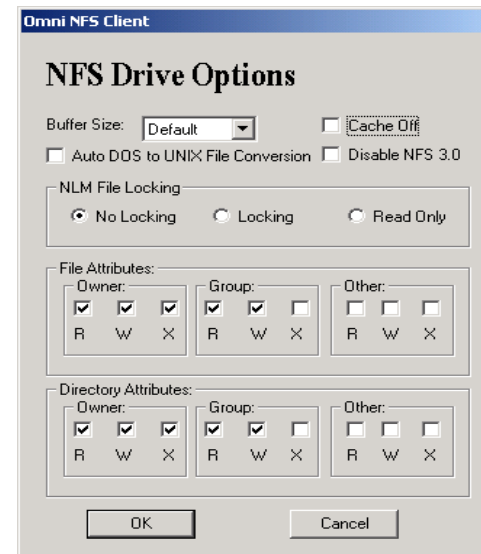
### 1. From Network Neighborhood / Windows Explorer

If you are mounting from **Network Neighborhood** or **Windows Explorer**, do the following steps to configure the advanced options.

1. Click on the NFS Client icon to bring up the NFS Client main interface.
2. To set the file attributes and filename case for any new file created through NFS connection, click on **UTILS** button then select **File Attributes and Filename Case**.
3. To set read and write buffer size for the NFS connection, click on **UTILS** button then select **Read/Write Buffer Size**.

**Note:** Any changes on the option settings are only effective before the NFS drive is mounted.

### 2. From NFS Client GUI



If you are mounting from **NFS Client GUI**, you can modify the following advanced options:

### **Cache Off**

If this option is checked, the data from NFS drive will be retrieved directly from the NFS server. If it is unchecked, data will be stored in the local cache memory to improve performance.

#### *Example:*

*Assuming that the Cache Off option is not checked.*

*When a user has the NFS drive mounted on his system; Any changes made to this NFS resources by anyone else on the network will not be updated immediately.*

### **Disable NFS 3.0**

Enables the user to select NFS 2.0 protocol as the connection protocol. It is recommended, however, to leave the setting unchanged as the NFS driver automatically negotiates for the best protocol automatically.

### **Buffer Size**

Buffer size is initially set to default, and its value is automatically adjusted by the NFS Client. You can also manually adjust the buffer sizes for the mounted drive. If connection to the NFS resource is not stable, you may want to reduce the Buffer Size setting.

### **Auto DOS to UNIX File Conversion**

Convert files from DOS to UNIX or UNIX to DOS format within the connection. It is recommended to set this option with text only connection; otherwise, non-text files might be corrupted by the conversion.

### **NLM File Locking Box**

Enable user to select file-locking option.

#### ***Locking & No Locking***

The file locking option is application dependent. When the “Locking” option is set, File locking will be supported only when user uses an application that supports such function to access the resources on the mounted drive.

## 26 NFS Client

*Example:*

*Assuming “Locking” is set.*

*If a user opens a file on the NFS resources with a text editor, the access permission for the same file by another user will be determined by the text editor’s built-in locking function.*

### **Read Only**

This option will set all the resources in the mounted drive to read-only mode.

### **File Attributes**

Sets the default file attributes for any new file created through NFS Client.

The file format under the **File Attributes** is defined according to the standard UNIX file format.

Each group has three boxes representing:

**R** – Read, **W** – Write and **X** – Execute

*Example:*

*Assuming the file attribute is set to be:*

*Owner -> R,W*

*Group ->R*

*Others-> --*

*Any file created in the mounted drive by “Owner” (Owner) can be read/write by “Owner” and read by any other user in the same group (Group) as the owner. No other user will have access to it (Others).*

File attributes can also be modified after the drive is mapped.

Please refer to **NFS Drive Property** for more information.

## **NFS Authentication**

There are three types of authentication with NFS client.

### **1. PCNFSD Authentication**

An authentication daemon runs on remote NFS Server.

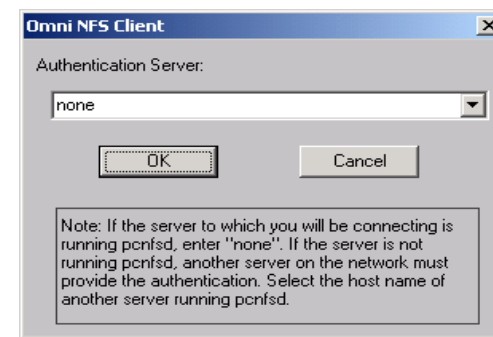
You can specify a PCNFSD authentication server by clicking on

**UTILS** button from the NFS Client interface and select

**Authentication Server**. If the UNIX station to which you will be



connecting is not running PCNFSD, enter **none** or leave it empty, otherwise enter the name of a UNIX station running PCNFSD as the authentication server.



This type of authentication requires username and password to be entered for UID and GID translation. Please refer to **Appendix B** for details.

## 2. NIS Authentication

NIS stands for Network Information Service. This authentication use NIS to translate the UID and GID from username and password. You will need to set up the NIS server entry before applying this option. Please refer to **Chapter 6 – Host Editor** – for how to setup references to NIS Servers.

## 3. UID and GID Authentication

Authenticate directly by using UID (**User ID**) and GID (**Group ID**) on the remote NFS Server machine. If the remote NFS Server is an UNIX machine, you can find your UID and GID by logging into your account and typing “id” at the command prompt.

## Mount Wizard

Please refer to **Mounting with NFS Client GUI / Mount Wizard** section for detailed information on the mounting procedure.

Once you have completed the Mount Wizard drive definition process, the NFS drive will be mounted and can now be accessed as a normal Windows network drive.

## Auto-Mounting NFS Drives

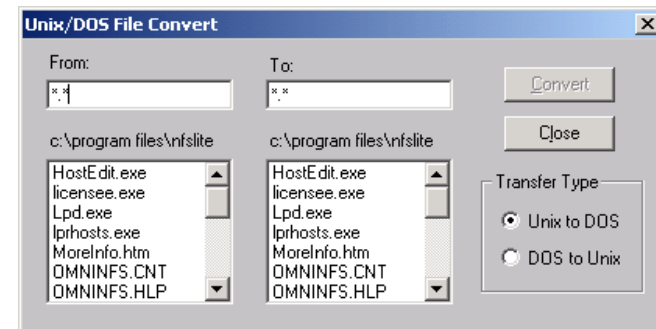
There are two ways to automatically mount NFS drives :

1. Map drives through Windows Explorer with **Reconnect At Logon** option checked and shut down the system without unmounting them. Windows will always try to reconnect previous network drives once you logon to the system again.
2. Selected the **AutoMnt** option in the **NFS Drive Definition** dialog box. NFS drives will only be mounted when the main NFS Client interface is initialized.

## Other Utility for NFS Client

### File Format Convert

This utility allows you to convert DOS-created text files to UNIX format or UNIX text files to DOS format. Simply mark the type of transfer you wish to make, then highlight or fill in the appropriate entries and press the **Convert** button. It is advised to apply this function to text files only.



## Symbolic Link Support

NFS Client will automatically get the final target file for a symbolic link if the paths for the symbolic link and those target files are both exported.

*Example:*

*File /usr1/test is pointed to /usr2/test.*

*Linked /usr2/test will only be seen on mounted drive only if both /usr1 and /usr2 directories are exported on the remote system.*



## Troubleshooting

### ❖ *Why can't I see the exported file systems on the NFS host?*

If you can not see any exported file systems, you will need to check to see if:

- TCP/IP connection is set up properly.
- NFS Server and other daemons are running on the host. ie. nfsd, mountd, lockd..etc.
- Host information in Host Editor is correct.
- Your user account has permission to access the NFS host.
- Your user account has permission to access the exported files.
- Linked path is included in the export file on the NFS host.

### ❖ *Do I have to unmount NFS drives if I want to change the buffer size or file attributes?*

If your operating system is Windows 95/98, then you will need to go through all the definition described in setting up a NFS drive. If your operating system is Windows 2000/NT, you can modify these settings by right clicking on the NFS drive icon (from explorer) and select **properties** to edit the setting.

### ❖ *Why am I getting "Authentication failed. Please check if PCNFSD is running" message?*

You will get this message when the remote NFS Server you are mounting does not have PCNFSD program running. If this program is not available on your NFS Server, then you have to start the PCNFSD on the remote system or change the authentication type to either NIS or UID&GID.

### ❖ *Why does the Authentication Dialog keep popping up after I have filled in all the information?*

The authentication dialog will appear if the authentication failed.

Authentication failure may be caused by:

- Your remote NFS Server does not have your host information in the host table for access permission.
- NFS program has detected a license violation or expiration (demo version only).



## CHAPTER 5

---

# *NFS Server*

### Introduction

NFS Server turns your windows system into a NFS server system so that you can export your local Windows drives or printers to remote NFS Clients. This chapter explains how to export your local drives or printers, and explain the difference between the Windows 95/98/ME version and the Windows 2000/NT/XP version of NFS Server. One of the key features of *NFSD* is its ability to operate with any Winsock-compliant TCP/IP.

### Features

The NFS Server incorporate the following features:

- Use Windows 98/95/ME/NT/2000/XP native TCP/IP
- Run as an Windows service , no logon needed
- Support FAT, NTFS, CDFS, HPFS file systems
- Support NFS version 2.0 and 3.0
- Support PCNFSD version 1.0 and 2.0
- Support mount version 1 and version 3
- Support Network Locking Manager (NLM)
- Seamlessly integrate with NT security, uses NT local or domain accounts. For this feature, all NFS users must also be NT users
- Works on Windows 95, Windows 98, Windows ME, Windows NT 4.0 Workstations or Servers, Windows 2000, and Windows XP.
- Centralized configuration program
- Support NFS printing through PCNFSD
- Include portmapper on both TCP and UDP protocols
- Provide NT/2000/XP accounts and groups to UNIX UID and GID mapping
- Integrate with Windows Explorer. Enable users to share NFS directories from Windows Explorer or Network Neighborhood
- Provide asynchronous fast write access for NFS 3.0
- Automatically recovers when windows 2000/NT/XP restarts

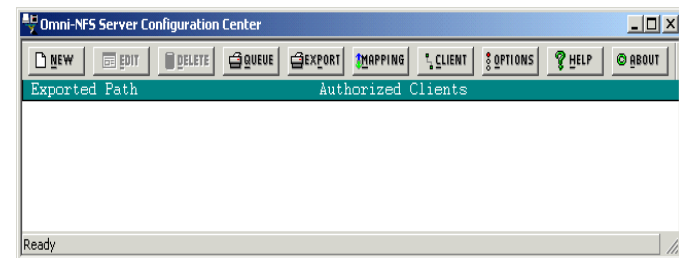
## 32 NFS Server

- Support up to two billion GB (64bit) long file size
- Show clients' connections that are active (showmount -a IP\_addr)

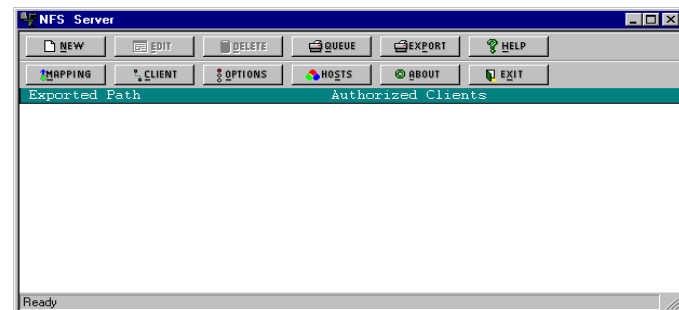
## Setup NFS Server

The **NFS Server** application is used to view the status of exported paths, define exported paths and exported printer and show printer queue status. Once you have defined or modified a resource within the **NFS Server** application, you need to restart the **NFS server** to activate them.

