

ESKER *Tun*[®] *Plus*

Tun Net – Network
Resource Access

Tun Plus 2009
Issued May 2008

Copyright © 1989-2008 Esker S.A. All rights reserved.

© 1998-2002 The OpenSSL Project; © 1994-2003 Sun Microsystems, Inc.; © 1996 Wolfgang Platzer (wplatzer@iaik.tu-graz.ac.at); © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved. Tun contains components which are derived in part from OpenSSH software. See the copyright.txt file on the Tun CD for additional copyright notices, conditions of use and disclaimers. Use and duplicate only in accordance with the terms of the Software License Agreement - Tun Products.

North and South American distributions of this manual are printed in the U.S.A. All other distributions are printed in France. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means without the prior written consent of Esker S.A..



Esker S.A., 10 rue des Émeraudes, 69006 Lyon, France
Tel: +33 (0)4.72.83.46.46 ♦ Fax: +33 (0)4.72.83.46.40 ♦ info@esker.fr ♦ www.esker.fr

Esker, Inc., 1212 Deming Way, Suite 350, Madison, WI 53717 USA
Tel: +1.608.828.6000 ♦ Fax: +1.608.828.6001 ♦ info@esker.com ♦ www.esker.com

Esker Australia Pty Ltd. (Lane Cove - NSW) ♦ Tel: +61 (0)2 8596 5100 ♦ info@esker.com.au ♦ www.esker.com.au

Esker GmbH (München) ♦ Tel: +49 (0) 89 700 887 0 ♦ info@esker.de ♦ www.esker.de

Esker Italia SRL (Milano) ♦ Tel: +39 02 57 77 39 1 ♦ info@esker.it ♦ www.esker.it

Esker Ibérica, S.L. (Madrid) ♦ Tel: +34 91 552 9265 ♦ info@esker.es ♦ www.esker.es

Esker UK Ltd. (Derby) ♦ Tel: +44 1332 54 8181 ♦ info@esker.co.uk ♦ www.esker.co.uk

Esker, the Esker logo, Esker Pro, Extending the Reach of Information, Tun, and Tun Emul are trademarks, registered trademarks or service marks of Esker S.A. in the U.S., France and other countries.

The following are trademarks of their respective owners in the United States and other countries: Microsoft, Windows, Back-Office, MS-DOS, XENIX are registered trademarks of Microsoft Corp. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corp. IBM, AS/400, and AIX are registered trademarks of IBM Corp. SCO is a registered trademark of Caldera International, Inc. NetWare is a registered trademark of Novell, Inc. Sun, Sun Microsystems and Java are trademarks of Sun Microsystems, Inc. Oracle is a registered trademark of Oracle Corp. Informix is a registered trademark of Informix Software Inc. Sybase is a registered trademark of Sybase, Inc. Progress is a registered trademark of Progress Software Corp. All other trademarks mentioned are the property of their respective owners.

Table of Contents

Introduction to Tun Net	11
Configuring TCP/IP applications	11
Functionality.....	11
The NIS Browser.....	13
What is NIS?.....	13
Tun products and NIS	13
General NIS Browser information.....	13
Exporting an NIS configuration	14
Importing an NIS configuration	14
Testing the NIS server	14
Introduction to the NIS Browser.....	15
Resources.....	15
Icons	16
User mode.....	16
Accessing the available resources	16
Viewing resource properties.....	16
Using resources	17
Creating shortcuts.....	18
Administrator mode.....	18
Table administration.....	19
Managing resources.....	21
Creating a resource.....	21
Moving a resource.....	21
Copying an Object Paths resource from the Windows Explorer.....	21
Resource properties	22
Modifying resource properties	22
Name syntax	22
Server properties.....	22
Printer properties	23
Network drive properties.....	24
FTP configuration properties.....	25
Tar configuration properties: General tab	25
TFTP file properties: General tab.....	25
Emulation configuration properties: General tab	26
Mail address properties: General tab.....	26
Address book properties: General tab	26
Data source properties: General tab	26
Virtual data source properties : General tab.....	26
URL address properties: General tab	26
Application properties: General tab.....	27
Object path properties: General tab.....	27
Modifying, deleting or restoring a resource	27
Changing resource properties	27
Deleting a resource.....	27
Restoring a resource before compilation.....	28
Saving and restoring an NIS configuration	28
PING	29
Tun PING and NIS	29
Running PING	29

Using the NFS client	31
What is NFS?.....	31
Tun Net and NFS Client.....	31
Tun NFS and NIS	31
Using NFS Client with 32-bit Windows.....	32
Declaring remote file systems in 32-bit Windows	32
Filesystem.....	32
Parameters	33
Communication	34
Security.....	35
Saving changes	35
Mounting NFS file systems in 32-bit Windows	36
Using the NFS configurator.....	36
Using the Windows Explorer	36
Using the Network Neighborhood.....	36
Disconnecting NFS drives	37
NFS drive properties	37
Settings tips	37
Remote NFS file properties	37
General Tun NFS options	38
Caches.....	38
Mapping.....	38
Parameters/Communication	39
Security.....	39
Using the NFS server	41
Using the NFS server in a multi-user environment	41
Configuring the NFS server.....	41
Defining a directory.....	42
Defining users' rights in a multi-user environment	43
Export	43
Running the NFS server.....	43
Mounting an NFS file system from another PC	43
Mounting an NFS file system from UNIX	44
Unmounting a file system from UNIX	44
Statistics	44
Using remote printers	45
Declaring a remote printer in 32-bit Windows	45
Installing printers.....	46
Installing a remote printer in DOS based 32-bit Windows.....	46
Printing in DOS on a printer installed in DOS based 32-bit Windows	46
Sharing PC Printers.....	49
Using the LPD server in a multi-user environment.....	49
Setting up printer sharing.....	50
Error log.....	50
Creating a new configuration	50
Defining users' rights in a multi-user environment	51
Sharing printers	51
Activating public printers	51
Statistics	51
Using public printers directly from PCs	51
FTP in ActiveX version	53

Opening an FTP session	53
FTP connection settings.....	53
General	53
Connection.....	54
Conversions	54
Changing a connection	54
Security gateway.....	55
Display parameters	55
Browsing remote file systems	55
Display server directories and files as icons or lists.....	55
Display source file	55
Filters.....	55
Interactive File transfer.....	56
Type of transfer	57
Other actions.....	57
UNIX commands sent to the server.....	57
Example of UNIX command.....	57
Macros	57
FTP API	58
Encrypting a string	58
Running a macro in EScript	58
FTP profiles	58
Definition.....	58
Creating a new profile	59
Field Descriptor.....	60
Field separators.....	62
Profile examples	63
Profile checking.....	64
File transfer with FTP clients	65
Tun Net and FTP	65
Tun FTP and NIS.....	65
Starting Tun FTP	65
NIS configuration	65
Direct configuration.....	65
Options	66
Connection.....	67
Multiple connections	67
Closing a session	67
Using a firewall	67
Interactive mode	68
Navigation	68
File structure representation	68
Directories first.....	68
Simple transfers.....	68
Transferring several files.....	68
Transfers using “drag and drop”.....	68
Transferring directories	69
Transfers between servers	69
Applying Filters.....	69
File management	69
UNIX commands sent to the server.....	69
Automated file transfer.....	70
Macro example	70
Language description.....	71

Variables.....	71
List of instructions.....	71
Defining Server Profiles.....	73
Directory Lists.....	73
Profile Section.....	73
Field Descriptor.....	73
Field Separators.....	74
Example.....	74
Field Descriptor Modifier.....	74
Field Descriptor Test Mark.....	75
Scan Direction.....	75
Compatibility.....	76
Using the FTP server.....	77
Using the FTP server in a multi-user environment.....	77
FTP server configuration.....	77
Defining a directory.....	78
Defining users' rights in a multi-user environment.....	79
Exporting.....	79
Execution of the FTP server.....	79
Statistics.....	80
Transferring files.....	80
VT320 Terminal Emulation.....	81
Tun VT320 and NIS.....	81
Using Tun VT320.....	81
Multiple connections.....	81
Closing sessions.....	81
Terminal options.....	81
Changing the display.....	81
Screen.....	81
Terminal Font.....	82
Attributes.....	82
Saving your changes.....	82
Emulation options.....	83
Session Options.....	83
Firewall.....	83
Copy Option.....	84
Executing Remote Commands.....	85
Tun RSH and NIS.....	85
Using Tun RSH.....	85
Multiple connections.....	86
Closing sessions.....	86
Command execution.....	86
Command recall.....	86
Result Panel.....	86
Customizing Tun RSH.....	86
Defining a macro in Tun RSH.....	86
Adding commands to a macro.....	87
Macro execution.....	87
Opening Tun RSH in button mode.....	87
Remote Command Server.....	89
Tun Net and RSHD.....	89

Setup	89
Adding a new user	89
Adding a new machine	89
Properties of a machine or user	89
Removing a machine or user	90
Options	90
Examples	90
Remote Backup (32-bit Windows).....	91
Running the application	91
Managing archives	91
Adding an archive.....	91
Modifying an archive	92
Deleting an archive.....	92
Creating a group of files	93
Selecting files	93
File filters.....	93
Saving a file set	94
Backing up files	94
Selecting an existing file set.....	94
Backing up a new file set.....	94
Selecting the backup archive	94
Performing the backup	94
Saving the catalog locally.....	95
Canceling the backup	95
Restoring files	95
Selecting files to restore	95
Selecting the archive.....	95
Performing the restore	95
Canceling the restore	96
Settings	96
Backup mode settings.....	96
Restore settings.....	96
Printing	97
Print Setup	97
Printing	97
WALL and WALLD.....	99
Sending a message	99
Message composition	99
Transmission mode.....	99
Selecting recipients.....	100
Receiving a message.....	100
Answering a message	101
Tun Accessories.....	103
Tun TFTP	103
NIS configuration	103
New configuration.....	103
Read/write.....	103
Security.....	104
TIME.....	104
Configuration.....	104
NIS.....	104
Tun Accessories and NIS.....	105