The status of all exported paths is presented in this window:



(Under Windows 2000/NT/XP)

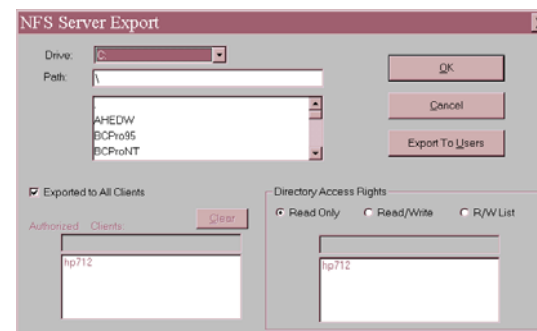


(Under Windows 98/95/ME)

Please perform the following steps in order to export Windows resources to remote NFS clients:



1. Click on the **New** button to start defining a new exported path. **NFS Server** then uses this information to export the resource you have defined when you restart the **NFS Server**.
2. In the **NFS Server Export** dialog box, select the path to be exported, including drive and directory.



By default, the **Export to All Clients** box is checked. If this path is restricted to certain remote hosts for access, uncheck the **Export to All Clients** and enter the host names (or IP) which you have previously defined in the **Host Editor** to be **Authorized Clients**.

If you want to export your file system to specific users use **Export to Users** (this option is only available for Win95/98/ME version of NFS Server). Please refer to the **Security Mapping** section.

3. The **Directory Access Rights** privilege setting defaults to **Read Only** for all authorized clients. You can grant read/write privilege to all authorized clients by selecting **Read/Write** radio button. In case you would like to grant read/write privilege to any of the authorized clients, simply check the **R/W List** radio button, and double click on the client in the list below. Any authorized client not selected in the **R/W List** setting will have Read Only privilege. Notice that each authorized client granted the Read and Write privilege is separated by a comma (,).
4. When all the parameters are correctly entered, press **OK** to save all definitions. The NFS Server window will then show the parameters that you have defined.
5. The changes to the export function will not be operational until NFS Server restarts.

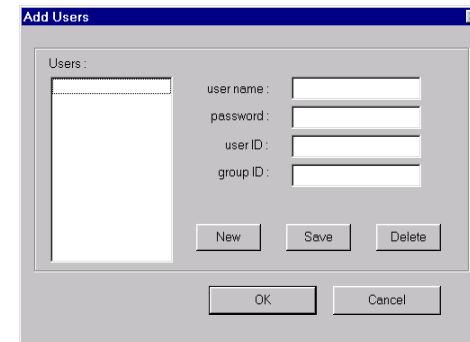
### 34 NFS Server

6. You can repeat the procedure to define as many export paths as you require. You may modify existing resource definitions that you need to change by clicking on the **Edit** button.

## Security Mapping

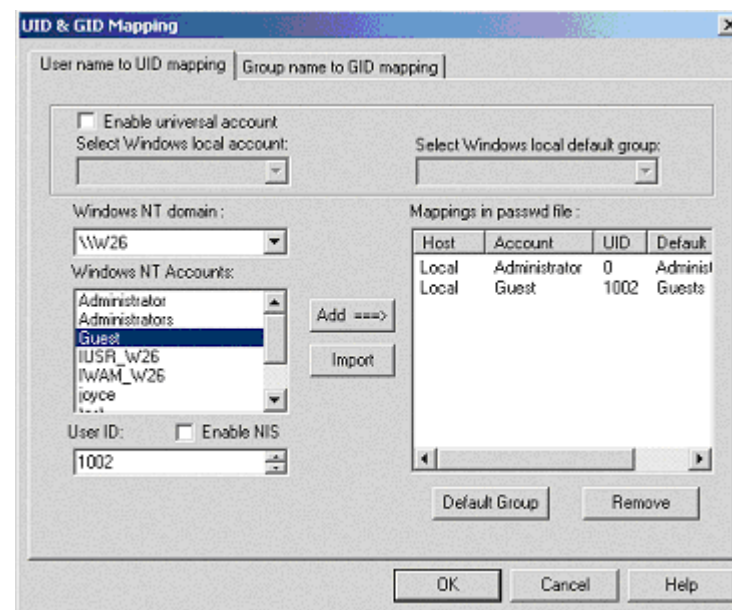
### With Windows 98/95/ME

You may specify each user's read and write permission to your exported path. To add users with specific read/write permission, click on the **Mapping** button from the main NFS Server interface or click on **Export to Users** button on the **NFS Server Export** dialog. A user's authorization always takes precedence over a host's authorization. For example, if a user can read and write to a directory, then both read and write permission are authorized to this user, regardless of the permission authorized to the host from which the user is connected.



### With Windows 2000/NT/XP

If you have FAT system, security mapping is not applied. If your system is NTFS formatted, you need to setup the security mapping before any file transaction takes place. The security mapping between your Windows 2000/NT/XP and UNIX file systems can be configured by pressing the **Mapping** button in NFS Server program.



### User Name to UID Mapping

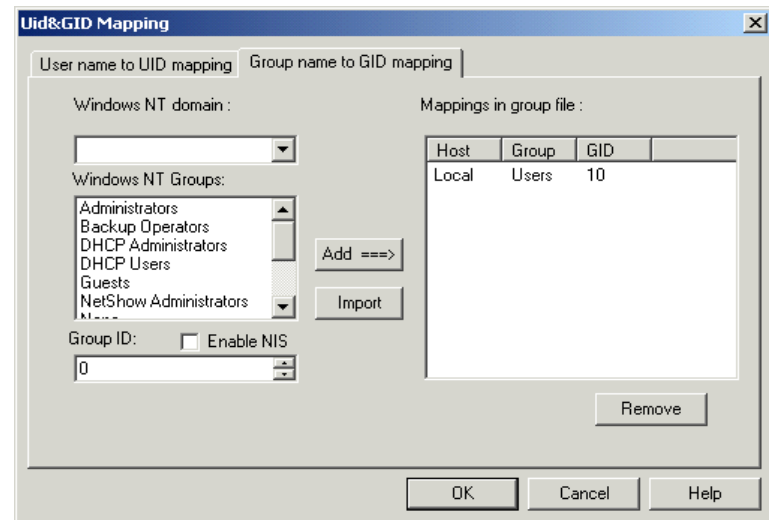
In this dialog, you see two tabs: **User name to UID mapping and Group name to GID mapping**.

Under User name to UID mapping screen, you can perform one-to-one mapping between your local user or domain user accounts and remote NFS client accounts. For each account mapped you have to specify a default group that corresponds to each mapped entry. You may also setup a universal mapping to a specific local/domain user account by checking the **Enable universal account** box and select the desired account. Enabling this option will allow any user on the remote NFS client machine without one-to-one mapping to access exported NFS resources with the security subscribed for the selected universal mapping entry.

Follow the steps to perform the User ID mapping:

1. Highlight the desired user account from the **Windows NT Accounts** list box.
2. Set the UNIX corresponding user id number to be mapped in the **User ID** edit box.

3. Click on **Add** ➔ button to add the selected pair to the mapping database. The **Mapping in Password File** box will now have the entry you entered. Please note that each NT/2000/XP account can only be mapped to one unique UID number and vis versa.
4. Highlight the entry you have just added in the **Mapping in Password File** box and click on the **Default Group** button to setup a default group for the selected user account.
5. In the **Default Group** dialog, highlight the desired entry from the list, then the box below lists all the groups that the user is a member of. Choose a group from the list as the default group for the mapping followed by **OK** button to return to the **Username to UID** mapping dialog.
6. Follow the above steps to do mappings for other users.



### **Group Name to GID Mapping**

The “Group name to GID mapping” needs to be done for both types of UID mappings: universal and limited. In this dialog, you can list the user accounts on your domain name server or on local machine. Follow the steps to perform the Group ID mapping:

1. Highlight the desired user account from the **Windows NT Groups** list box.

2. Set the UNIX corresponding group id number to be mapped in the **Group ID** edit box.
3. Click on **Add** ➔ button to add the selected pair to the mapping database.
4. The **Mapping in Group File** box will now have the entry you entered. Please note that each NT/2000/XP account can only be mapped to one unique UID number and vis versa.
5. You may repeat the above steps to map other groups to the corresponding GID number.

The result of UID mappings are saved in the file `\winnt\system32\drivers\etc\passwd` and GID mappings is saved in the file `\winnt\system32\drivers\etc\group` (assuming "winnt" is the Windows NT directory). The "mappings in passwd file" list box shows the contents in the current passwd file. The same applies to the group file.

You may import UNIX password or group file into the mapping list by copying them to your local system and clicking on the **Import** button to load the file content. The password field in the password file is not used in the NFS Server because it uses the NT internal account information to authorize the user for access rights.

Default Group is assigned to the file/directory object if group information does not exist or a new object is created.

## Working with Security

In order to keep the security structure of both the NFS Server and UNIX based system on the same ground, the security mapping structure is designed as UNIX file and security permission. eg. Assuming `c:/temp` has been mounted to `/mnt` on UNIX machine with Read/Write permission.

### *UNIX Information Table*

User / UID	Groups / (GID)
Root / 0	Sys / 2, root / 0, bin / 3, user / 20, staff / 50
John / 100	user / 20
Mary / 103	user / 20, staff / 50

### *NT Information Table*

User	Groups
Administrator	Administrators, Power User, User, Operator, Engineer

### 38 NFS Server

John	User
Amy	User, Engineer

#### *UID Mapping*

UNIX UID	NT User	Default Group
0	Administrator	Administrators
100	John	User
103	Amy	Engineer

#### *GID Mapping*

UNIX GID	NT Group
0	Administrators
20	User
50	Engineer

#### *NT File Permission*

C:\temp (owner = Administrators)	Everyone full control
----------------------------------	-----------------------

Once the drive is mounted, anyone who is on the mapping list will have Read/Write permission. Others will only have read permission since NFS Server cannot determine file permission setting with incomplete user information.

If **root** on UNIX machine creates a file, then the file security structure will be:

On UNIX	On NT
Owner = root, group = root	Owner = Administrators, group = Administrators
(permission depends on UNIX file mask)	

If you would like to have a group of users to access a specific directory, you can either assigned one user account for all the members of the group, perform mapping for each member and set the group permission accessible, or setup universal account for any file transaction.

*eg. John creates a **Staff** directory on the mounted volume and set the group permission to read/write/execute. Since John's default group is set to **User**, the directory will be accessible to members in **user** group; therefor, any user with **User** default group is included.*

If the owner or the group is viewed as **Nobody** or numbers on the UNIX client, then the mapping is either incomplete or failed. Please check the correct ownership of the file or directory for proper access permission.

Even if you are a super user account on the UNIX machine, you have to perform the security mapping to gain the proper permission.

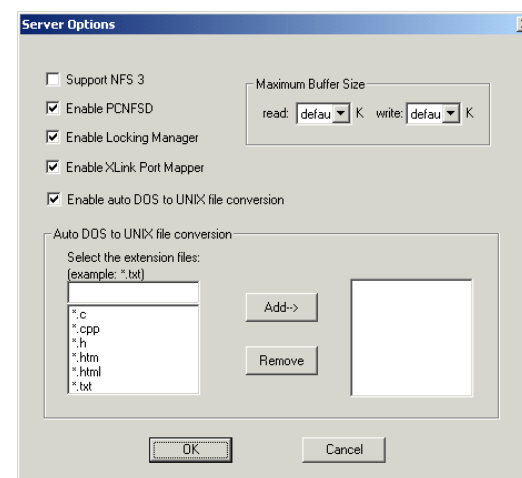
**Note:** If you want to connect to the NFS server using PCNFSD from the remote NFS Client, you must know both the user name and password of your NT account to do a successful mount. Since UNIX operating systems use UID and GID as user identity, and UID/GID are not supported by Windows 2000/NT/XP, you must map UID and GID into NT user accounts. By doing so, NFS server can determine the access permissions for each request from the NFS client. Mapping for users who are members of Administrators group will fail except Administrator account.