References.....	107
INDEX.....	107
WADM2.....	108
WALL.....	108
WALLD.....	108
WFTP.....	108
WFTPD.....	109
WLPD.....	109
WMOUNT.....	109
WNFSD.....	110
WNISS.....	110
WPING.....	111
WRSH.....	111
WRSHD.....	112
WSNTP.....	112
WTAR.....	113
WTFTP.....	113
WUMOUNT.....	114
WVT320.....	114
Tun FTP macro commands	117
Index.....	117
aget.....	118
append.....	118
aput.....	118
ascii.....	119
bget.....	119
binary.....	119
bput.....	119
ClearMessage.....	119
debug.....	119
delete, mdelete.....	120
Dos.....	120
drive.....	120
Echo.....	120
Exit.....	120
fcd, parent.....	120
get, mget.....	120
Goto.....	121
Hide & ShowMessage.....	121
host_text.....	121
IfConnected.....	122
IfEqual, IfNoEqual.....	122
IfError, IfNoError.....	122
Label.....	123
lcd.....	123
local.....	123
login.....	123
logoff.....	123
mkdir, rmdir.....	124
put, mput.....	124
option.....	124
Pause.....	124
ReadPasswd, ReadVar.....	124
rename.....	125

Set	125
stat.....	125
text_codes	125
Title.....	125
Index.....	127

Introduction to Tun Net

Tun Net is a software package that lets you access resources in a TCP/IP network:




- NIS - Network Information Service (excluding in the Citrix/Microsoft TSE version of Tun Plus).
- PING - Connection testing.
- NFS client - File sharing (using Microsoft's TCP/IP stack in 32-bit Windows).
- NFS server - File sharing.
- LPR - Printer redirection.
- LPD - Printer sharing.
- FTP client - File transfer. Available in ActiveX version with Tun Plus.
- FTP server - File transfer daemon.
- TELNET VT320 - Terminal emulation.
- RSH/REXEC - Remote command execution.
- RSHD - Remote command server (excluding in the Citrix/Microsoft TSE version of Tun Plus).
- TAR - Remote backup.
- WALL - LAN communication utility.
- TFTP - Trivial file transfer protocol implementation (excluding in the Citrix/Microsoft TSE version of Tun Plus).
- TIME / SNTP - Network time coordination (excluding in the Citrix/Microsoft TSE version of Tun Plus).

Configuring TCP/IP applications








In 32-bit Windows, choose Start > Programs > Esker Tun > Network Resources Access > Configuration, and then choose the program to configure.

Functionality

The table below describes the functionality of the applications you can access from the Configuration option of the Esker Tun, Network Resources Access program group (32-bit Windows).

Administration toolbar	Start menu	Functionality
 Tun NFS	NFS	Defines the working parameters of the NFS client layer. Defines, mounts and unmounts remote NFS file systems.
 Tun LPR	Print	Defines the working parameters for printer redirection.
 Tun FTPD	FTP Server	Defines and exports PC directories which can then be accessed by FTP by other machines on the network.

Network Resource Access

Administration toolbar	Start menu	Functionality
 Tun NFSD	NFS Server	Defines and exports PC directories which can then be accessed by NFS by other machines on the network.
 Tun LPD	Print Server	Defines the working parameters for printer sharing.
 Tun RSHD	Remote Command Server	Configures Tun RSHD (configuration and declaration of authorized machines and users).
 Tun NIS (excluding WinFrame)	NIS	Configures the network resource browser, Tun NIS.
 General Setup	Hosts Table	Lets you complete the host table called by the Tun Plus suite
 Language	N/A	Sets the language used in the Tun suite's user interfaces: menus and program messages.
 Help	N/A	Displays online help and program version number.

When you choose Start > Programs > Esker Tun > Network Resources Access > Configuration > Hosts Table (32-bit Windows), a dialog appears. In this dialog, complete the hosts table called by the Tun Plus applications. The servers in this file (hosts in the \Windows\System directory) are displayed in a listbox.

To complete the table, first enter the hosts file path (you can also select it from the directory tree by clicking Import).

You can add new entries to this table using IP address and machine name. To do that, use Add, Modify, or Delete and fill in the IP address and Name fields, if necessary

The NIS Browser

This module is not available in Tun Plus for Multi-User Windows.

What is NIS?

NIS (Network Information Service) lets network users see available network resources and access them from their PCs. They don't need to worry about the location or the configuration of the resources.

NIS is based on the following architecture: A UNIX server manages the resources, which are stored as tables. Typically, the NIS server isn't an independent entity but works as part of a master/slave architecture: The master server manages a domain, and one or more slave servers duplicate the domain's files. Each client connects to the first NIS server to reply.

NIS Tables	NIS Domain	NIS Servers	NIS Clients
Table W		Master	Client 1
Table X	Domain A		Client 2
Table Y	Domain B		Client 3
Table Z		Slave	Client 4

The NIS server tables are known as “yp” tables (for “Yellow Pages,” the original name of NIS that had to be changed because it was the trademark of British Telecom's phone book).

Tun NIS lets NIS clients access resources from a PC with a “browser”. The browser serves a double purpose:

- It lets PC clients easily access the network resources from a Windows environment. They can view and use the resources without taking into account the type of system used.
- The administrator can use it to manage the resource tables on the remote NIS server.

The NIS browser lets you access remote servers and PCs, use remote printers without having to install the necessary drivers, mount NFS drives, access data files such as mail address books, data sources, and even run remote applications.

The Tun NIS administration of NIS tables consists of creating, modifying and deleting resources, and making them immediately available to the network's users. Since the information is centralized, it only needs to be entered once to provide the users with the most up-to-date configurations.

Tun products and NIS

Tun products can use the NIS for different reasons, depending on their configuration.

If you call the NIS browser from an application, you can only access the resources associated with this application. However, if you run the NIS browser directly from the Windows desktop, you can access all the tables on the NIS server that the administrator has made available.

Only information on the general setup of the system is included in this chapter. For details on the use of applications, please refer to the relevant section in the respective user manuals.

General NIS Browser information

Before you can use the Tun NIS Browser or NIS functionality in Tun applications, you must activate Tun NIS.

Before the NIS Browser can be started, the NIS server must be put into operation.

In 32-bit Windows, choose Start > Programs > Tun Plus > Network Resources Access > Configuration > NIS.

To use the NIS browser directly, or from the Tun applications installed, check Use NIS. The resources declared on the NIS server are then accessible directly from the Tun applications that use them. By default, this is unchecked. If left unchecked, these resources won't be accessible from Tun applications.

If you have an existing NIS configuration (created by the administrator, for example), refer to the section “Importing an NIS configuration”. Otherwise, complete the following fields:

Server tab

- **Server:** Enter the name or IP address of the server. If you enter the server's name, make sure you have a name server that can look up the IP address for the name. If you don't know the name or IP address of the NIS server, enter the address “0.0.0.0” or “255.255.255.255” to scan the network.
- **Domain:** Enter your NIS domain name. An NIS domain is different from an Internet domain. By default, the NIS domain name is “nis-domain”.

Other tabs

The Settings tab contains the following options:

- **Number of retries:** Number of retries to access the NIS server before the attempt is aborted. The default value is 3.
- **Timeout:** Duration in milliseconds between each access attempt. The default value is 1000 ms (1 second).
- **Server Recognition Delay:** As there can be several NIS servers on the network, the NIS browser may have to wait some time while it looks for the server corresponding exactly to the configuration. Enter the time allowed in this field. The default value is 1000 ms (1 second). This means that the result of the search for the NIS server is only returned after one second.

The NIS Commands and UNIX Commands tabs contain settings for the compilation and decompilation of the NIS tables, and also for the default commands and values required to update the tables from the browser. Only change these values if your configuration is not standard. Contact your administrator for this information if you don't know it.

Exporting an NIS configuration

As NIS server administrator, you can save a configuration and make it available to the users. As a local user of the NIS browser, you can save an NIS configuration on your PC. That way, you don't have to redo the same configuration tasks. This is useful if there are several NIS servers on the network.

To do that, click Export when you've finished completing the fields. Save the NIS configuration in a file with the extension “.ncf”. By default, Tun NIS proposes its own installation directory. To make the configuration available to other users, choose a shared directory.

Importing an NIS configuration

If you aren't sure of the configuration settings for Tun NIS (server or NIS domain name), you can import an existing NIS configuration created, for example, by the administrator.

To load an NIS configuration saved on the local machine, click Import in the Tun NIS configuration dialog. Select the NIS configuration file to import (extension “.ncf”) and click Open.

Testing the NIS server

Test the NIS server when you load a configuration to verify the communication between the server and the PC. Click Test. A message appears, describing the state of the NIS server.




Introduction to the NIS Browser


When you've finished configuring Tun NIS, you can start the Browser. Run by clicking NIS browser in the Network Resources Access group. A message appears if you haven't activated NIS correctly.

The NIS browser delivered with Tun is a window with a left pane showing different categories (or tables) of resources, and a right pane showing the contents of each table.

To access the contents of a table, select the table in the left pane of the window.















You can modify the way a table's contents are displayed by choosing the appropriate option in the View menu, or by clicking the relevant button in the NIS browser toolbar:

	Large icons
	Small icons
	List Windows (only under 32-bit Windows)

Tun NIS uses the same user interface for both user (the default) and administrator modes: Only the functionality differs. You can switch from one mode to the other by choosing File > Administrator Mode from the main menu, or by clicking Administrator Mode  in the toolbar. In Administrator Mode, the button is depressed.

Resources

There are fourteen categories of resources, corresponding to fourteen NIS Server tables:

	Servers	Network servers
	Remote printers	Shared network printers
	Network drives	Shared network drives
	FTP configurations	Network FTP servers
	TAR configurations	Backup devices
	TFTP files	Network TFTP servers
	Emulation configurations	Network emulation configurations
	Mail addresses	E-Mail addresses (all types)
	Mail address books	Address books accessible on the network
	Data sources	Network data sources
	Virtual data sources	Network virtual data sources
	URL addresses	URLs selected via the network
	Applications	Applications available through the network
	Object paths	Access to different objects available on the network

A resource has the following characteristics:

- An icon.
- Properties.
- Associated applications.

Icons

As the NIS Browser uses a large number of icons, they are not all shown here. Remember, however, that each type of resource in each table has its own icon for easy identification. Additionally, a green spot indicates a device such as a drive or a printer that is connected to the user's PC. A grayed icon represents devices that aren't connected.

User mode

In user mode, you can:

- View the list of available resources on the network and their properties.
- Use these resources through the applications associated with them.
- Create shortcuts for resources so you can access them directly from the Windows desktop.

Accessing the available resources

You can display the list of resources accessible on the network by type. Not all the resource types, however, may be visible:


- Administrator level: The administrator can choose to make some resource types available to users, but not others.
- User level: The user can choose only the resources he wants to see from the visible resources. This reduces the contents of the NIS window, making it less cluttered.
- Application level: The applications that use the NIS Browser can only access the resources that are relevant to them. For example, the emulation application lets you access emulation configurations (Emulation Configurations resource type), but not other resources.