## Setup NFS Printer

You may setup NFS printer server on your system by clicking on the **Export** button from the NFS Server main interface. On the Exported Printer dialog, click on **New** button to add an NFS printer server entry. You may modify or remove any existing entry with the corresponding buttons. To view the print job queue for any defined NFS printer server, click on the **Queue** button from the NFS Server main interface. You may pause, remove, resume or modify printer setting on **NFS Printer Queue** dialog.

## Options for NFS Server

By pressing the **Option** button, the following dialog box appears:



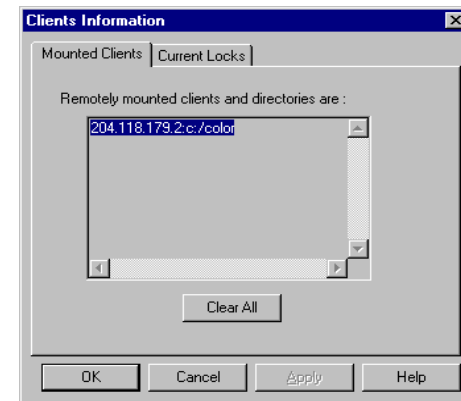
## 40 NFS Server

This dialog allows you to enable or disable NFS version 3.0, PCNFSD, Network Locking Manager, Xlink Port Mapper or Auto DOS to UNIX file conversion. You can specify the buffer size as well. After you have changed these options, you must restart the NFS Server service to have the changes take effect. The default setting is everything enabled.

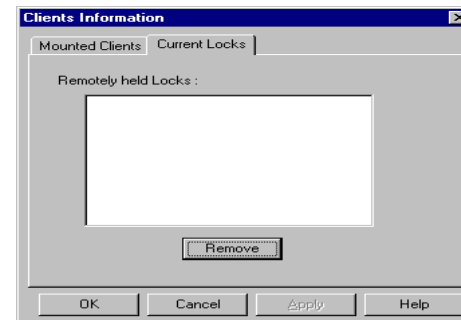
You can also modify the buffer size at run time from **Performance Tips** program (please refer to **Appendix C** for more detail information).

### Utility for NFS Server

Clicking the **Client** button will allow you to browse and modify two things: current mounts and current locks.



Current mounts will show you who is currently connected to the NFS Server.



Current locks will show you the file locks currently held by remote clients.



The mounts are saved in the file **mountd.list**. Sometimes if a client does not mount or unmount when it cannot access the NFS server across the network, or an unmount request is not sent correctly, a stale entry can be left in the mountd.list file. When you are sure there are no clients connecting to your NFS server, you can click "Clear All" to remove all the stale entries. Clear mount entries will cause the NFS Server to rebuild its internal file caching structure. Make sure to disconnect any NFS links prior to clearing mount entries.

The current locks show all the locks currently held by remote clients. These locks will recover themselves after a server crash or restart. If the clients crash or restart, they can still hold some locks and in this case, you must remove the locks manually from this dialog page. The removed locks will be removed from the system the next time you start the NFS server service.

## Auto Start NFS Server Service

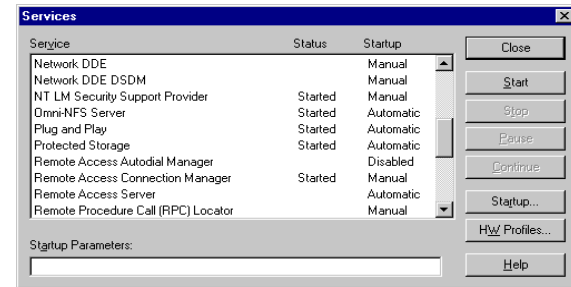
NFS Server on Windows 98/95/ME can be set to start at boot time by checking the "**Restart at Boot Time**" option with the NFS Server service icon in the system tray. On Windows 2000/NT/XP, NFS Server operates as an Windows Service and automatically starts whenever Windows 2000/NT/XP boots up. You can stop and restart the service or change the method of starting service in **Control Panel / Services**. If there are any errors while NFS Server service is starting on NT/2000/XP system, it will be logged as a Windows 2000/NT event. You can use Windows 2000/NT/XP Event Viewer to find out the detail of the NFS Server error.

## How to Export Network Drives (NT/2000/XP Only)

Special setting is needed if Windows network drives are to be exported through NFS Server Service. Before exporting an NT network drive, please perform the following steps:

1. Go to **Control Panel/ Services** and select **Omni-NFS Server**.

## 42 NFS Server



2. Click on the **Startup** to modify the settings.



3. In the **Log On As** group box, select **This Account**.
4. If the account name is not set to **Administrator**, you will need to click on the list button to get a list of accounts.
5. Select **Administrators** followed by the **Add** button to set the account name and click **OK** to validate your changes.
6. Once all the setting is set, restart the **Omni-NFS Server** service.

**Note:** The passwords of the administrator accounts for both local system and the peer workstation from which the network drive is mapped have to be the same.

## Troubleshooting

### ❖ *How do I mount the Windows exported resources from UNIX?*

You may issue the following commands on your UNIX client to mount the exported drive:

Mounting entire drive:

**(a) mount HostNameOrIPAddress:DriveLetter/ /MountPoint**

eg. mount 204.1.1.1:c/ /mnt

**(b) mount HostNameOrIPAddress:/DriveLetter/ /MountPoint**

eg. mount 204.1.1.1:/c/ /mnt

Mounting directory:

**(a) mount HostNameOrIPAddress:DriveLetter/Dir /MountPoint**

eg. mount 204.1.1.1:c/temp /mnt

**(b) mount HostNameOrIPAddress:/DriveLetter/Dir /MountPoint**

eg. mount 204.1.1.1:/c/temp /mnt



## CHAPTER 6

---

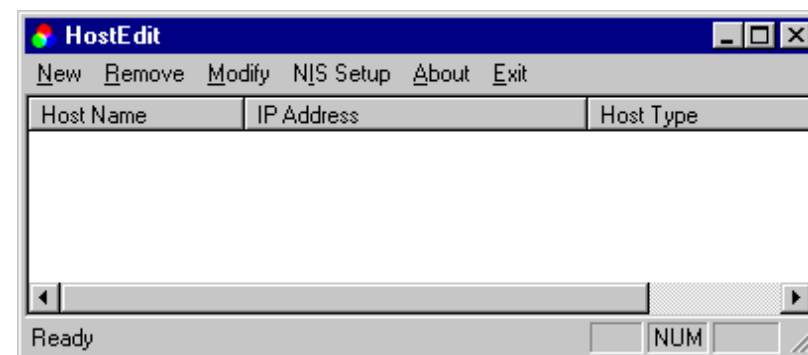
### *Host Editor*

#### Introduction

The **Host Editor** utility is used to create a host table on your local system, which is used by many Omni-NFS components such as NFS client, NFS Server, VT420, FTP client, etc.

#### Setup Host Editor

To add a new host to the host table, click on the **Host Editor** icon. The Host Editor dialog box will pop up.



Please perform the following steps to add a new host entry:

1. Click on the **New** menu to define a new host or double click on any of the existing listing (if previously added) to **Modify** settings for any selected host.

At the **Host Name & Address** dialog box (see picture in next page), enter a name (anything you want to call it) for the Unix system in Host Name.

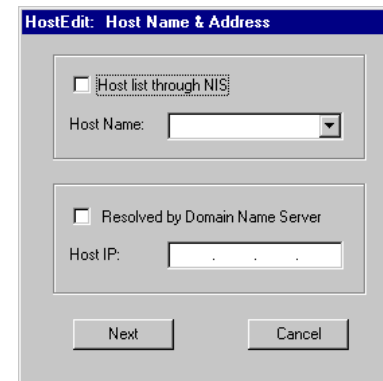
*(Note: The same host IP can be listed multiple times with different Host*

## 46 Host Editor

*Names.*) This name will be displayed in the Host Editor host list. Then you enter the IP address of the remote host to which you are trying to connect.

If you are authenticating through the NIS Server, and have set up the NIS Server settings in the **NIS Setup** menu (please see next session for details), check the **Host List Through NIS** box, and select the host from the drop down list.

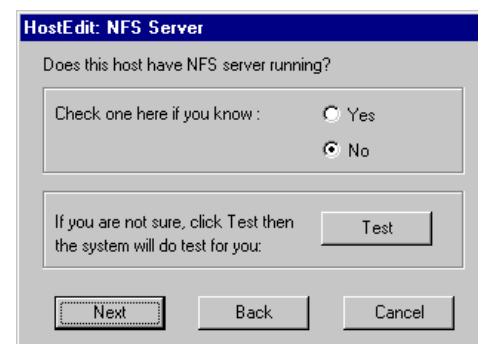
For Host IP, if you do not know the IP address of the remote host but know the real host name, enter the exact real host name in the **Host Name** field, and check the **Resolved by Domain Name Server** box to get the Host IP.



If you are running NFS client product, you will need to do following steps by click on the “Next” button. For all other products, Host Editor definition ends here. The “Next” button is now showing “Close”, and by click on it, you indicate the finish of Host Editor definition job.

2. In next dialog box, click on the **Test** button to check if NFS server function is running on the NFS server system. If the NFS server function is active, the *Yes* radio button will be selected for you, and you may proceed by clicking the **Next** button. Otherwise the radio button will stay at “No”. You will then need to manually start the NFS server function to run NFS client program.

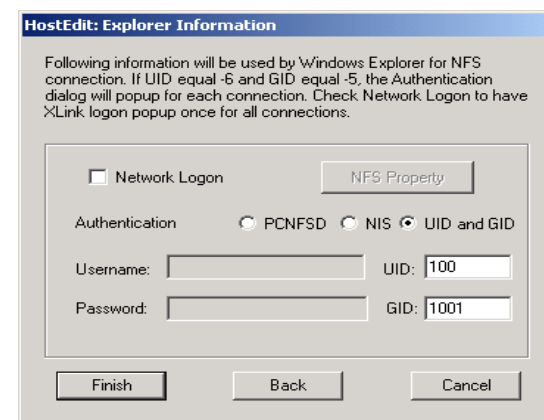
Examples on how to start NFS server on some Unix systems are listed in **Appendix D**.



3. In the **Explorer Information** dialog box, the file access authentication is assigned. The default authentication method is PCNFSD. With this radio button checked, enter the *User Name* and *Password* of your account on the NFS server system.

If your NFS server system doesn't have PCNFSD installed, you will get an error message later. One way to get around it is to use UID/GID method. Select this radio button, and enter the UID and GID numbers of your account on the NFS server system will get you though this part of the setting.

**Note:** To get UID/GID numbers, you login the NFS server system with your account, then type "id" at the prompt.



See next session (in next page) for details on NIS setup.

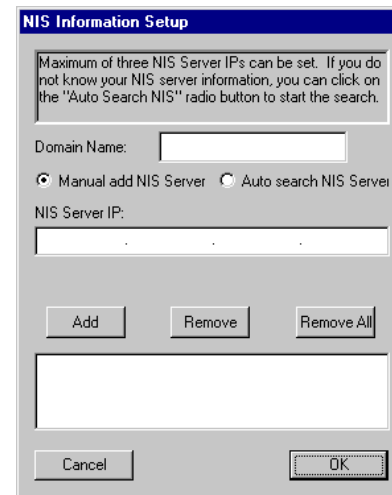
## 48 Host Editor

If **Network Logon** is checked, **XLink Logon Window** will popup once to prompt for Username and Password when making all NFS connections.