To select the resource types displayed by the NIS Browser, choose View > Resource Display from the main menu.

Check or uncheck boxes to select individual resources. Click Select all to select all resources. Click Clear all to clear all resources. Click OK to finish selection. You can then access the properties of the resources.

Viewing resource properties

To access the resource properties dialog box (to view them in user mode, or modify them in administrator mode), select the resource, then do one of the following:

- Click Resource Properties  in the NIS Browser toolbar.
- Choose Properties from the context menu for the selected resource.
- Choose Resource > Properties from the main menu.

The dialog box that appears contains two, three or four tabs, depending on the resource you selected.

The General tab always contains the following items:

- The resource icon and name.
- A comment field for the resource. This comment appears as a tooltip when the mouse pointer is positioned on the resource icon in the browser window (32-bit Windows only). The resource, for example, can be a server name or IP address, or the name of the LPD server for a remote printer).

The Advanced tab, if there is one, contains the parameters for an advanced configuration. The Options tab can be used to include additional configuration parameters.

The other parameters on these tabs vary from one resource to another. They're described in detail in the section on NIS table administration.

Using resources

One or more applications are associated with each resource. The applications vary from single programs (for example, a 3270 emulator) to a series of operations (such as installing a printer). The applications also vary according to the resource type and the individual characteristics of the resource.

To run an application, select the resource and display its context menu. The list of applications associated with the resource appears in the top section of the menu. The default application is shown in bold print. This application is run if you double-click the resource icon. You can also choose Resource from the main menu to access these applications.

When you run an application from the NIS Browser, you're actually executing the program installed on your PC. If the program isn't installed, the application can't be run. This is true for all the resources except the Applications resource which runs an application located anywhere on the network. In this case, you can use remote applications on your PC.

The following table shows the applications associated with each resource type, although not every resource uses them. The application in bold print is the default application that's executed when you double-click the resource icon.

See the relevant chapters in the Tun SQL and Tun EMUL manuals for details of the applications related to databases and terminal emulation.

Servers	Open Ping Emulators (VT 320, Tun Emul, 3270,5250) Time/SNTP Open DB Show
Remote Printers	Install Uninstall
Network Drives	Connect Disconnect
FTP Configurations	Open FTP
TAR Configurations	Open TAR
TFTP Files	Retrieve
Emulation Configurations	Start the Emulator
Mail Addresses	Open Mail
Mail Address Book	-
Data Sources	Install Datasource Use Data Source
Virtual data sources	Install Datasource
URL Addresses	Open the Internet Browser
Applications	Run
Object Paths	Open Copy as

Creating shortcuts

You can create shortcuts to resources: This feature lets you use your favorite resources straight from the Windows desktop or Program Manager without opening the NIS Browser. The resource can be a server you connect to for emulation, a remote archive you frequently access for backups, or even a URL resource that runs your Internet browser. You simply click the shortcut icon.

To create a shortcut, select the resource, and then choose Create a shortcut from the context menu or the Resource menu.

You can also drag and drop a shortcut from the NIS Browser to the 32-bit Windows.

For Remote printer and Network drive resources, you can create two shortcuts at the same time by holding down the Ctrl key while you drag and drop the resources. The first shortcut installs a remote printer or mounts a network drive and the second uninstalls the printer or unmounts the drive.

Administrator mode

This section completes the first stage of Tun NIS configuration begun in the section “General NIS Browser Information”. The following assumes that the administrator has successfully completed the initial configuration steps before continuing.

If you haven't already displayed the Tun NIS configuration dialog, do the following:

- In 32-bit Windows, choose Start > Programs > Esker Tun > Network Resources Access > Configuration > NIS.

Note:

You can access this dialog box from the NIS browser in Administrator mode.

Server tab

Check Use NIS, and complete the Server and Domain fields, as described in “General NIS Browser Information,” above. If you haven't done this, please refer to that section before continuing. The other parameters on the Server tab are as follows:

- Administrator: Is the administrator's login for accessing the NIS server to maintain the tables.
- Path to temporary files: These two fields contain the name of the working directory on the NIS server in which the different files created are placed, and the name of the working directory on the administrator's PC. You may change the default values if necessary.
- Local Mail Address: An e-mail address is created for access to the anonymous FTP accounts (the address replaces the password for anonymous access).
- Internet Browser Path: The path to your Internet browser (for example: C:\Program Files\Internet Explorer\Iexplore.exe).

Other tabs

The Settings tab contains the following options:

- Number of retries: Number of retries to access the NIS server before the attempt is aborted. The default value is 3.
- Timeout: Duration in milliseconds between each access attempt. The default value is 1000 ms (1 second).
- Server Recognition Delay: As there can be several NIS servers on the network, the NIS browser may have to wait some time while it looks for the server corresponding exactly to the configuration. Enter the time allowed in this field. The default value is 1000 ms (1 second). This means that the result of the search for the NIS server is only returned after one second.

The NIS commands and UNIX commands tabs contain settings for the compilation and decompilation of the NIS tables, and also for the default commands and values required to update the tables from the browser.

The default values are those for a SCO server. Only change these values if your configuration isn't standard or you're using a different type of server. Refer to the documentation for your NIS server if you need to change these fields.

Testing the NIS server

As mentioned in “General NIS Browser information,” you're advised to test the NIS server to verify PC-server communication. To do that, click Test. Refer to “General NIS Browser information” for details on the messages displayed.

Exporting an NIS configuration

As mentioned above, in “General NIS Browser information,” you can save an NIS configuration to make it available to other users. Refer to that section for instructions on exporting NIS configurations.

Validating a configuration

When you've entered the settings you want, click OK to save the changes. To exit the configuration dialog box without saving the changes, click Cancel.

NIS Server stoppage

If the NIS server goes down for some reason, you must use the Tun NIS configuration tool to verify that it starts up correctly. Run Tun NIS (Setup) (from the Start menu in 32-bit Windows) and click the Test button. You'll see a message saying if the server is running or not.

Table administration

Administrator mode lets you access the NIS server tables with a password. Tables and resources in the tables are updated on the local machine as follows:

- The selected table is automatically locked: The administrator makes his changes to the table while users use the version on the server.
- After modification, the table is unlocked: Users can then use the latest version, updated by the administrator.

An administrator can't access a table that another administrator is currently modifying. Different administrators, however, can update different tables, simultaneously.

When a resource is being changed, the whole table is under the administrator's control and can't be modified by another administrator.

To switch to administrator mode, click Administrator Mode in the NIS Browser toolbar, or choose File > Administrator Mode from the general menu.

The user name is the same as the name used for the configuration of Tun NIS. The default is the login ID root. Be careful if you changed this when configuring Tun NIS. Enter the password for this user name (as specified in the NIS server settings), and click OK.

Restoring the sample table

When Tun NIS is first used, the administrator can load the sample table supplied by Esker. To do this, enter administrator mode, choose File > Restore NIS Tables from the main menu, and then select services.nis.

Administrator mode icons

The screen display doesn't change in administrator mode, except that the icons are modified slightly to show the status of the resources. When administrator mode starts, all the resources are present and compiled in the table. They have the same icons as in user mode, only with an added green check mark:



Indicates a server

Table and resource operations

For each table in the database, the administrator can:

- Create new directories or change the existing directory hierarchy.
- Create a new resource.
- Change resource properties.
- Delete a resource.
- Restore a deleted resource before recompilation of the table.

The permissions vary depending on the login ID you use to connect to the NIS server. If you use the super administrator login ID, you have full permissions.

After modifying one or more resources, the administrator can compile the relevant table.

Finally, the administrator can save a copy of the NIS tables to file on the local machine; he can later compile these tables if he wants.

These administrative operations are described in the following sections.


Compiling a table

After carrying out modifications, the administrator must update the NIS table on the server. This means compiling the table.

To compile a table, do one of the following:

- Click Compile NIS Table in the NIS Browser toolbar.
- Choose File > Compile Resources from the main menu.
- Choose another table.

The updated version of the table is available to other users.

Note that if you change from one table to another in administrator mode, the first table is compiled if you made changes to it. If you only want to compile at your express demand (using one of the methods described above), you must click Automatic Compilation Off  in the NIS Browser toolbar.

Note that simply quitting administrator mode or exiting from the browser recompiles the table, that is, the changes are saved.

Choosing NIS Browser tables

The administrator can choose the tables he wants to make available to NIS Browser users. This could be useful, for example, if a table hasn't been updated and the administrator doesn't want to make it publicly available.

To choose the tables click View > Resource Display to select the tables to display on screen.

The only difference from user mode is that Export is active. The administrator uses this button to impose his choice of displayed resources on the system's users. When the button is pressed, a special NIS server table (the View table) is modified.

Example:

The administrator doesn't want to display the list of applications available from the NIS server. He clears the Applications check box, then clicks the Export button to apply these settings to the NIS server's users. The users can now access all the resource lists except the applications list.


The other functions in this dialog box are the same as for user mode. Thus, to avoid viewing a particular type of resource, he unchecks the resource and clicks OK.

Managing resources

A grayed icon represents a new resource.


Creating a resource

To create a new resource, select the table for the type of resource in question, then do one of the following:

- Click New Resource  in the toolbar of the NIS Browser.
- Choose New from the Resource menu.
- Right-click anywhere in the right pane of the NIS Browser window (with no resource selected), then choose New from the context menu.

A dialog appears displaying the properties for the resource type.

You can also copy an existing resource to the same directory. You can use its properties to configure the new resource. Do this to create similar resources with minor differences. Select the initial resource and do one of the following:

- Click Copy  in the NIS Browser toolbar.
- Choose Copy from the selected resource's context menu.
- Choose Resource > Copy from the main menu.

The properties dialog of the initial resource appears. Refer to the instructions below to change the resource's properties. The instructions vary according to the selected resource type.

Moving a resource

To move a resource to a different part of the directory hierarchy, select a resource and drag and drop it to the target directory (the target directory can be the directory root, that is, the resource class level itself).

Copying an Object Paths resource from the Windows Explorer


You can drag and drop Object Paths type resources straight from the Windows Explorer: Select the object to copy in the Windows Explorer (for example, a bitmap image) and drag and drop it to the right pane (list view) of the NIS Browser. The Object Paths resource class in the left pane must be selected.

Choose Copy files to if to specify a particular target directory. Otherwise the files are copied by default to the Object Paths class of the NIS Server.

A tabbed dialog appears: You can change the object's properties on the Properties tab, if necessary.

Resource properties

As administrator, you can view a resource's properties without modifying them. To do this, select a resource and do one of the following:

- Click Resource Properties  in the NIS Browser toolbar.
- Choose Resource > Properties from the main menu.
- Choose Properties from the selected resource's context menu.


Modifying resource properties

A modified resource displays without a green check mark, and its icon appears in user mode:



Indicates a server whose properties have been modified but that hasn't been compiled in the NIS table yet.

To modify a resource's properties, select the resource and do one of the following:

- Double-click it.
- Click Modify Resource  in the NIS Browser toolbar.
- Choose Resource > Modify from the main menu.
- Choose Modify from the selected resource's context menu.

Name syntax

In 32-bit Windows, you're allowed to use the backslash character (“\”) in the name of a resource, but you then can't create a shortcut to the resource.

As a general rule, avoid using backslashes, parentheses and commas in resource names.

In all Windows versions, the file paths to files and applications for the “Emulation Configurations,” “Address Books,” “Applications,” and “Object Paths” resource types are as follows:

c:\...\...	local file (used for a file on the local machine)
\\server\path\file	Workgroups file (the PC server must remain switched on to allow access to the resource)
nfs://server/path/file	file accessible with Tun NFS
tftp://server/path/file	file accessible with Tun TFTP (the path must be authorized by TFTP)
nis:resource name	reference to an NIS “Object Paths” resource type that contains the path of the file or application

The syntax used for URL addresses is as follows:

type://server/path/

You must replace type by *http*, *ftp* or any other protocol supported by your Internet browser.

Note:

The name of a printer resource mustn't be longer than 30 characters.

Server properties

General tab

- Enter the name of the server (as it will appear in the NIS Browser) in the field beside the server icon. Respect the

authorized formats.

- Enter an optional comment: This comment appears as a tooltip when the mouse pointer is placed on the resource icon.
- Enter the name or IP address of the server. If you enter the server's name, make sure you're using a DNS (name server). The DNS maps the name to the IP address (IP address resolution).
- Select the server type: telnetd, 3270 Site, 5250 Site or PC. If your server isn't one of these types, leave this section clear.

Advanced tab

Use this tab to declare the host's attributes, that is, the servers and services installed. You can then change the settings depending on the host configuration. With the list of servers and services, you can:

- Add a server or service. Click Add.
- View the settings of a server or service in the list. To do that, click the server or service to select it (but not the check box), and click View.
- Change a server's or service's settings. To do that, click the server or service to select it (but don't click the check box), and click Modify.
- Delete one or more servers or services from the list. To do that, click the server(s) or service(s) to select it or them (but don't select or clear the check box or boxes), and then click Delete.
- Activate or deactivate a server or service. Select or clear the check box in front of the server or service.

When you add a server or service, or view or modify a server's or service's settings, a dialog box appears (with the fields grayed or not depending on the item selected).

If you're adding a server or service or modifying the settings, you can modify these fields:

- The name of the server or service: This name appears in the preceding list (the field beside the icon).
- The key you assign to the server or service.
- The port number attributed to the server or service.
- A comment.

Use the Options tab to complete the settings.

Printer properties

General tab

- Enter the printer name as it will appear in the NIS Browser. Respect the authorized formats. The name of a printer resource mustn't be longer than 30 characters.
- Enter an optional comment: The comment appears as a tooltip when the mouse pointer is placed over the resource icon.
- Choose the type of printer: "LPR" for a printer redirected with Tun LPR, or else Workgroups/Novell.
- Enter the server name and also the printer's shared name.
- For an LPR printer, select the protocol the TCP connection uses when printing. Enter, if necessary, the UNIX print command (for the RSH and REXEC protocols) and the UNIX user name that's used to start the print job. For more information, see "Printer Redirection".

Advanced tab

The parameters on the Advanced tab are the same as those on the printer's test page. You obtain a test page by accessing the printer properties and printing the printer's test page.

To create a new Remote Printers resource type, first install the printer on the administrator's PC.

To install the printer in 32-bit Windows, choose Start > Settings > Printers. Double-click Add Printer and follow the instructions given by the Add Printer wizard.

When you've entered the printer settings, go back to the NIS Browser. Display the Remote Printers dialog for the resource to create or modify. Click Local printer on the Advanced tab.

Select the local printer you want.

Set the file location option:

- Don't copy associated files: The files associated with the printer aren't copied to the NIS server. The File path field on the Advanced tab remains empty. You can fill it out manually later, if necessary.
- Copy associated files to NIS server: The printer configuration files are copied to the NIS server.
- Copy associated files to: Copies the associated files to a drive or directory. This can be a directory on a Workgroups machine. In that case, users who install the printer from the NIS must be able to access the machine.

Click OK. The operation is longer if you chose to copy the associated files. Otherwise, the printer settings are immediately copied to the Advanced tab:

If the printer you create on the NIS server isn't configured locally on the administrator's machine, you must fill out the fields on the Advanced tab manually. To find the information required, print the printer's test page from the machine it's connected to.

To do this from a 32-bit Windows, open the properties dialog for the printer (double-click My Computer on the desktop and then double-click Printers). Choose Properties > Print Test Page.

Use the information on the Printer test page to complete the fields on the Advanced tab:

Advanced Tab Fields	Test Page Information
Driver Name	Printer model
Driver number	Driver version (converted to binary)
Driver	Driver name
Date file	Data file
Configuration file	Config
Dependent files	Files used by this driver
Data type	Data format

You need only supply the path to the drivers directory that was created when you installed the server on the UNIX host (see "Tun NIS setup"). Separate each file with a comma without using spaces. The names must be written in capitals.

The other fields are for the help file (same as the driver file name, only with the extension ".hlp"), and the monitor.

Network drive properties

General tab

- Enter the name of the network drive as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the icon's tooltip.
- Choose the type of network drive: Nfs for a drive that's accessible with Tun NFS or Workgroups/Novell.

- Enter the name of the relevant NFS server, the UNIX directory path and the user name used to access the remote drive.

Advanced tab

This tab only appears for NFS type network drives. It contains the NFS settings for the selected network drive. See the chapter “NFS Client” to enter the settings. The settings are:

- Read size: Maximum size in bytes of a read request to the NFS network drive. It's recommended to check Auto. If you don't, you can enter your own value in the field beside the check box once you've cleared it.
- Write size: Maximum size in bytes of a read request to the NFS network drive. It's recommended to check Auto. If you don't, you can enter your own value in the field beside the check box after clearing it.
- Timeout: The request is resent after this time (in milliseconds) (if the NFS server hasn't replied).
- Multiple retries: Number of times the request is sent if the server's not responding.

FTP configuration properties

General tab

- Enter the name of the FTP configuration as it will appear in the NIS browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the resource icon's tooltip.
- Enter the name of the FTP server to use for the FTP connection. Check Anonymous for anonymous FTP access.
- Enter the type of server used and the type of data on the server.

For more information on the last two points, see the chapter on FTP Client, especially the section on server profiles.

Advanced tab

- Enter the name of the subdirectory that acts as the access directory. This stops the user from making unnecessary directory changes to the server. Select the Stay under home directory check box to stop the user going up the directory structure on the server.
- Choose ASCII or Binary to set the default type of data transfer for this connection. If you choose ASCII, specify the data type exchanged with the UNIX system in the Transfer data type area.
- Change the service port number, if necessary, in the Service field.
- Change the default data size, if necessary: The default is 8.
- Clear the direct and passive mode check boxes.

Tar configuration properties: General tab

- Enter the name of the Tar configuration as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears in the resource icon's tooltip.
- Enter the name or the IP address of the server that the backup device is installed on, and the user name used for the backup.
- Enter the type of backup device you want, and the protocol to be used for the connection.

TFTP file properties: General tab

- Enter the name of the TFTP file as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears in the resource icon's tooltip.

- Enter the name of the remote server.
- Enter the names of the source and destination files.

Click Copy local file and choose the file to send by TFTP to perform the transfer.

Emulation configuration properties: General tab

- Enter the name of the emulation configuration as to see it in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the tooltip for the icon.
- Select the type of emulation required, and the configuration file to use, if there is one. Respect the authorized formats.

Mail address properties: General tab

- Enter the name of the e-mail address as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the tooltip for the resource icon.
- Select the type of address you want, and enter the e-mail address of the mailbox used.

Address book properties: General tab

- Enter the name of the address book as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the tooltip for the resource icon.
- Enter the name of the file containing the address book. Respect the authorized formats.

Data source properties: General tab

- Enter the name of the data source as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the resource icon's tooltip.
- Enter the name of the driver for the data source.
- Enter the name of the server containing the data base, and the service name used (that is, the server process linked to the DBMS with the database to use - tunodbc.ora, for example).
- Enter the name of the data source and (optionally) a description.
- Enter the name of the user authorized to access the data source, and the associated password.

For more information on these four points and the settings on the other tabs, see the Tun SQL manual.

Virtual data source properties : General tab

- Enter the name of the virtual data source as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): The comment appears as the resource icon's tooltip.
- Enter the name of the real data source that the virtual data source is based on.
- Enter the name given to the virtual data source when it was created.
- Select the .DBR file check box, if there's a .DBR file, and enter the full path to this file.

URL address properties: General tab

- Enter the name of the URL as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the resource icon's tooltip.
- Enter the complete URL address. Respect the authorized formats.

Application properties: General tab

- Enter the name of the application as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the resource icon's tooltip.
- Choose the type of application you want (Tun, Windows, or Other).
- Enter the program's file path. Respect the authorized formats.

Object path properties: General tab

- Enter the name of the object as it will appear in the NIS Browser. Respect the authorized formats.
- Enter a comment (optional): This comment appears as the resource icon's tooltip.
- Enter the object's path. Respect the authorized formats.
- Enter the type of object (optional).

Modifying, deleting or restoring a resource


Changing resource properties

A resource that's been modified is displayed without a green check mark, and its icon appears in user mode:



Indicates a server whose properties have been modified but that hasn't been compiled in the NIS table yet.

To modify the properties of a resource, double-click its icon or else select the icon and do one of the following:

- Click Modify Resource  in the NIS Browser's toolbar.
- Choose Modify from the resource's context menu.
- Choose Resource > Modify from the main menu.

The resource properties box is displayed. See “Creating a new resource,” and modify the resource properties.


Deleting a resource

A resource that's to be deleted when the table's compiled is represented by the same icon as in administrator mode, except it's marked with a red cross:



Indicates a server that will be deleted when the table's recompiled.