The **NFS Property** button allows you to set properties such as file name creation case for drives mounted through Windows Explorer or Network Neighborhood.

## NIS Setup

Click **NIS Setup** button to setup your NIS domain and NIS server address. Host Editor allows user to get specific host information from the NIS host list.



The image shows a dialog box titled "NIS Information Setup". At the top, there is a blue header bar with the title. Below the header, a text box contains the following message: "Maximum of three NIS Server IPs can be set. If you do not know your NIS server information, you can click on the 'Auto Search NIS' radio button to start the search." Below this message is a text input field labeled "Domain Name:". Underneath the domain name field are two radio buttons: "Manual add NIS Server" (which is selected) and "Auto search NIS Server". Below the radio buttons is another text input field labeled "NIS Server IP:". Underneath the IP field are three buttons: "Add", "Remove", and "Remove All". At the bottom of the dialog box are two buttons: "Cancel" and "OK".

### **Domain Name**

Enter the NIS domain name in this field.

*eg. MyNetwork.com*

### **Manual Input NIS Server IP**

Click on this radio button to manually input NIS Server IP.

*e.g. manually type in "192.11.1.1"*



**Auto Search NIS Server IP**

Click on this radio button to start auto searching your entire network for the NIS Servers.

Note: Only three NIS Server entries are allowed in the browse list.

## Troubleshooting

❖ *What is the main purpose of filling out the user authentication information at the end of the Host setup?*

The purpose of filling out the authentication method in the Host Editor is for users who wish to mount drives through Windows Explorer or Network Neighborhood.

❖ *Why can't I detect my NFS Server from the automatic detecting mechanism in the Host Editor?*

If you can not detect the NFS Server running on your host system, you may want to verify:

- If the NFS services are running on the remote system
- If the IP address is entered correctly



## CHAPTER 7

---

# LPD Server

### Introduction

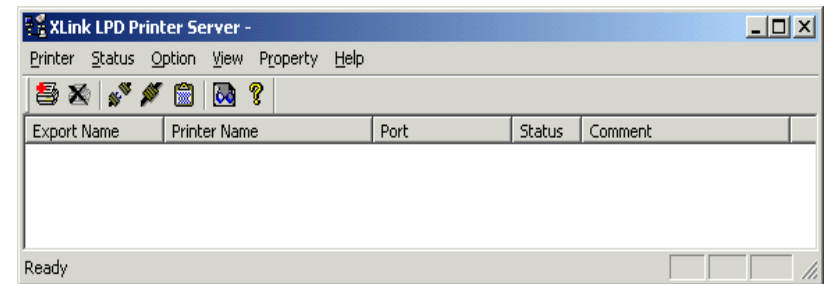
LPD server application provides UNIX print spooling services on your Windows operating systems. LPD accepts print jobs from many hosts or users on the network, queues the jobs and then sends them to any printer attached to the host running LPD.

To send a printing job from a Unix system to a remote printer attached to a Windows system with Xlink LPD installed, a standard Unix print command will do the job.

An added feature of “virtual printer” makes Xlink LPD more versatile. A file on the remote LPR client system can be sent to a specified folder on the LPD server system for later printing.

### Configure XLPD server

XLink LPD will automatically configure your system after installation. It generates a **spool** directory to store print jobs under your install directory. Make sure that there is an adequate amount of free disk space available in the installation drive. Printer queue names defined in the LPD are the remote queue names defined in the remote LPR clients.



The functionality of button selections in this GUI are explained following:

### **“Printer” Menu**

- **New:** Define the printer information.
- **Delete:** Highlight the export name, then delete the specific printer information.
- **Exit:** Exit the LPD program.

### **“Status” Menu**

- **Pause:** Temporarily stops LPD from sending print jobs to the specified printer.
- **Start:** Resumes the printing being sent to the printer (usually used after **Pause** button has been pressed)

### **“Option” Menu**

- **Toolbar:** Show/hide toolbar icons.
- **Status Bar:** Show/hide status bar.
- **Refresh:** Refresh the current connecting information.

### **“View” Menu**

- **Queue:** View the print job queue. It is also capable of deleting, aborting or resuming print jobs.
- **Setting:** Set and modify the spool directory and LPD port number.

### **“Property” Menu**

Highlight the export name, then press this option, it will pop up a dialog box with the information of the printer.

### **“Help” Menu**

- **About xlpd:** About XLPD server.
- **XLPD Help:** Access to On-line help file.

**Note:** the printer name assigned in “New” must match that set in remote LPR client system. In following example, “myprinter” is defined in LPD and LPR client system. (this is a HPUX command)

eg: `lp -dmyprinter myfile`

## How to setup LPR on remote Unix systems

Listed below are examples of how to setup LPR on remote Unix system on four kinds of Unix systems.

### 1. Sco UnixWare

Open “Sco Admin” dialog box, select “Printer Setup Manager”

Select ‘printer => ‘Add TCP/IP printer’

- a) name – give a name you want to call the printer
- b) Portocol Type – lpd
- c) Make/model – select the matching one
- d) Printer connection type – select “on remote server”
- e) Remote system – select or type the remote server system
- f) Remote Printer – the name defined in XLPD

### 2. HPUX

#sam

select ‘Printer/Plotters’ => actions => add remote printer/plotter

- a) printer name – give a name you want to call the printer
- b) remote system name – can be either the remote system name or its IP address
- c) remote printer name – the printer name defined in XLPD

## 54 LPD Server

### 3. Linux

From KDE drop-down menu, select KDE menus => system =>

KDE control panel => Printer

Click on “New” in the ‘Printer’ dialog box

- a) Queue name – give a name you want to call the printer
- b) Queue Type – select ‘windows printer’ or ‘Novell Printer’
- c) Select the match printer model

### 4. IBM

#smit

Select Print Spooling => Add a Printer Queue => Remote

=> Standard Processing

- a) name of queue to add – give a name you want to call the printer
- b) Host name of remote server – type in the remote windows system where XLPD is defined
- c) Name of queue on Remote server – type in the printer name defined in XLPD

## Troubleshooting

### ❖ *Is LPD a service?*

Yes, LPD server is running as a service.

### ❖ *Why can't I get a print out from LPD?*

The possibilities for the failure to receive or send print jobs are:

- Unrecognized option defined in the control file
- File content is corrupted
- Invalid remote printer name set
- Unstable network connection
- Critical timing issue when connecting through modem
- More than one LPD process running at the same time

## CHAPTER 8

---

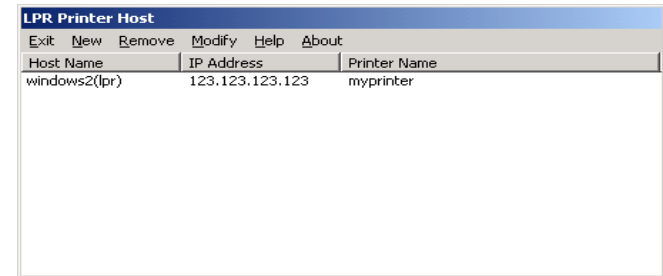
# LPR Hosts

## Introduction

The **LPR Hosts** utility is used to define hosts running **LPD** as **LPR** printer servers. The purpose of this application is the same as the Host Editor. In order to add an **LPR** printer to a Windows operating system, it is required to run this utility first to create a list of hosts with remote LPR printers for Network Neighborhood on Windows systems.

## Starting LPR Hosts

Click on the **LPR hosts** icon, the **LPR hosts** dialog box will show as following:



Click the **New** button to open up "Printer Editor" dialog box. In this box, you enter (remote) Host Name, its IP Address and the Printer Name. You will see an entry like the one shown in above GUI when you finish define a new remote printer. Now an LPR printer server is inserted into an LPR host list.

You will then be able to add the LPR printer to your local system and set it as the default printer as if it is local to your system. For details on how to add an LPR printer to your local system, go to next chapter.





## CHAPTER 9

---

# Adding Network Printers

## Introduction

Omni Print functions are seamlessly integrated with the Printer Manager on Windows platforms and supports both NFS and LPR printers. This chapter explains how to set up remote printers.

## Setting Up and Using NFS Printer

To setup NFS printer, the remote UNIX stations or printer servers must have **PCNFSD** or **RPC.PCNFSD** running. Following are the details on how to add a NFS printer to your Windows systems.

## Remote Printer Name

A printer name is a printer queue you have defined and exported on NFS servers or UNIX stations. Two important steps are needed on remote UNIX stations or NFS Servers before you are able to add a remote NFS printer to your Windows 95, Windows 98 or Windows 2000/NT. First, you need to export the spool path, (e.g. “/usr/spool”) from the UNIX system to the network. Second, you need to define a dumb printer or a printer queue with no filter on the UNIX system.

*Example:*

*If HP712 is your NFS server and has a HP Laser Jet III connected to it, the first step is to export the spool path “/usr/spool”, then define a printer name for HP printer on HP712 station. Please note that you MUST select a “dumb” driver for this printer name instead of HP Laser Jet III driver. Type the command “exportfs -a “ to get the export list and command “lpstat -t” to get the printer name list.*

*Special Note for SCO System:*

If SCO System is your NFS server, you may need to set access permissions of the path '/usr/spool' so that it is opened to everyone by the command 'chmod 777 /usr/spool'.

## Adding NFS Printer To a Windows system

On the Windows system,

1. Double click on **My Computer** icon
2. Double click **Printers** icon from **My Computer** window.
3. Click **Add Printer** icon from the **Printers** window.
4. Select **Next**
5. Select **Network Printer** in ADD PRINTER WIZARD box
6. Select **Next**
7. Click the **Browse** button.
8. Double click **Entire Network**

The dialog box will prompt you to enter the path and the name of a printer in the Printer field, or you can click **Browse** to select a printer from the Entire Network windows. For example:

1. Click **Browse**
2. Double click **Entire Network** icon
3. Select: **HP host**
4. Double click **Dumb1**

When the desired printer has been selected, click on **OK**. You may be prompted to select a driver for the printer if one is not currently installed on the network. The connected printer will appear as the default printer on the Printer Manager Toolbar.

## Setting up and Using LPR Printer

In order to add a remote LPR printer to your Windows system, you need first to run **LPR hosts** to define some hosts running the LPD printer servers. Please refer to Chapter 8 - *LPR Hosts* for more details.

To Add LPR Printer to Windows systems:

1. Double Click **My Computer** icon
2. Double Click **Printers** icon
3. Double Click **Add Printer**
4. Click **Next**
5. Follow the steps of Add Printer Wizard and select **Network Printer**
6. Click **Next**
7. Click **Browse**
8. Double click **Entire Network** to get hosts list
9. Select a host printer with **lpr** extension

*e.g. hp(lpr)*

Continue on to complete the printer adding process until you see a new printer icon showing in the printer group.

## Troubleshooting

### ❖ *Why can't I print after I add the printer to my system?*

There is always a chance that your print job may not behave as expected. You will need to see if:

- TCP/IP connection is set up properly
- PCNFSD is running if you are using NFS printer
- LPD is running if you are using LPR Printer
- Spool directory is accessible
- Correct filtering option is set
- Correct printer path is defined

### ❖ *Why do I get errors if I try to define a network printer under Win NT?*

In Windows 2000/NT, even if you browse the printer path, it might only show the printer name. If this is the case, you need to manually add the full path before the printer name.