To delete a resource, first select it, and then do one of the following:

- Click Delete/Restore Resource  in the NIS Browser toolbar.
- Press Del on the keyboard.
- Choose Delete/Restore from the resource's context menu.
- Choose Resource™Delete/Restore from the main menu.

The resource properties dialog appears. Check the contents of the resource, then click Delete to confirm. The resource is deleted from the table when the administrator compiles it.

Restoring a resource before compilation

A resource deleted from the table (with a red cross on its icon) is only really deleted after recompilation of the table. You can restore the resource as long as the table hasn't been recompiled.

To restore a resource marked for deletion, follow the same steps as for the delete, but use Restore. The Delete/Restore Resource button now looks like this: 

Saving and restoring an NIS configuration

The administrator can save a backup NIS server configuration locally. Use this to restore a previous configuration or to manually modify a configuration. For this, you need a clear understanding of the structure of the NIS tables and their contents.

You can save an NIS configuration partially or totally: The save is partial if only the NIS server resource tables are saved, and total if the entire server, including the resource tables, is updated.

To save a configuration, choose File™Save NIS tables from the main menu.

- Choose the directory to save the configuration in.
- Choose the type of save, partial or total. By default, the save is partial.
- Enter the file name with the extension “.nis”.
- Click Save.

To read or change a configuration file, open it with Wordpad or a similar application.

Example of a “.nis” file:

```

---NIS:Path (esker.fr) --- OK -----
3270_16 1|1|||bmp|C:\EMULSYNC\3270_16.bmp
as400 1|1|||pan|tftp://194.51.34.1/tftpboot/yp/files/as400.pan

---NIS:Appli (esker.fr) --- OK -----
Notepad 1|1|||999|\pcmechin\temp\notepad.exe

---NIS:Url (esker.fr) --- OK -----
Microsoft\Server 1|1|||http://www.msn.com
URL\Esker 1|1|||http://www.esker.fr

---NIS:proto.nam (esker.fr) --- OK -----
hello hello63HELLO
HELLO hello63HELLO
ospf ospf89OSPF
    
```

In this example there are four tables from the domain esker.fr, namely, Path, Appli, Url, proto.nam. Three of the tables are resource tables.

The file syntax is always the same: The name of the table is preceded by “NIS” and followed by the domain name. Then, in sequence, come the table’s resources with the name of the resource and the related fields separated by vertical lines (the pipe character “|”). No spaces are used at the beginnings and ends of lines.

To restore a configuration saved on the local machine, choose File™Restore NIS Tables from the main menu, and select the configuration file you want.

Click Yes to replace the current configuration with the restored configuration. The modifications are permanent only when the table is recompiled. Remember that if you restore a saved configuration, you won't be able to return to the previous one unless you saved it to file.

PING

Tun PING is a TCP/IP application that tests links between PCs and other machines on the network. It works on the principal of emitting packets over a network to a server. If the server is a viable link, it returns the packet (echo).

Tun PING and NIS

Tun PING is enhanced by access to the NIS server via the NIS browser included with Tun applications. This feature can be used to view the servers on the network that are defined on the NIS server. The network administrator must, of course, have previously configured the NIS server and defined the Servers resource table using the NIS Browser. For a full description of the NIS Browser, see the chapter “The NIS Browser.”

Running PING

In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > TCP-IP Utilities > Ping.

Address or Host Name

Enter the name or the IP address of the server to ping, or select the server from the drop-down list. This list contains the servers declared in the hosts file and on the NIS server (NIS server resources have yellow icons).

Time interval

Specify the time interval between consecutive packets (in seconds).

Timeout

Specify the time (in seconds) before a packet is considered to be lost.

Length of data

Specify the length of the data packet to send. This can change depending on the routers passed to reach the server.

Options

The first two options in the Options menu let you specify the packet type to use to test the connection:

- ICMP Echo: This option is only valid with the Tun TCP/IP Kernel. If you're using a different kernel, use the ping application supplied with that kernel.
- UDP Echo: This option is only valid if the specified server uses this mode. To test the connection with another Windows PC, you should use ICMP.

Choose Beep to hear a beep with each echo. This function is useful if you're trying to reconnect a PC to a server and you're not continually looking at the screen.

Choose Tun Admin to run the administration program Tun ADMIN+ (see the section “Using the Tun Net administrator” in the chapter “Introduction to Tun Net”).

Choose Tun NIS Browser to open the NIS browser and access the NIS servers and other network resources with a mouse click.

Use Language to choose the interface language used.

Start

When you've set the test parameters, click Start to run the test. The Statistics section shows the results of the test: The number of packets sent, the number of packets received, the percentage of emitted packets returned, and the average round-trip time (in milliseconds).

Stop

Click Stop to stop the connection test.

Using the NFS client

What is NFS?

Network File System (NFS) is a transparent mechanism that's independent of operating systems: It lets PCs mount remote directories over a network, and treat them as if they were ordinary local directories on the PC. With Tun NFS, the server is “stateless,” and doesn't maintain a specific context for each client.

For example, when a client opens a remote file, the *open request* isn't transmitted to the server. The name, position, and length of the zone to read is only transmitted when the client wants to read part of the file. The server opens the file, positions itself at the zone it wants to read, performs the read, then returns the results and closes the file. After this transaction, the server “forgets” the client.

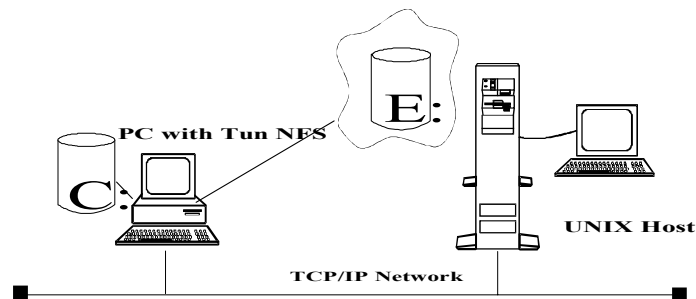
Clients and servers aren't linked by a permanent connection. If the client reboots, there are no resources or residual processes left on the server. If the server reboots, the client only loses the use of its remote volume while the server is being restarted.

Tun Net supports file and/or record locking. Windows file names are represented on UNIX hosts without problems.

Tun Net and NFS Client

Tun Net implements the PC-NFS client protocol, with the exception of printer management (this is obtained using a different procedure). The Tun Net NFS function uses the UDP or TCP layers, depending on the NFS server configuration.

Tun Net lets PCs mount remote directories with virtual DOS/Windows drive letters (D:, E:,..., Z:), and treat them as local DOS/Windows drives.



With Tun Net, a UNIX host becomes a Windows file server, providing a common area for storing files and executing Windows programs in a multi-user environment.

Tun NFS and NIS

Tun NFS is enhanced by access to the NIS server with the NIS Browser included with Tun applications. This functionality lets you view the NFS network drives that are defined on the NIS server. The administrator must have previously configured the NIS server and defined the Network Drives resource table using the NIS browser. See the chapter “The NIS Browser” for comprehensive instructions on that application's use.

Using NFS Client with 32-bit Windows

In 32-bit Windows, Tun NFS is governed by a VxD (Virtual Device Driver), which only works with the TCP/IP kernel supplied with the system (Microsoft's). The VxD implementation enables any Windows or MS-DOS application to access files on the UNIX server.

Note:

Tun NFS for 32-bit Windows only works with the TCP/IP kernel supplied by Microsoft with 32-bit Windows.

Declaring remote file systems in 32-bit Windows

Select Start > Programs > Esker Tun > Network Resources Access > Configuration > NFS. Or, run the NFS configurator from Network Neighborhood:

- Click Network Neighborhood in the Windows Explorer.
- Select Entire Network from the list of workstations that have exported a resource.
- If Tun NFS is correctly installed, a list is displayed that includes the entry Tun NFS.
- Choose Administration NFS from the context menu of the entry Tun NFS.

The dialog shows previously defined and currently connected drives. If no file systems have been declared, the lists in the dialog box are empty. To use a previously defined NFS configuration, click NIS. In the displayed window, double-click the resource to activate.

Note:

Only remote NFS network drives are shown in this screen.

To define a new file system, click New. To modify or simply view the settings of an existing configuration, click Setup.

Filesystem

Name

Enter the volume name used by the Windows Explorer. This is the file system name that users see. The name itself is of little importance: It's simply for identification purposes.

Remote host

Enter the name or IP address of the UNIX host where the NFS file system is located (only enter a name if your network uses a DNS). You can select a host declared in the host table (hosttab) or on the NIS server by clicking the down arrow next to the field. NIS resources are shown in yellow.

Remote path

Enter the absolute directory path of the remote file system to mount. The remote file system must be exported (that is, listed in `/etc/exports`) by the server before it can be mounted.

To view the NFS file systems available on the host, click the arrow next to the field. This queries the host and displays the paths of the currently exported file systems.

When the file system is mounted, the directory you assign appears as the root directory of the DOS/Windows virtual drive.

User name

Enter the name of a valid user account in this field. When an NFS mount is started, the user is prompted to enter a password. If you enter the pseudo-user nobody, no password is required, but access rights are usually reduced to a strict minimum.

Note:

It's generally recommended not to use "root" to log in, as Tun NFS doesn't recognize the user root (considered as nobody if accepted at all).

For a user name other than nobody, pcnfsd must be running on the host.

Default local drive

Assigns the drive letter used by Windows for the mounted file system, for example, E:.

Make sure that the DOS "lastdrive" command in the config.sys file on the PC lets you assign the drive letters you want. For example, if to assign virtual drives up to M:, add the following line to config.sys:

```
lastdrive=m
```

Reconnect at logon

Check this to remount the file system automatically each time Windows runs. Otherwise, you must mount the file system manually each time Windows is started.

Parameters

Transport protocol

The NFS server can be accessed using the TCP or UDP transport layer protocols, depending on the server's environment.

There are three options:

- Full TCP: The NFS client tries to use TCP to access the lockd, pcnfsd, portmapd and mountd servers. If one of the servers doesn't support TCP, the NFS client tries to use UDP for that server.
- TCP or UDP: The NFS client tries to use TCP to access the nfsd server and UDP for the others. As for the first option, if the nfsd server doesn't support TCP, the NFS client tries to use UDP.
- UDP: No TCP access is attempted: UDP is used.

NFS version 3 required

If you select this check box, the client tries to connect to the NFS server using NFSD version 3. If the server doesn't use version 3, version 2 is used.