*For Example:*

*If the printer is defined as hp5p on an HP1000 (UNIX server name), Windows 2000/NT will only show 'hp5p' as the printer location. You will need to add the following line; \\HP1000\hp5p for the printer to be validated properly into your Windows 2000/NT system.*



## CHAPTER 10

---

# FTP Server

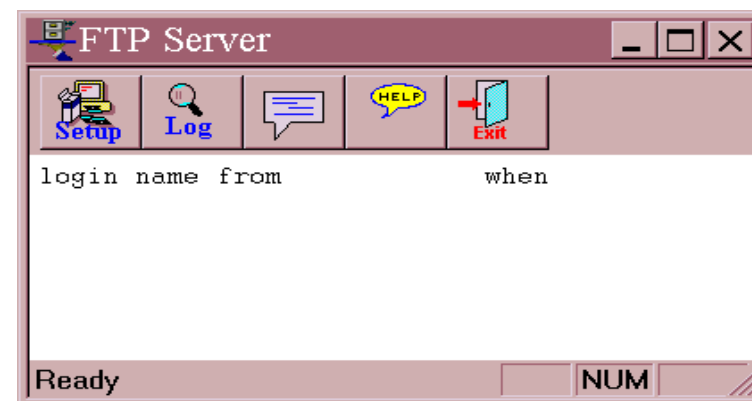
## Introduction

Omni FTPD utility allows you to configure a Windows system to become an FTP server. It provides tools to set up user accounts with assignments to the home directory, as well as individual access permissions.

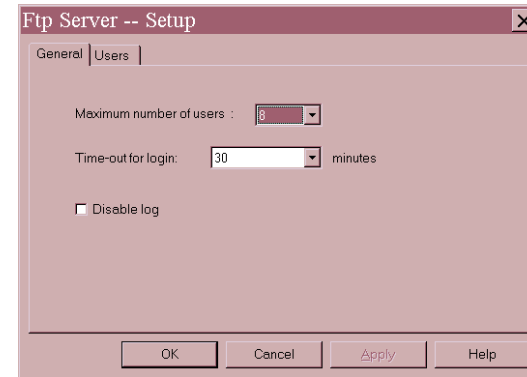
Anonymous account is not supported in this FTP server.

## Starting FTP Server

1. To start the FTP Server, double-click the **FTPD** icon in the XLink OMNI-NFS series software program group. An FTP Server dialog box will appear.



2. Click on the **Setup** button to configure your FTPD. First, go to **General** Setup to assign the maximum number of users and time-out. You may also disable or enable log files in General Setup.



### **Maximum number of users**

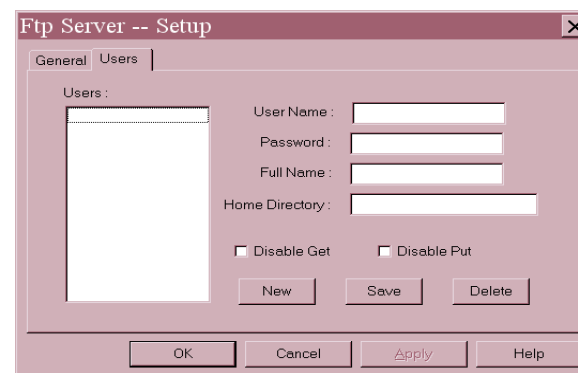
The default number of users is set to 8. If the number of users logged in exceeds the maximum value assigned, then the subsequent connection to the FTP Server will be refused and closed.

*e.g. If the max is set to 1 and **user2** tries to log in through the FTP service while **user1** is on, the connection will be terminated by the FTP Server.*

### **Time-out for login**

If a user's idle time exceeds the assigned timing in this field, the FTP connection will also be terminated.

3. You can set up new user accounts for the FTPD in the **Users** tab. In order to create new users, you need to assign their user name, password, full name, home directory, and access permission.

**Note:**

- If no password is assigned, user login will fail.
- Current version of FTPD does not support anonymous login.

4. Click Save button to save new configuration.
5. After creating all the users you need, click **OK** button to go to the **FTP Server** dialog box.
6. By clicking the **Log** button, it will show you a history of FTPD operations.
7. **Exit** button allows you to shutdown the FTP Server. Make sure that there are no users connected at the time, as their connection will be dropped.

**Troubleshooting**❖ *Why did my login failed?*

Failure to login may be caused by...

- Number of login users exceeds the maximum assigned
- Multiple FTPD's are running at the same time
- User does not have password assigned
- Anonymous login not supported





## CHAPTER 11

---

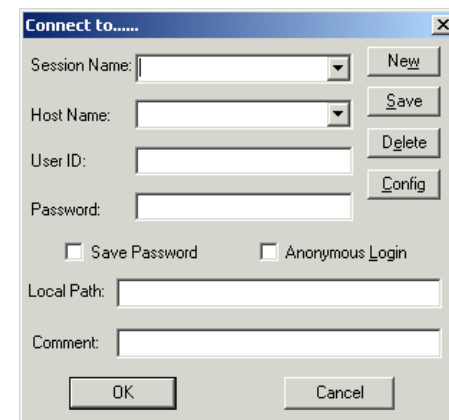
### *FTP Client*

#### Introduction

Omni FTP client is used to provide file transfer services across a wide variety of systems through the use of the File Transfer Protocol (FTP). It enables users to copy files and directories from one system to another. Simple types of files such as an ASCII text or a sequence of binary data records can be transferred through FTP connection. This connection also allows users perform remote file system control such as listing files, changing directories, and switching local drives.

#### Using FTP Client

Using FTP client to transfer files to and from FTP servers, click on the FTP client icon in an XLink program group.



## 66 FTP Client

Start by selecting the session configuration from the dropdown menu or create a new session name, then select(or enter) a host name or IP address. Enter the user name and password for the remote FTP system. You also have the option to save the password for future connections. For anonymous login, check on the “Anonymous Login” box. You can assign a local directory as the default directory after you successfully connect to the remote FTP server.

After login, user is able to:

- Transfer files and directories between local and remote systems.
- Delete files on a local or remote system.
- Rename the file on a local or remote system.
- View the file on a local or remote system.
- Make new directories on a local or remote system.

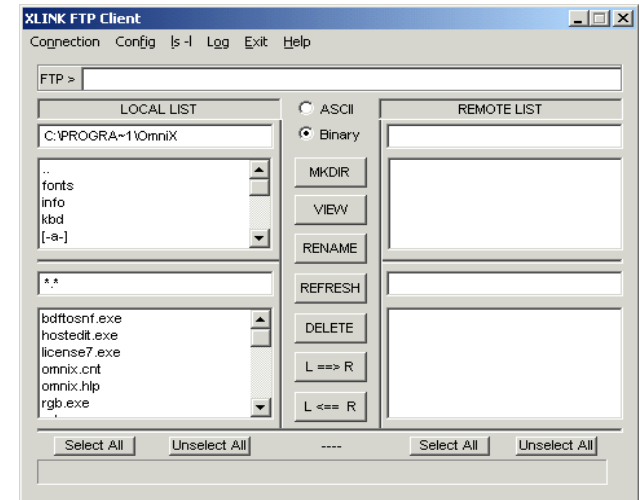
There are also commands that enable the user to:

- Connect and disconnect from the remote system.
- Configure the viewer functions.
- List all the files on a remote system.
- Display the login status message.
- Identify whether ASCII text or binary data is to be transferred.

All transfers are executed in either ASCII (text) or binary mode. ASCII mode performs carriage return/line feed translation and is only needed when transferring text files for use on a non-Windows system.

**Note:** If an anonymous user is defined, connection attempts for "anonymous" are accepted, regardless of the defined password or the password supplied in the pop up windows.

The FTP Windows allows you to connect and disconnect from the remote host, transfer files between local and remote systems, and view the contents of a file. The following is the description of these functions.

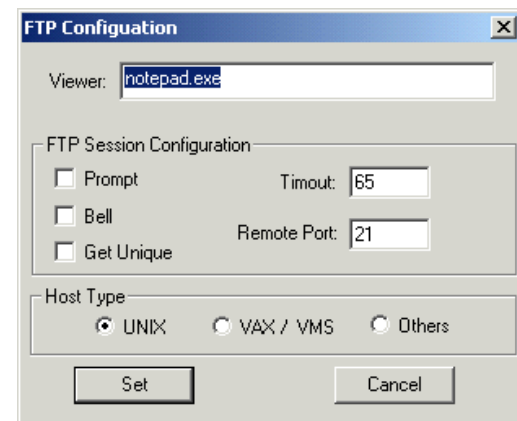


**“Connection” Menu**

This menu allows you to connect and disconnect from the remote host you select.

**“Config” Menu**

This field allows you to select the Edit program utilized to view the file. The default is Notepad.



## 68 FTP Client

The FTP Configuration includes the following options:

- Prompt: If you select this option, you will get a prompt dialog box before you send or receive files.
- Bell: This option enables bell sound if any error occurs.
- Time Out: The maximum time allowed to establish a connection.
- Remote Port: You can set the port number in this field.

The host type field includes three options, you can choose one of them.

- UNIX
- VAX/VMS
- Others

### “ls -l” Menu

This menu will show the details of the file list on the current directory of the remote host.

### “Log” Menu

This menu shows you the details of login and transfer status.

### “Exit” Menu

Press this button to close the FTP application.

### The “ASCII” Button

Check this box while you perform carriage return/line feed translation and transfer text files for use on a non-Windows system.

### The “Binary” Button

Select binary mode for transferring binary raw files.

### The “MkDir” Button

To make a new directory on a local or a remote system, you simply select the parent drive and directory and press the MkDir button. After pressing this button, the dialog box will prompt you to enter the new directory name.

### The “Delete” Button

To delete files on a local or a remote system, highlight the files you wish to delete, then press the “Delete” button. The files you have highlighted will be deleted.

### The “Rename” Button

To rename the file on a local or a remote system, highlight the file you wish to rename, on the local drive or on the remote system, then press the “Rename” button. A dialog box will prompt you to enter the new file name.

### The “View” Button

To view the file on a local or a remote system, highlight the file either on the local drive or on the remote system, and press the “View” button. The dialog box will show the content of the file you want to view. The default viewer/editor program is Windows Notepad.

### The “L==>R” Button & The “L<==R” Button

To transfer files between local and remote systems, highlight the files or directories you wish to transfer, then press the arrow button. The files you have highlighted will be transferred to the other system, into the directory currently displayed. You can also select this transfer command from the Commands menu bar.

## Troubleshooting

- ❖ *If you experience difficulties in using the **FTP** application, check the following items:*
  - ❑ Verify that installation and setup has been successfully completed.
  - ❑ Make sure the remote system provides an FTP server and that it is running. Note that some operating systems do not supply TCP/IP services with the standard package (for example, VMS).
  - ❑ If the FTP application reports a failure to connect error message, use the Ping application to verify that the connection to the remote system is working.
  - ❑ If the FTP application reports a failure to login, verify that the user name and password were entered correctly.
  - ❑ Make sure the correct transfer type (ASCII/binary) is chosen correctly. Transferring a binary file when the transfer type specifies ASCII may cause a failure in transfer.
  - ❑ Make sure you have permission for specific operations (for example, write access to a directory).

## CHAPTER 12

---

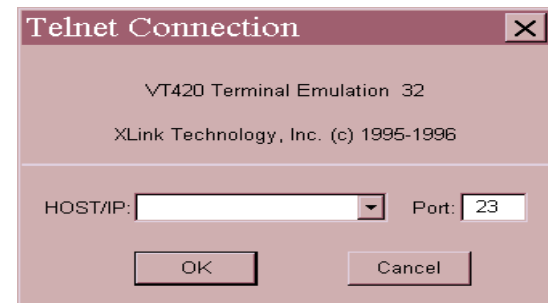
### *VT420(Telnet)*

#### Introduction

Omni VT420 is a terminal emulation program. With added features, such as keyboard mapping, background/foreground color selection and personal control of many general system settings, Omni VT420 has become a useful tool one enjoys using while getting work done.