The grayed NFS version/protocol used check box indicates the NFSD version set by the server, and the transport protocol used for the previous NFS access.

Share/Lock

Check this to have the remote file system support file and/or record locking. Most word processing and spreadsheet software require Share/Lock to be active. It is also required for accessing databases.

Symbolic links

Select this to authorize users to view, open and delete symbolic links in UNIX files.

Use lowercase

Check this to send lower case names to the UNIX server.

Use server cache

If you choose version 3 (NFS version 3 required), Use server cache is activated. Check this to have the server use its write cache to store received data. When data has been copied from the client to the server, the server returns control to the client and can then flush its cache. At this point the server performs a write using the data in the cache. Check to enable the write operation.

Created file permissions

Sets the access rights (using UNIX format) for created files.

Communication

Read size

Read size refers to the maximum size, in bytes, of *read requests* to the NFS server. For example, if a Windows program reads a remote file, Tun NFS uses the Read size value to divide the request into as many packets as necessary.

Check Default to use the default size (4096 bytes). Otherwise, Uncheck enter the Read Size number of bytes per packet in the field that appears.

Write size

Write size refers to the maximum size, in bytes, of write requests to the NFS server. If a Windows program makes a write request to a remote file system, the requested data is broken down into as many packets of Write Size bytes as necessary.

Check Default to use the default size (4096 bytes). Otherwise, uncheck and enter the Write Size number of bytes per packet in the field that appears.

Automatic read/write settings

Check this to make the read and write settings the sizes that you chose. The settings are dynamic and temporary: They are discarded on disconnection. New automatic settings are used for the next connection if the check box is still selected.

Search buffer size

Specify the buffer size used for a directory search (dir command). The default value is 4096 bytes.

Timeout

Specifies the period of time in milliseconds after which packets are re-sent to the server if there's no response.

Retry mult.

This sets the number of times a packet is re-sent if there's no response from the server. The default value is 3 times. You shouldn't need to change this value when you first start using the software.

Burst read/write

These fields only apply to Windows NT. They contain the number of packets that can circulate at the same time in read or write mode. The maximum value in both cases is 8. If the value is zero, requests are made asynchronously.

Use lookup cache

The lookup cache stores information on the accessibility of a file with Tun NFS. By selecting this check box, you activate the cache function and accelerate access. The size of the cache and the refresh rate can be set with the Options button in the Tun NFS window. See “General Tun NFS options.”

Use read cache

The read cache is used in two situations:

- Anticipated read: If an application requires data to be read in small packets (or even byte by byte), the Read size packets are stored in the read cache. This reduces server access from the application.
- Recent data access: If an application reads the same data block repeatedly, this data is stored in the read cache. There's then no need to access the server for each read request.

Security

Password

To save the password associated with the User name (on the first tab), check Use specific password and enter the password in the field that's activated (Password). That way, the password isn't requested each time you connect.

Note:

This option is available for every configuration. You can use the same password for every configuration by completing the appropriate field in the Options dialog box (see “General Tun NFS Options”).

Use centralized PCNFSD server

Access to a server by NFS requires a user name and password. Typically, the PCNFSD attributes an identifier to the user (UNIX user and group ID) that's used for the connection. Each PCNFSD server attributes UIDs and GIDs to users each time they connect.

Using a centralized PCNFSD server means one server is responsible for attributing UIDs and GIDs to NFS users. It works as follows: When an NFS connection is requested, the centralized server attributes an identifier to the user. It then connects to the NFS server called by the client using this identifier.

This has the following advantages:

- Once you're connected, the same identifiers (UID/GID) are used for any other connections you make, even connections to a different server.
- If a UNIX server doesn't have PCNFSD (as with earlier systems), it can still be accessed with the UID/GID attributed by the centralized PCNFSD server.

Firewall

Check Connect via PROXY server to secure connections to outside servers. The check box is deactivated if you haven't first configured the proxy server in this or another Tun application. To configure the proxy server (IP address, port number, etc.), click Options in the main Tun NFS dialog. See “General Tun NFS Options” for more details.

Saving changes

To save a configuration, click OK: This also returns you to the initial Tun NFS window. The file systems you' configure are displayed in this window.

Note:

To edit or delete a remote file system configuration, click Setup or Remove.


Mounting NFS file systems in 32-bit Windows

There are several ways to mount configured file systems:

- Use the NFS configurator.
- Use the Windows Explorer.
- Use the Network Neighborhood.

Using the NFS configurator

Select Start >Programs > Esker Tun > Network Resources Access > Configuration > NFS. If you've declared a remote NFS file system, it appears in the top list.

Select a file system from the top list, and click the down arrow () to mount it. If you didn't provide a user name and password when you configured the file system, a dialog appears to request this information.

Click OK. If the password is accepted by the NFS host, the new drive appears to Windows Explorer as if it was a local drive.

Using the Windows Explorer

Once you've declared an NFS file system with Tun ADMIN+, you can mount it directly in Windows Explorer: Choose Tools>Map Network Drive Explorer.

Notes:

A file system can be mounted directly with Windows Explorer even if it hasn't been previously declared using Tun ADMIN+. To perform the mount, enter a character string in the Path field as in the following example:

```
//host/directory
```

where *host* is the name of the NFS server and *directory* the name of the directory to be exported. In this case, the file system is mounted with the default options (Read size, Write size).

The option Map Network Drive establishes the connection using one of the file systems on the machine: for example, Workgroups or NFS. The file systems are examined one after the other, with NFS last. If the directory exists in the Workgroups system, for example, it'll be mounted in Workgroups.

Using the Network Neighborhood

Mounting a file system with the Network Neighborhood is a special case. You don't have to associate the file system with an MS-DOS drive (D:, E:, F:, etc.). In fact, the file system is associated with a pseudo-drive with the name Network Neighborhood. The pseudo-drive is visible to all the Windows applications. The linking of the file system to the Network Neighborhood isn't permanent and Windows doesn't try to reconnect when the machine is booted.

To perform the mount using Network Neighborhood:

1. Open Network Neighborhood.
2. Select Entire Network from the list showing the workstations with exported resources.

3. If Tun NFS has been correctly installed, this operation displays a list, which includes the entry Tun NFS. Select this entry.


A new window appears containing the list of NFS servers installed on the network. Select one of the servers to display the directories exported by that server:

There are two options in the context menu of the directory to mount:

- Connect to network drive via NFS establishes a connection immediately using NFS.
- Map network drive connects one of the file systems on the machine: Workgroups or NFS, for example. The systems are examined one after the other with NFS the last. If the directory exists in the Workgroups system, for example, it'll be mounted in Workgroups.

Disconnecting NFS drives

To disconnect an NFS network drive:

- Use the up arrow () in the Administrator (Tun ADMIN+) dialog.
- Choose Tools > Disconnect Network Drive from the Windows Explorer (in 32-bit Windows).

NFS drive properties

In 32-bit Windows, you can view an NFS drive's properties.

Note:

Some properties are only available if the NFS drive is mounted on your machine.

To do that from Explorer, select the NFS drive and choose File>Properties from the main menu. You can also choose Properties from the NFS drive's context menu. The drive properties are displayed on three tabs: Used and free space, connection parameters (user, password, server, NFS version used, protocol, etc.) and UNIX attributes.

Click Details on the NFS Drive tab to view the connection options (read and write size, cache use, etc.). To obtain connection statistics, click Stats.

If the NFS drive is mounted on your machine, the Tips button is shown. The Tips button lets you fine-tune your connection to optimize performance.

Click Refresh to update the statistics and Reset to use the initial settings (that is, the settings for the current configuration).

Settings tips

To optimize the performance NFS connection:

- Click the NFS drive tab in the NFS drive's properties dialog, and then click Stats.
- Click Tips. The Tips button is only available if the NFS drive is mounted on your machine. Otherwise, you can't do any tuning but only view and refresh the statistics displayed.

Remote NFS file properties

In 32-bit Windows, you can view the attributes of a remote NFS file and change them if you have the necessary access rights.

To do that, select the remote NFS file from the Explorer. Then, choose File > Properties from the main menu. You can also choose Properties from the remote NFS file's context menu.

The UNIX file permissions for each type of user are shown: Read permission (R), write permission (W) and execution permission (X). You can change the permissions by selecting or clearing the check boxes. Whether or not your

choice is validated depends on your own access rights for the remote file (displayed in the You have the rights of field). Click Apply to validate any changes you've made, otherwise click Close.

General Tun NFS options

Click Options in the main Tun NFS screen to set general options for all your NFS configurations, or view the Tun NFS Options dialog. In 32-bit Windows, you can also access the options from the Network Neighborhood.

1. Click Network Neighborhood in the Windows Explorer.
2. Select Entire Network from the list of workstations that have exported a resource.
3. If Tun NFS is correctly installed, a list is displayed that includes the entry Tun NFS.
4. Choose NFS Settings from the context menu of the entry Tun NFS.

Apart from the Timezone offset field, the other fields in this dialog are the same as those on the Caches and Mapping tabs in 32-bit Windows.

Caches

Max locks

Sets the maximum number of file locks that NFS can create.

Lookup cache

In this area you enable and configure the lookup cache. The cache is enabled by default: Clear the Enable lookup cache check box to disable it. Otherwise enter the cache size in bytes (8192 is the recommended value) and the cache refresh rate in bytes (30 through 40 recommended).

Read cache

In this section you enable or disable the read cache and change the number of buffers (6 recommended) and the cache refresh rate (60 s recommended), if necessary.

Use OEM code page

This option is available in DOS-based 32-bit Windows. By default, the check box is selected. This means that the OEM code page is used for writing to files. However, you can use the ANSI code page, depending on your system. In this case, clear the check box. In NT-based Windows, the ANSI code page is always used.

Timezone Offset

In 32-bit Windows, the time zone offset in relation to GMT is handled by Windows.

Mapping

Check Enable file name mapping to have Tun NFS to take into account the differences in file name formats on different operating systems (Windows/UNIX).

Enter the cache size in the Requested cache size field, that is, the size of the map used for the different file names. The current cache size appears in the Current cache size field. As the cache isn't updated automatically, you must flush the cache when the current and requested cache sizes are close (Reset). Use the Refresh button to update the cache's contents.

Note:

On the three remaining tabs of the Options dialog box (Parameters, Communication and Security), the values are default values for subsequent configurations. However, if you change these values in the Setup dialog box, later changes in the Options dialog box won't have any effect.