#### Using VT420 Terminal Emulation

VT420 is a terminal emulation program that allows you to connect and communicate with hosts that support VT100, VT220, VT320, and VT420 terminal modes.



#### Multiple Session Capability

You can start more than one session at a time and use VT420 to open multiple Telnet windows on a single host or a group of different hosts.

You can also create custom icons using the "Program Manager " which allows you to click on the icon to directly start your VT420 session.

## Starting and Terminating VT420

To start a VT420 session, follow the steps below:

1. setup Host Editor (see chapter 6)
2. start VT420 by double clicking on the VT420 icon in the Omni-NFS Program Group
3. a "Connect Host" dialog box will appear, you select the host from the drop down menu
4. click "OK"

Once you have connected to a host, the VT420 window will appear on your display. The host name you specified will appear at the top of the VT420 window, and the host login prompt will appear in the window.

Enter the login info required for your host system. Once the connection is established, the VT420 window will appear active on your display. You can interact with the host by choosing commands from the displayed menus, or by typing commands in the VT420 window.

To terminate a VT420 session, you double click on the "close" icon of the Control Menu box, or by selecting **Exit** from the Telnet **Commands** menu.

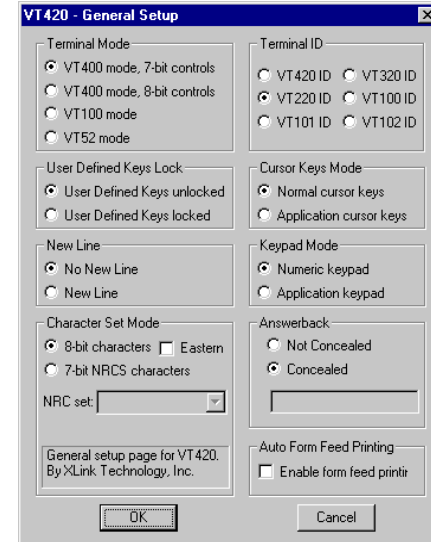
In the connected VT420 windows, a "Setup" button is there for you to manipulate the settings of the connection. Following are the detailed explanations on items in "Setup".

### General Setup

This General Setup menu item allows you to choose the terminal and cursor type, UDK, or keypad. (see picture in next page)

Here is a list of General Setup items available:





## **Terminal Mode**

### ***VT400 mode, 7 bit controls***

Lets the terminal uses all available VT420 features. The terminal normally uses 8-bit graphic characters and 7-bit control characters. You can also select this mode for VT200 and VT300 applications. This mode is recommended for most applications.

### ***VT400 mode, 8 bit controls***

Lets the terminal use all available VT420 features. The terminal uses 8-bit control characters. If your application uses 8-bit control characters, you must select this mode.

### ***VT100 mode***

This mode lets the terminal operate as a VT100 terminal. Use this mode for applications that require VT100 compatibility.

### ***VT52 mode***

Lets the terminal support VT52 applications. VT52 mode is not compatible with VT100 and VT400 modes.

The default terminal mode is VT400 mode, 7 bit controls.

### **Terminal ID**

The terminal emulator can report to the remote host as different terminal types. If your operating system or application programs on the remote host need (or only supports) specified types of terminals, you may change the Terminal ID parameter to fit the requirement.

In ANSI modes (VT100 or VT400 mode), you may set the terminal ID to VT420, VT320, VT220, VT102, VT101 or VT100 ID. In VT52 mode, the terminal only has VT52 ID.

The default terminal ID is VT220 ID.

### **Users Define Keys Lock**

The User Denied Keys (UDK) can be changed or not changed by the remote host. If UDK is locked, the remote host can not change the definition of UDKs. You may change the UDK definitions locally. See User Defined Keys Setup.

The default value of this parameter is UDK unlocked.

### **Cursor Keys Mode**

Cursor keys act in two modes: Normal cursor mode and Application cursor mode. The cursor keys send different codes to the remote host depending on the cursor mode. Normally, you don't need to change this parameter. It may be changed by control codes of the remote host.

The default cursor mode is Normal cursor keys.

### **New Line**

If the parameter of "No New Line" is selected, the terminal will only send the **Carriage Return (CR)** code to the remote host when you press **ENTER** key. Otherwise, it will send both Line Feed (LF) and CR code to the remote host in "New Line" mode. The default value of this parameter is "No New Line".

### **Keypad Mode**

Keypad mode acts in two ways: Numeric mode and Application mode. Normally you don't need to change this mode setting. It may be changed by control codes of the remote host. The default keypad mode is Numeric mode.

### **Character Set Mode**

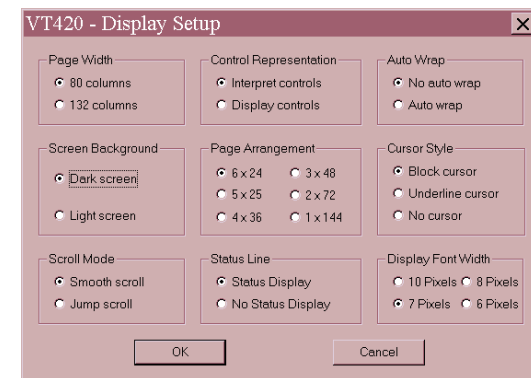
Allows you to set characters to either 7 bits or 8 bits.

### **Answerback**

The Answerback message Specifies a sequence of characters that are sent to the host when ^E (Control E) char is received. If **Not Conceal** is set, then the terminal will display the answerback message.

## **Display Setup**

This Display Setup menu item allows the user to adjust the terminal page width, screen background, cursor style, and scrolling method. Here is a list of Display Setup options available;



### **Page Width**

The width of the terminal can be set to 80 columns or 132 columns. If you change the width of the page, the display of the current terminal screen will be erased. The default page width is 80 columns.

### **Control Representation**

The terminal emulator can display, interpret, and then execute the control code when receiving a control codes from the remote host. When you select the display control mode, all control codes will be displayed using a special font. This is usually used for debugging.

### **Auto Wrap**

Auto Wrap allows to you to select whether or not the text will automatically wrap to the next line when you reach the right margin.

### ***No Auto Wrap***

This feature lets the terminal display each new character in the last column of the line when you reach the margin. Each character will overwrite the previous character at that position.

### ***Auto Wrap***

This feature lets the terminal display the new character on the next line when you reach the margin. By default, the terminal does not invoke the auto-wrapping mode.

### **Screen Background**

This feature allows you to select light text on a dark background, or dark text on a light background. The default screen background is the Dark Background.

### **Page Arrangement**

This feature allows you to select the number of lines per page. The following modes are supported.

6x24, 5x25, 4x36, 3x48, 2x72, or 1x144.

The default page arrangement is 6x24 lines.

### **Cursor Style**

This feature allows you to enable or disable the cursor. You can also select block or underline cursor when the cursor is enabled.

## **Scroll Mode**

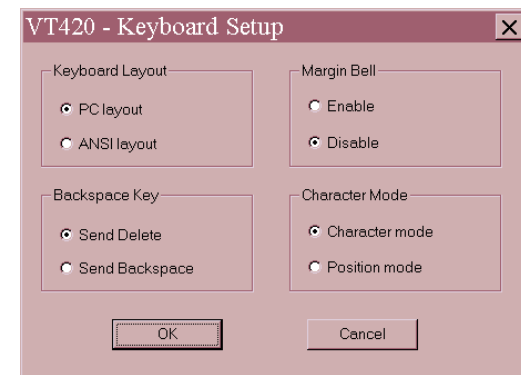
### ***Smooth Scroll***

Selection of this mode sets the screen scroll whenever it detects a scroll request. This is the default scroll mode.

### ***Jump Scroll***

Selection of this mode prevents the terminal from scrolling until there are no longer any characters received. This mode makes the terminal scroll at a faster rate.

## **Keyboard Setup**



## **Keyboard Layout**

### ***PC Layout***

Allows you to use the PC keyboard definition for sending key codes to the remote host.

### ***ANSI Layout***

Allows you to use ANSI keyboard definition when sending key codes to the remote host. This layout is convenient for you if you are familiar with the ANSI keyboard layout.

### **Margin Bell**

Allows you to enable or disable the margin bell. If the margin bell is enabled, the speaker will sound when the cursor is eight characters from the right margin.

By default, the margin bell is disabled.

### **Backspace Key**

Allows Backspace key to send a Delete code. Some applications require the Backspace key to send a Delete code. In such case, change this parameter to fit the application you are running.

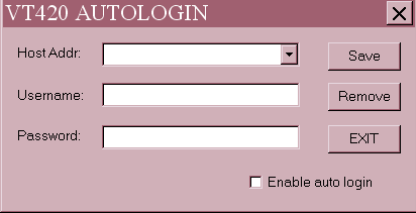
By default, the Backspace key will send the Delete code.

### **Character Mode**

Allows the user to select the keyboard operating mode.

## **Auto Login**

Auto Login enables the user to predefine the user name and password to a specific Host listed in the Host Editor. Users can now login without having to manually type in his/her User Name and Password. It is designed to simplify tasks for users with multiple UNIX accounts and different identities.



VT420 AUTOLOGIN

Host Addr:  Save

Username:  Remove

Password:  EXIT

Enable auto login

### **Host Addr**

The default host addresses contained in this list are the host addresses defined in the host database (using Host Editor). User can also manually type in other IP addresses or domain names in the editable area.

### **Username**

Enter user login name for the selected Host Address.

**Password**

Enter login password for the selected Host Address

**Enable Auto Login**

This option enables/disables the auto login function for a specific Host Address.

**Printer Setup**

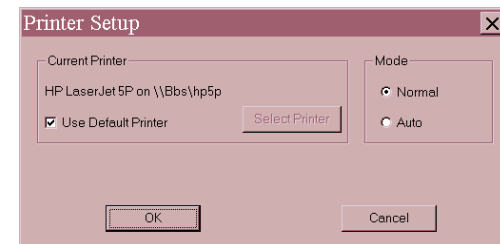
Select the Printer button to see the Printer Setup dialog box. In this dialog, you can designate the output device for your printer setup. The Printer Setup dialog contains the following options:

**Normal**

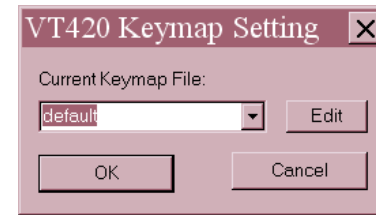
This option sends no output to the printer. This is the default.

**Auto**

This option sends the current line of text to the printer when the terminal receives a line feed character. This mode is most useful when the printer is operating in scrolling mode; it does not work well in full-screen mode. This mode may be toggled on and off by the user as well as by the host software.

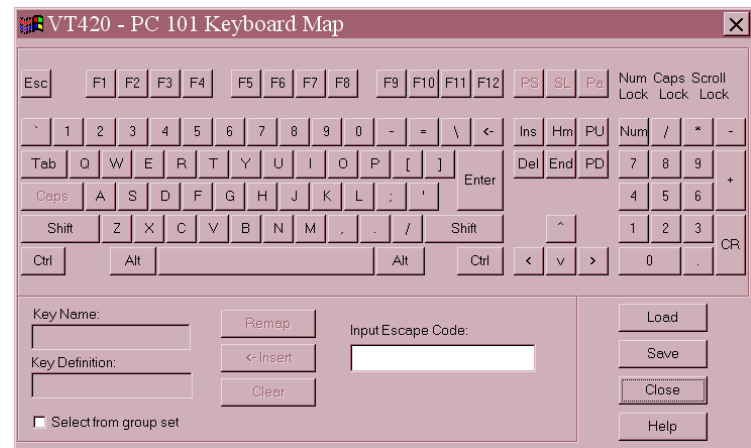
**Keymap**

VT420 also provides keyboard re-mapping utilities on the VT420 sub-menu which allows you to select XLink predefined keymap files or create your own key definitions.

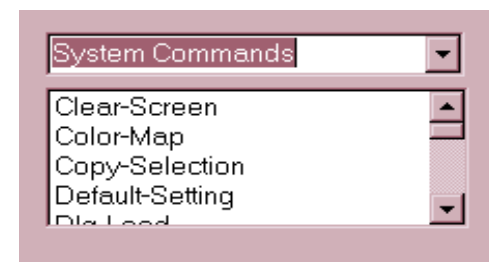


Keymap files can be modified by selecting a file from the list followed by clicking **Edit**. Keyboard settings are applied immediately after selection.

By clicking on the **Edit** button, a keyboard layout will be displayed for the user to modify any key definitions.



User can either specify the **escape code** or select from the list by checking the **Select from group set** box as shown below.





Follow these steps to define a key:

1. Select a key by pressing the key buttons on the keyboard layout; (Key name will display the key button that is selected for modification).
2. Click on the **Remap** button and input the key definition in the **text box** or **select from group set** followed by pressing the **Insert** button. (**Remap** button is changed to **OK** button)
3. Click **OK** button to finish the mapping.
4. After all the key definitions are completed, the user can click on the **Save** button to save the keymap file (all keymap files have the extension .kmp); otherwise, the modification will be discarded upon exiting VT420 or re-editing of the current keymap.

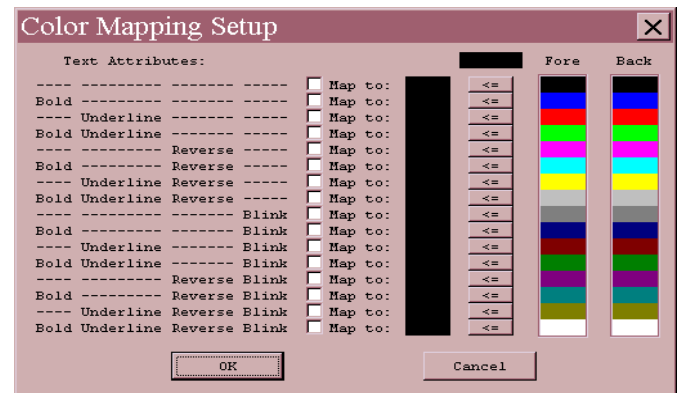
## Color Mapping Setup

You can simulate host session color schemes or create your own window colors by using the Color Mapping Setup.

Within this dialog box you can choose preset color schemes, make your own, or assign specific colors only to specific character attributes. A number of preset color schemes are available for you to choose from. These color schemes include colors for text attributes and background.

### Assigning colors to individual text attributes

You can assign any color shown on the available color palette to any one of the text attributes or to the screen background.



## Troubleshooting

❖ *If you are starting up a VT420 and the VT420 window isn't created, check the following list:*

1. Verify the host is up and running.
2. Verify the host name or IP address you entered. If you specified a host name that didn't work, specify its IP address instead.

Addresses are specified in dot notation as follows:

value.value.value.value

Each value must be in the range of 0 through 225. Values starting with **0x** or **0X** are treated as hexadecimal. Values starting with **0** are treated as octal. All other values are treated as decimal.

If this format works and entering a host name doesn't, then somewhere in the network your host name is not being translated to the correct address.

If your transport resolves the host names with a hosts file, you can view and edit this file from the **Host Editor**. If your transport uses a different method to translate host names to addresses, consult your transport documentation.

3. Ask your network administrator if the Telnet daemon is up on the host. Sometimes it is not running.
4. Lastly, confirm that your host supports Telnet. Some hosts do not.

## CHAPTER 13

---

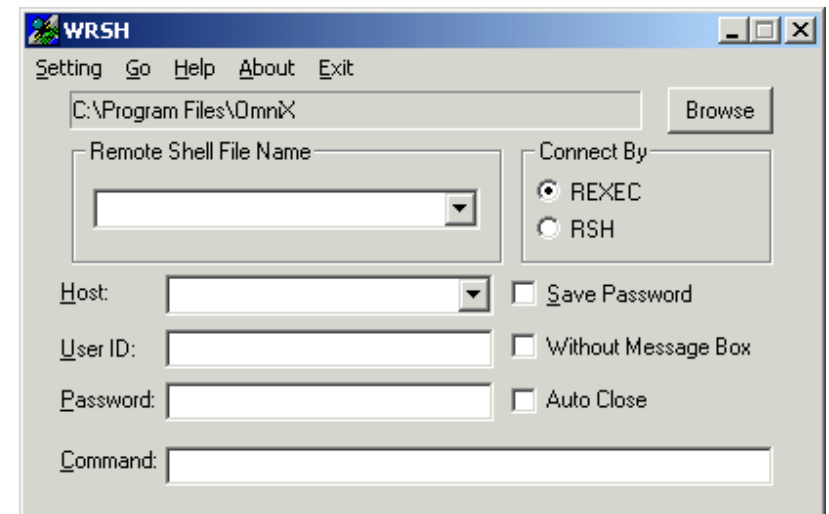
# *RSH (REMOTE SHELL)*

### Introduction

The RSH application allows you to execute commands on the remote host without having to login first. To use RSH, your machine may need an entry in the **.rhost** file in your home directory on the remote host, depending on the UNIX system.

### Using RSH

When you run the RSH application, you will get a **Remote Shell** dialog box:



In the dialog box, you must specify the **Host** to which you wish to connect, and your **User Id** and **Password** for the host. The Host name can be selected from the drop down box. The **Command** you wish to execute must be a UNIX command native to the particular UNIX host.

*e.g. # ls -l ( current directory listing )*

*# pwd ( show current path )*

You can save the current settings as default. After you have provided all the information that the RSH application needs, you can click on the **GO** button to execute the command.

#### **Without Message Box**

Check this box if you wish to disable any message box that informs users the status of the command.

#### **Auto Close**

Enables users to terminate RSH application right after the execution of commands.

Note: Only one simple command can be performed each time. The RSH files can also be run as script files to execute simple commands from your desktop.

## APPENDIX A

### **NETWORK LOCK MANAGER (NLM File Locking)**

The Network Lock Manager (NLM) is an RPC service that provides advisory locking of files across the network. There are various versions of the NLM in existence; this implementation is version 3.

Because the NFS protocol is stateless and has no knowledge of locks that may or may not have been granted, clients that wish exclusive access to a particular file must call the Network Lock Manager on the server to request access. The server Network Lock Manager is responsible for creating and destroying locks on files, as well as mediating requests for shared or exclusive file access.

This version 3 implementation supports file locking and sharing for DOS machines under **Windows 95/98** and **Windows 2000/NT** on the net. File sharing is a mechanism which allows a DOS process to open or create a file and to restrict the way in which subsequent processes may access the file. For example, a DOS client may request that a file be opened for reading and writing, and that subsequent users may only open it for reading.

File locking is a mechanism that only allows one DOS process to open or create a file using the same name in the same location at the same time. For example, a DOS client may request that a file be opened for reading and writing, and the subsequent users can not open it.

#### **File Locking**

All the files in this mounted drive will follow File Locking mechanism while File Locking is selected. For example, if a DOS NFS client with **File Locking** has already opened a certain file, then another NFS client with **File Locking** can not open the same file simultaneously.

#### **No Locking**

All the files in this mounted drive will *not* follow the File Locking mechanism while No Locking is selected. For example, a DOS NFS client

with **No Locking** can open any files for reading and writing no matter which file is opened whether it is dedicated to be locking or no locking.

### **Read Only**

All the files in this mounted drive can only be opened for reading and not for writing when **Read Only** is selected. For example, a DOS NFS client with **Read Only** can only open files for reading no matter which file is opened by locking or no locking.

## APPENDIX B

### *PCNFSD*

#### **PCNFSD Protocol Definition**

The purpose of the PCNFSD protocol is to provide a personal computer NFS client with the authentication and network printing services that are usually available in larger and more capable systems. Its use, while not necessary, is highly desirable. The source code for the server implementation of PCNFSD is freely available from Sun Microsystems.

#### **Authentication**

The NFS file access control model is based upon the uid/gid mechanism used in X/Open-compliant systems. All NFS remote procedure calls must be made with AUTH\_UNIX credentials from which a uid and gid can be extracted. If a client implementation supports the use of NFS services without any form of authentication, it should use the uid/gid pair (0xffffffff, 0xffffffff) (i.e., (-2, -2)), which is conventionally associated with the identity “nobody”. Client and server support for access as “nobody” is an implementation or administrative option.

Operation as “nobody”, while feasible, is undesirable, since the client can only access file system hierarchies with unlimited “other” permissions, and administrators of server systems have no way of controlling resource usage. For this reason, it is expected that personal computer NFS implementations will require or encourage users to establish valid access credentials. A typical implementation might be to prompt the user to enter a username and password, which could then be validated using the PCNFSD\_AUTH procedure, which will return a uid/gid pair. The client can then use this information to synthesize the AUTH\_UNIX credentials for subsequent RPC requests.

Since it is undesirable to pass clear-text passwords over a network, both the username and the password are mildly scrambled using a simple exclusive-or operation. The intent is not to be secure but to defeat “browsers”.

## **Print Spooling**

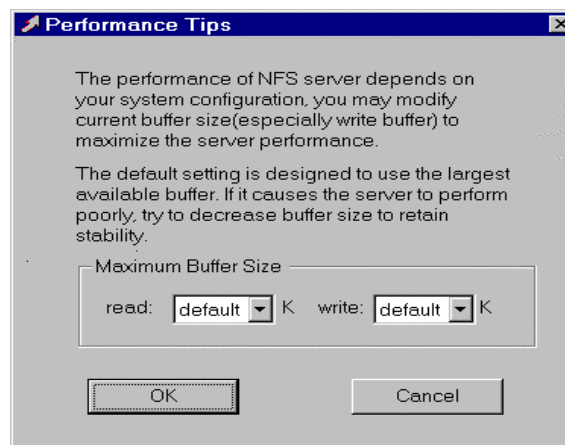
The availability of NFS file operations simplifies the print spooling mechanism. The PCNFSD returns the name of a directory on the server which is exported via NFS and in which the client may create spool files. It also accepts start-print request from the client.



## APPENDIX C

### *Performance Tips*

Performance Tips is a stand-alone program that allows users to modify the buffer size (read/write) for NFS Server. The default buffer size is automatically set to the maximum available buffer according to your system configuration. However, default buffer size may at times not be the best setting for some system environments. Modifying the buffer size to fit your system could minimize the package delay time and maximize the NFS Server performance.





## APPENDIX D

### ***Examples on how to start NFS server on a Unix system***

Five examples on four kinds of Unix operating systems are listed below. First login as “root”, then follow the steps to get NFS server service started.

#### **1. HPUX**

- a) sam (open up System Admin Manager) <RT>
- b) select Networking/Communications
- c) select Networked File System (FNS)
- d) select Local Directories Exported
- e) click on “Actions”, then select Enable NFS Server

#### **2. IBM AIX**

- a) #smit <RT>
- b) select Communications Applications & Services
- c) select NFS
- d) select Network File System (NFS)
- e) select Start NFS

#### **3. Linux**

- a) #cd /usr/sbin <RT>
- b) #rpc.mountd& <RT>
- c) #rpc.nfsd& <RT>

OR

#/etc/rc.d/init.d/nfs start/stop <RT>

**4. Solaris**

- a) #cd /usr/lib/nfs
- b) #./nfsd&
- c) #./mountd&

**5. Sco UnixWare**

- a) #cd /usr/lib/nfs
- b) #./nfsd&
- c) #./mountd&

# GLOSSARY

## ***Active Window***

Also known as the focus window. This is the window currently accepting input. The mouse cursor must be in the window to make it active, and you may need to click on the window to make it active. If you can not see the cursor, you can generally tell which window is active because its border is highlighted. However, this depends on what window manager you are using.