Example:

Say you selected the Use centralized PCNFSD server for the server zeus in the Options dialog box. You then create a new configuration called "nfs." This configuration uses the centralized PCNFSD server by default. You decide "nfs" will connect to pluto rather than zeus.

If you later change the PCNFSD server to mercury in the Options dialog box, the configuration "nfs" will still use the server defined at configuration level (pluto).

Parameters/Communication

These tabs are the same as those in the Setup dialog. See the subsections "Parameters" and "Communication" in the section "Declaring an NFS file system in 32-bit Windows."

Security

Authentication

The default user name for new configurations is "nobody." You can change this in the Default user field. You can also associate a password with this name in the Password field. That way, the password isn't requested when the server's NFS directories are accessed.

The Use centralized PCNFSD server option is the same as that in the Setup dialog. See the subsection "Security" in the section "Declaring an NFS file system in 32-bit Windows."

As indicated above, this option applies to new NFS configurations.

Firewall

The Connect via PROXY server option makes NFS connections to the outside safe. Click Setup to configure the firewall (IP address, port number, etc.).

In the Firewall Configuration dialog, check Use a Proxy server. Enter the name or IP address of the server. Only enter a name if you use a DNS. You can also choose one from the drop-down list (click the down arrow to the right of the field). The list contains the names of the servers listed in the server table (hoststab) and on the NIS server (NIS resources have yellow icons).

Also enter the SOCKS port number (usually the default value 1080).

To avoid using the firewall for local connections, select Do not use for local addresses.

The firewall configuration can be applied to all the Tun applications: To do that, check Use these settings for all Tun applications. To apply the general configuration to all the Tun applications in use (after using a specific Tun NFS configuration, for example), click Restore general settings.

Using the NFS server

Tun NFSD for Windows is an implementation of a complete V2 and V3 (PC) NFS server protocol (excluding printer management, which is handled differently).

The NFS server option lets a PC export its directories so that another PC can view them as virtual drives (D:, E:, Z:). It also lets a PC export directories so that a UNIX machine can treat them as new virtual file systems.

The NFS server option lets a UNIX machine access the contents of the PC's hard drives: It allows a centralized backup of the network files. A central server can automatically update specific data or executable files on the PC. The NFS server option also enables PCs to share a CD-ROM drive.

Using the NFS server in a multi-user environment

You can connect to the multi-user server from a client PC (or from the server machine itself) in administrator or user mode. The way you use the NFS server depends on the connection mode you use.

In Administrator mode, you can:

- Choose the start mode for the Esker NFSD service, and start and stop this service.
- Define one or more NFSD configurations.
- Define configuration rights for the ordinary user.

In User mode, depending on the rights defined by the administrator, you can do one of the following:

- Define one or more NFSD configurations.
- Only view existing configurations.

To use the NFS server in the multi-user environment, you must start the Esker NFSD service on the multi-user server and configure the NFS service with Tun NFSD.

Configuring the NFS server

To configure the NFS server, you declare one or more directories on the PC so that they're accessible from an NFS client application.

- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources > Configuration > NFS Server.

If the NFSD server isn't already running, a dialog box proposes to start it.

If you're connected to the multi-user server as administrator, an extra check box is available labeled Limited access. This option lets you attribute to users the right to change or only view the NFSD configurations defined by the administrator.

If you're connected to the multi-user server as a user, you can do the following (depending on the access rights the administrator has given you):

- Define NFSD configurations: In this case, follow the instructions below.
- Only view existing configurations: In this case, following a warning message reminding you of your limited access rights, the same dialog box as the one above is displayed except that the Setup button is replaced by Consult.

Note: If there are exported NFS directories, Tun NFSD runs as a background task (if this isn't already the case) when you activate the dialog.

You can also display this dialog by running Tun NFSD and selecting the Setup option in the system menu (select Start > Programs > Esker Tun > Network Resources Access > Local Server Startup > NFS in 32-bit Windows).

You can hide the Tun NFSD icon by checking Hidden Server. This option reduces the number of icons displayed in the Windows environment when the keystrokes Alt-Tab or Ctrl-Tab are used.

Defining a directory

To define a directory to export, click New.

Directory

This field contains the full pathname to the Windows directory that to export (to allow NFS access to).

Export Name

Due to the difference in pathname notation on Windows and UNIX systems (c:\tmp\xxx and /usr/tmp/xxx), the Export Name field lets you rename the exported directory for the UNIX operating system. The new name must comply with the UNIX system standard.

Comments

The Comments field lets you attach a comment, perhaps explaining why the directory is exported.

Read Only

The Read only check box limits access to the exported directory to read only. This is a very useful option for nobody type access. It prevents users logged on from writing unauthorized information to the exported directory.

Unrestricted Read

This check box authorizes nobody type access. That is, a user may access the exported directory by supplying the name nobody as user's name, with no password. In any case, Unrestricted read doesn't authorize him to modify or delete the files in the exported directory.

Clients

Access to the NFS server can be restricted to a certain number of machines. The Clients button lets the user create or modify a list of IP addresses or names of machines that are authorized to access the exported directory. Machines not on the list simply can't log in. If the list is empty, any machine can log in.

Unrestricted Access

This option allows users unrestricted access to clients irrespective of whether their names appear in the Authorized clients list or in the PC-NFS authentication entry fields or not.

Authorized Clients

For a client to be authorized, its host name, IP address or domain name must be indicated in the list of Authorized clients.

Authenticated Users

This option indicates that the user name and password entered when the file system is mounted must correspond to the entries in the PC-NFS authentication section.

Authorized Clients + Authenticated Users

If this option is selected, either of the two preceding situations is acceptable. That is, the user must be either an Authorized client or an Authenticated user to access the file system.

Authenticated Users on Authorized Clients

This option provides the corresponding situation, that is, the user must be both an Authenticated user and logged on to an Authorized client.

Authorized Clients list

Contains the list of authorized clients in the form of an IP address, host name, or domain name. The IP addresses can contain one or more zeros as a mask. For example, 194.51.34.0 gives access to all the clients whose IP address starts with the same first three bytes.

PC-NFS Authentication


Enter the name of the user (and optionally a password) who is to be granted access to the file system. The PC-NFS Authentication protocol isn't generally used by UNIX users.

Defining users' rights in a multi-user environment

In the main Tun NFSD screen, select or clear the Limited Access check box to define users' configuration rights:

- Unchecked, users can declare, modify or delete NFS directories and export them.
- Checked (the default), users can only view the existing NFS directories.

Export

To export a directory, select it from the list of directories in the Tun NFSD window, then click . This directory can now be accessed from a client machine if the NFSD server is running.

Running the NFS server

The directories and files exported by the NFS server are only accessible to another machine if the NFS server is running.


- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > Local Server Startup > NFS.

Note:

The server is running when the program's icon appears in the taskbar.

If you're going to use Tun NFSD regularly, you can copy the Tun NFSD icon to the Windows Startup group.

Mounting an NFS file system from another PC

To mount an exported file system from another PC, you must define a new file system  with the NFS (client) configuration program and mount it using the activation arrow (see the chapter "NFS Client"):

Mounting an NFS file system from UNIX

To mount a file system exported on a PC from a UNIX machine, run the following command:

Unix type	Command
SunOS, AIX, and OSF1	<code>mount pc:export_name /mnt</code>
SCO	<code>mount -f NFS pc:export_name /mnt</code>
HP-UX	<code>mount -t nfs pc:export_name /mnt</code>

in which:

- `mount` is the UNIX command.
- `pc` is the name of the PC running the NFS server.
- `export_name` is the name of the directory exported from the PC (in the example we use the Export name).
- `/mnt` is the name of the UNIX directory in which the remote directory will be mounted.

Note:

To perform the mount, UNIX uses the user number governing the execution of the mount command. The PC doesn't know what this number is. For the UNIX machine to be able to write to the exported directory, its name must figure in the list of authorized clients when the export process is defined.

Unmounting a file system from UNIX

To unmount a remote directory from a UNIX machine, execute the following command:

```
umount /mnt
```

Statistics

To view Tun NFSD server statistics, choose Stat from the Tun NFSD system menu (on the task bar). Alternatively, click Stat in the Tun NFSD configuration dialog.

The dialog displays information on requests made by other machines to the NFSD server. To obtain real time updates, click Refresh.

Using remote printers

Tun LPR allows a PC to use a network printer or a printer directly connected to a UNIX system or to another PC. This is printer redirection. A Windows program can use a choice of network printers to edit its documents.

A Printer Provider and a Network Provider perform remote printing with Tun LPR under 32-bit Windows, which renders this functionality perfectly compatible with that environment. The physical ports (LPT1, LPT2...) are not redirected.

To carry out the print job, the TCP connection respects the RSH, REXEC and LPD protocols. The connection is immediately closed once there are no further characters to print.

Notes:

This connection mechanism does not require permanent host processes or connections. If a PC with redirected ports is re-booted, it doesn't leave residual processes on the host.

Print redirection can run on any UNIX host-every UNIX server with TCP/IP has RSH/REXEC services, and many are equipped with LPD.

Declaring a remote printer in 32-bit Windows

Select Start > Programs > Esker Tun > Network Resources Access > Configuration > Print.

The list is empty when this screen first displays. Click New to declare a remote printer.

Name

Enter a symbolic name for the remote printer.

Remote Host

This is the name or the IP address of the remote machine that the printer to use is connected to. You can select one of the machines in the local host table for this field. For a network printer, this field is the IP address or the name of the printer.

Protocol

Select the type of protocol that the TCP connection uses to transfer the print job to the remote machine. There are three possibilities:

Protocol	Description
rsh	Works on all UNIX machines but requires previous configuration of the server
rexec	Works on all UNIX machines, doesn't require prior configuration of the server but requests a password for each print job.
lpd	Doesn't work on every UNIX machine, requires no prior configuration of the server, and doesn't require a password for each print job.

If the server to use implements the LPD protocol (AIX, SunOs, Solaris, HP-UX), it's better to use it.

Remote Command

This field only appears if you've selected the RSH or the REXEC protocols. Enter the name of the UNIX command that receives the characters to be printed on its standard entry. Typically, you enter the command "lp" in this field but you can use a different one (for example, cat >/tmp/tmp).

Remote Queue

This field only appears if you've chosen the LPD protocol. Enter the name of the UNIX print queue that the characters to be printed are sent to. You can use the command "lpstat -t" directly on the UNIX machine to obtain the list of print queues. Don't complete this field for a network printer.

User Name

This is the name of the UNIX user whose account to use to command a print job. The field is ignored if the printer is a network printer.