## ***Address***

A number that identifies a unique location in the computer's memory where information is stored.

## ***Address Resolution Protocol (ARP)***

A protocol that translates Internet addresses into Ethernet addresses.

## ***ANSI***

American National Standards Institute

## ***Application Clients***

Application programs that run under the X-Window system.

## ***ARP***

Address Resolution Protocol

## ***ASCII***

Acronym for American Standard Code for Information Interchange. A standard set of characters used in data transmission applications.

## ***AUI***

Attachment Unit Interface. Interface type for Ethernet.

## ***Baud Rate***

The number of binary digits transmitted per second over a serial line.

***Bitmap***

A highly structured file that contains not only an image's picture elements or pixels, but also the type, sizes and color information.

***Broadcast Address***

The address used to send information to all equipment on the network.

***Control Characters***

Characters that send a command to the terminal when you type them, rather than sending the character itself to the screen display.

***Data Bits***

The number of bits in a transmitted or received byte of data (usually either 7 or 8). The number of data bits needs to be determined when setting serial communications parameters.

***Default***

A value or instruction in effect unless explicitly changed.

***Download***

Transferring data from a host to a terminal.

***Ethernet***

A local area network technology that uses Coaxial or Twisted Pair cable to interconnect different computers.

***Ethernet Address***

An address identifying a module on an Ethernet network.

***Ethernet Driver***

A program that receives and de-multiplexes the various packet types available over the network.

***File Server***

A computer on the network that provides services to client computers on the network. File servers often contain large amounts of storage and many software applications that can be used by multiple users at the same time.

***Firmware***

Software that resides in the computer's read-only memory (ROM). It generally controls the operation of terminals, printers and other devices.

***Flow Control***

A software-determined method for controlling the rate at which data is transmitted. Flow control is mainly used to avoid network congestion.

***Font***

A collection of characters and symbols that share a common design.

***Font Directory/Path***

The directory on the host where the fonts are located.

***Gateway Machine***

The computer that serves as a link between two networks.

***Gateway Address***

The Internet address of the gateway machine for the network. This is important when dealing with multiple networks, so that applications know if a machine is on a local network or on a network connected by a gateway machine. If networks are connected by a gateway machine, the gateway machine's address is included in the routing information.

***Graphical User Interface (GUI)***

Describes both the appearance and the function of window components (such as frames and canvases) and control items (such as buttons, pull down menus, and slide bars).

***Host***

The computer that provides application programs and fonts to the terminal.

***Host Address***

The unique Internet address of a host machine on the network. This address must be different from that of any other machine on the network.

***Internet Address***

Address of a node on the network using the Internet.

***Internet Protocol (IP)***

The Internet standard protocol that defines the Internet "datagram" as the unit of information passed across the network.

***Modem***

Abbreviation for Modulator/Demodulator. A device that converts digital data from a device into an analog signal that can be transmitted on a phone line. It also converts the analog signal received back into digital for the device.

***Network File System (NFS)***

A method of accessing files over a network on a host machine. The files look like they are in a directory on your machine, and you can use them as though they were your own files (if the permissions are set properly).

***Network***

Two or more computers connected by cable that use communication software to exchange information.

***Network Address***

A 32-bit-wide address divided into four 8-bit fields, that uniquely identifies a machine on the network. Each field is separated by a period. For example: 192.2.1.24.

The three basic types of address, Class A, Class B, and Class C are characterized as follows:

- Class A*      Used for large networks. A value from 0 to 127 in the first 8-bit field identifies the network as Class A. The remaining 3 fields establish the host address.
- Class B*      Used for medium-sized networks. A value from 128 to 191 in the first 8-bit field identifies the network as Class B. The first two 8-bit fields indicate the network address, the last two 8-bit fields establish the host address.
- Class C*      Used for small networks. A value from 192 to 255 in the first 8-bit field identifies the network as Class C. The first three 8-bit fields address the network, the last 8-bit field establishes the host address.



***Packet***

A set of information of a certain size sent between on a network. Packets have specific destinations, as opposed to datagrams which have no specific destination.

***Path***

A location of a directory on a computer, usually shown as a list of directories and subdirectories separated by a delimiter. A relative path is a list of directories that stand between your directory and the file you want. An absolute path is the path starting from the root directory (/). Note that the path does not include file names.

For example:

Absolute path: /home/xlink/usr1/misc.

Relative path (if you are in "xlink"): usr1/misc.

***Protocol***

The set of language rules that two networked machines must follow in order to communicate.

***RAM***

Random Access Memory. Memory chips that can be written to or read from. Data stored in these chips is lost when the power is turned off.

***Reverse Address Resolution Protocol (RARP)***

The protocol that translates an Ethernet address into an Internet address. This protocol is needed for your unit to discover its Internet address from the network.

***ROM***

Read Only Memory. Memory chips that cannot be written to after they are manufactured. These chips are used to store permanent system information.

***RS232***

A type of communication over a serial cable characterized by serial binary data interchange.

***Server***

A station on a network providing a service, such as making a files or printers available.

***SLIP***

Serial Line Internet Protocol, a protocol that allows IP protocol to be used over an asynchronous RS-232-C port.

***TCP/IP***

Transmission Control Protocol/Internet Protocol. The type of communication used by UNIX machines connected to an Ethernet network. TCP provides reliable communication among computers once the data link is established. IP provides the services necessary to manage the movement of data through a computer network, including address resolution, routing, and switching.

***Telnet***

An application for remote terminal connection service. Using Telnet, a terminal can interact with any host on a network to which it is not directly connected. Telnet is accessed through the terminal's remote login window.

***TFTP***

Trivial File Transfer Protocol. One of the ways to transfer files between machines connected to an Ethernet network.

***Transceiver***

A device that connects devices to a Thick Ethernet network. A transceiver contains anti-collision firmware. It is needed on a Thick Ethernet network because of the volume of data on such a network.

***Thick Ethernet***

A network using thick coaxial cable.

***Thin Ethernet***

A network using thin coaxial cable.

***User Datagram Protocol (UDP)***

A simple datagram protocol layered above the Internet protocol.

# INDEX

## A

*Add Printer*, 58,59  
*ASCII*, 10, 65, 66, 68, 70, 93  
*attributes*, 6, 10, 24, 26, 30, 81  
*Authentication*, 6, 12, 22, 26, 27, 30, 47, 49, 87  
*AutoMount*, 20, 22, 23

## B

*Binary*, 65, 66, 68, 70, 93, 97  
*BROWSE*, 6, 7, 12, 15, 21, 22, 40, 49, 58, 59  
*Buffer Size*, 6, 10, 24, 25, 30, 40, 89

## C

*cache*, 6, 9, 25  
*Cache Off*, 9, 25  
*Color Mapping*, 81

## D

*default user*, 7, 8, 12, 13  
*Disable NFS 3.0*, 10, 25  
*Domain Name Server*, 36, 46  
*DOS to UNIX File Conversion*, 25, 40

## F

*File Attribute*, 6, 10, 11, 24, 26, 30  
*File Format Convert*, 28  
*File locking*, 6, 10, 25, 85  
*File Permission*, 38  
*FTP*, 20, 45, 61-70, 98  
*FTP Client*, 45, 65-70  
*Troubleshooting*, 70  
*FTP Server*, 61, 62, 63, 65, 66, 70

**G**

*GID*, 6, 7, 12-16, 27, 30, 31, 35-39, 47, 87

**H**

*Host Editor*, 6-8, 12, 20, 21, 27, 30, 33, 45-50, 55, 72, 78, 82  
*Troubleshooting*, 30  
*Host Name*, 7, 33, 45, 46, 54, 55, 66, 72, 82, 84

**I**

*IP address*, 7, 21, 46, 49, 53, 55, 66, 78, 82

**K**

*Keyboard Setup*, 77  
*Keymap*, 79, 80, 81  
*Keypad*, 72, 75

**L**

*Locking*, 6, 10, 25, 26, 30, 31, 40, 41, 74, 76, 85, 86  
*LPD Server*, 51, 52, 54  
*configuration*, 51  
*LPD Troubleshooting*, 54  
*LPR*, 51, 53, 55-59  
*LPR Hosts*, 55, 58  
*LPR Printer*, 55, 57, 58, 59  
*Add*, 59

**M**

*Map Network Drive*, 20  
*mapping*, 12-16, 28, 31, 33-39, 71, 79, 81  
*mount*, 6-8, 11, 12, 19-23, 27, 28, 31, 39-43, 49  
*Mount Wizard*, 11, 20, 21, 27  
*Multiple Session*, 72

**N**

*Network Neighborhood*, 19, 20, 24, 31, 48, 49, 55  
*Network Printers*, 57  
*NFS client*, 1, 5, 8, 19-28, 31, 32, 35, 39, 45, 46, 85-87  
    *Troubleshooting*, 30  
*NFS Drive Option*, 9, 20, 24  
*NFS Drive Property*, 11, 26  
*NFS Printer*, 39, 57-59  
    *Add*, 58  
*NFS Server*, 2, 6-9, 12, 13, 17-20, 24, 26, 27, 30-34, 37-42, 45-49,  
    57, 58, 89, 91  
    *Troubleshooting*, 43  
*NIS Setup*, 46-48  
*NLM File Locking*, 10, 25, 85

**O**

*Options*, 6, 9, 12, 20, 22, 24, 39, 40, 68, 75, 79

**P**

*PCNFSD*, 6, 7, 12, 22, 26, 27, 30, 31, 39, 40, 47, 57, 59, 87, 88  
*Performance Tips*, 40, 89  
*permission*, 8, 11, 12, 22, 26, 30, 34, 37-39, 58, 61, 62, 70, 87, 98  
*Port Mapper*, 40  
*Print Spooling*, 51, 54, 88  
*Printer Setup*, 53, 79  
*protocol*, 5, 25, 31, 65, 87, 93, 96-98

**R**

*R/W List*, 33  
*Read Only*, 10, 26, 33, 86, 97  
*Read/Write*, 11, 24, 26, 33, 34, 37, 38, 89  
*Reconnect At Logon*, 20, 28  
*Remote Printer*, 51, 53-55, 57  
*RSH*, 83, 84

**S**

*Save Password*, 22  
*SCO System*, 58  
*Security Mapping*, 33, 34, 37, 39  
*server Gateway*, 17, 18  
*sharing*, 1, 7, 12, 17, 85  
*Symbolic Link*, 28

**T**

*Telnet*, 71, 72, 82, 98  
*Terminal*, 9, 71, 773-777, 79, 94, 95, 98  
*Terminal Emulation*, 71  
*Terminal ID*, 74  
*Time-out*, 68

**U**

*UID & GID*, 6, 7, 12-16  
*UNIX Hosts*, 4  
*user*, 5, 7, 10-19, 25, 26, 31-38, 48-51, 62-66, 74, 75, 78-81, 84-89, 94  
*User Denied Keys (UDK)*, 74

**V**

*VT420*, 2, 4, 5, 71-73, 79, 81  
*Troubleshooting*, 82

**W**

*Windows Explorer*, 7, 11, 12, 19, 20, 24, 31, 48, 49  
*Windows Service*, 31, 41