Timeout

Time after which print jobs are considered as failed if they haven't been processed.

Number of retries

As well as setting a timeout, you can set the number of times a print job should be re-sent. The timeout applies to each try.

Installing printers

The Install button displays the standard Windows dialog box for declaring printers. Click Install from NIS to install a printer defined on an NIS server.

Installing a remote printer in DOS based 32-bit Windows

Tun LPD uses the ADDJOB function to spool print jobs to windows printer queues. ADDJOB only works with local printers.

To install a printer, open the Printers folder. You can also access the installation program by clicking Setup > Install in the Tun LPR dialog (Start > Programs > Esker Tun > Network Resources Access > Configuration > Print). A dialog appears.

Click the Add Printer object to install the printer. This runs the Windows Wizard.

To the question "How is this printer attached to your computer?" select Network printer.

To the question "Network path or queue name?" give the name of the printer as it was previously declared. If you can't remember, click the Browse button to display the list of printers under the entry Tun LPR.

The remaining questions asked by the Wizard don't concern a network printer.

As soon as Windows acknowledges the remote printer, it can be used like an ordinary printer.

Printing in DOS on a printer installed in DOS based 32-bit Windows

You can use an LPR printer configured in Windows from the DOS shell. To do that, first configure the printer as follows:

1. Declare the printer to use as a Tun LPR printer. Let's call the printer "Printer_LPR" for example.
2. Then add a second printer with the following settings:
3. To the question "How is this printer attached to your computer?," select "Local printer."
4. Then select the manufacturer and the printer model for the printer "Printer_LPR."
5. Keep the existing driver as proposed by the Add Printer Wizard.
6. Select a Printer Port type port.
7. Enter a name for the printer, for example, "Printer_DOS" to recall the LPR printer's name. Don't select it as the default printer for Windows-based applications.
8. Click Finish without printing a test page.

When the printer "Printer_DOS" appears in the list of printers, choose Properties from the printer's context menu. Click the Details tab.

On this tab, click Add Port. Select the port type Other and choose Esker Port Monitor from the list of port types.

Select a port from the list in the dialog box that appears. Enter (optional) a description of the printer. Finally, select the remote printer ("Printer_LPR" in our example) to make the link with.

You can now print to this printer from an MS-DOS window.

Example:

Say your DOS printer is connected to the LPT2 port. Enter the command:

```
copy c:\foo.txt lpt2:
```

to print the file "foo.txt" on the network printer.

Sharing PC Printers

Tun LPD is a program that lets PCs share their printers with other network users (UNIX machines, other PCs...). A UNIX program (management or calculating applications, etc.) can use a PC's printer to perform print jobs. This functionality is known as “printer sharing.” The principal is as follows:

- A PC with a public printer runs Tun LPD. This is actually an LPD and RSH server that sends print jobs to the Windows Print Manager.
- Printers that are declared public are referred to by their logical name, that is, the name of the Print Manager queue. For example:

```
printer1=HP LaserJet 4/4M on LPT2
```

```
printer2=Postscript on LPT1
```

- When a UNIX machine prints on a PC's printer, it opens an LPD or RSH connection with the PC, and specifies the name of the printer to use.
- Characters that are sent across the connection towards the PC are received by Tun LPD, and then sent to the appropriate Print Manager print queue.

The procedure behaves as if a UNIX “pipe” were created between the printing application and the serving PC's parallel port.

Note: Tun LPD does not establish a permanent connection between PCs and UNIX machines. Therefore, there are no residual processes left on the UNIX machine if the PC is rebooted.

Tun LPD can run with any UNIX server. All UNIX machines equipped with TCP/IP contain an RSH (RCMD, REMSH) client.

Using the LPD server in a multi-user environment

You can connect to the multi-user server from a Citrix/Microsoft TSE client PC (or from the multi-user server machine itself) in administrator or user mode. The way you use the printer sharing functionality depends on the connection mode you use.

In Administrator mode, you can:

- Choose the start mode for the Esker LPD service, and start and stop this service.
- Define one or more LPD configurations.
- Define configuration rights for the ordinary user.

In User mode, depending on the rights defined by the administrator, you can do one of the following:

- Define one or more LPD configurations.
- Only view existing configurations.

To use printer sharing in the multi-user environment, you must start the Esker LPD service on the multi-user server and configure printer sharing with Tun LPD.

Setting up printer sharing

- In 32-bit Windows, select Start\Programs > Esker Tun > Network Resources Access > Configuration > Print Server.

If the LPD server isn't already running, a dialog proposes to start it.

If you're connected to the multi-user server as administrator, an extra check box is available labeled Limited access. This option lets you attribute to users the right to change or only view the LPD configurations defined by the administrator.

If you're connected to the multi-user server as a user, you can do the following (depending on the access rights the administrator has given you):

- Define LPD configurations: In this case, follow the instructions below.
- Only view existing configurations: In this case, following a warning message reminding you of your limited access rights, the same dialog box as the one above is displayed except that the Setup button is replaced by Consult.

Notes:

If a public printer has been activated, this dialog gives the user the choice of running Tun LPD as a background process (if this is not already the case).

You can also display this dialog box by running Tun LPD and selecting the Setup option in the system menu (select Start > Programs > Esker Tun > Network Resources Access > Local Server Startup > Print in 32-bit Windows).

You can hide the LPD server icon by checking Hidden Server. This avoids having too many icons displayed in the Windows environment when the keys Alt Tab or Ctrl Tab are used.

Error log

In some cases, it isn't appropriate to display error messages on the screen. By default, a log file is created for each LPD configuration. To avoid this, uncheck Create log file. To create a log file, enter the file path and the maximum size (in bytes). A warning message warns the user when the file is 75% full.

Creating a new configuration

Click New to configure printer sharing. A dialog appears.

Public Printer

Enter a logical name for the public printer: This is easier than having to refer to the full Windows print queue name each time to print. The logical name is then used by the LPD or RSH client to print to the correct printer.

Timeout

Expressed in seconds, the value given in the Timeout field determines the length of time after which Tun LPD considers that a print job is finished. If Tun LPD doesn't receive characters within the timeout period, it closes its connection with the client.

With a default value of 60 seconds, this option releases Tun LPD if a client machine locks up during a print job.

Print Manager Queue

Enter the real name of the Windows print queue in this field. You can choose from a list of currently configured printers by clicking the button to the right of the field. Tun LPD shares Windows print queues, and not parallel ports.


Conversions

- Append a Form Feed: Check this to force a form feed at the end of the print run. This option is useful for printouts originating on a UNIX server don't always carry a final form feed.
- CR/LF Conversion: Select this to convert all LF characters received from a remote machine into CR/LF. As UNIX only uses LF to mark the end of a line, and DOS/Windows uses CR/LF, this option enables files sent by UNIX machines to be printed correctly.
- Conversion tables: Select the conversion table you want: ISO8859> PC850 or PC851 > PC437G. The conversion ISO8859 > PC850 is useful to print accents and special characters from a UNIX system. UNIX systems use the ISO8859 character table to encode national characters whereas DOS/Windows systems use the ASCII PC850 character table.

Defining users' rights in a multi-user environment

In the main Tun LPD screen, select or clear the Limited Access check box to define users' configuration rights:

Sharing printers

To share a printer, select it from the list of printers in the Tun LPD window, then click . This printer can now be accessed from a client machine if the LPD server is running.

Activating public printers

Tun LPD must be running for public printers to be available to other users.

- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > Local Server Startup > Print.

Note:

The server is running when the program's icon appears in the taskbar.

When using public printers regularly, place the Tun LPD icon in the Windows Startup group so that it's loaded automatically every time Windows is started.

Statistics

You can obtain statistical information on the functioning of the Tun LPD server. To do that, choose Stat from the Tun LPD system menu (when the application is running as an icon) or click Stat in the LPD configurator. A dialog appears.

The screen displays the number of jobs and also the number of characters received by the Tun LPD server, and supplies information on current printing operations. To obtain real time updates, click **Refresh**.

Using public printers directly from PCS

With Tun LPR, PCs can print directly to public printers without going through a UNIX system. In other words, the print redirection client (LPR) can declare another PC running LPD as the remote host. To configure direct PC-to-PC printing using LPR:

- In 32-bit Windows, choose Start > Programs > Esker Tun > Network Resources Access > Configuration > Print.

Then, click New:

Complete the form as if redirecting an LPT port to a UNIX host:

- Name: A local alias name for the remote printer.
- Remote Host: The name of the PC with the public printer.

- Remote Queue: Enter the logical name of the public printer (as declared on the other PC) in this field.
Choose RSH or LPD protocol (don't use REXEC protocol).
Click Install from NIS if to install a printer defined on an NIS server
Then, use the printer installation procedures described in the chapter "Using remote printers."

FTP in ActiveX version

The ActiveX version of FTP is available from the Tun Plus container. The container is an application that hosts ActiveX components. It is supplied with the UNIX and IBM emulations, along with the Esker FTP application. This chapter describes how to use the FTP application when an FTP session is run in the Esker Viewer application.

Opening an FTP session

To open an ActiveX FTP session:

- Select Start > Programs > Esker Tun > Network Resources Access > FTP. Esker Viewer starts and opens an FTP session.
- From Esker Viewer, select File > New.
- From the New session dialog, select FTP Session and click OK.

FTP connection settings

General

Name

Enter the name or IP address of the server that you want to connect to.

Note:

Only enter a name if you have a names server.

FTP Port

By default, the port number corresponding to the FTP protocol is 21. If the port number is different, enter the new value here. Check Use Passive mode to have the server choose the port to use during connection.

User/Password

Enter the user name and password for the FTP connection. Check Save Password to save the password for future connections. Check Anonymous Connection for anonymous FTP access: In this case, enter an e-mail address instead of the password (the e-mail address is saved).

Automatic connection at startup

If you save your FTP configuration in a workspace, you can request automatic FTP connection upon opening the workspace. For this, check Automatic connection at startup.

Connection

Account

Enter the name of the user's FTP account.





Initial directory

Enter the name of the sub-directory, which will act as the default access directory on the server.

Timeout

Specifies the period of time in milliseconds after which packets are re-sent to the FTP server if there's no response.

Commands

Enter the commands to send to the server when the connection is established (these commands depend on the server type: See the section “UNIX commands sent to the server” in “Interactive use of FTP”). If an FTP profile is selected (see the Conversions tab), the commands defined in the profile are displayed in the list and can't be changed or removed. To add a command, click . To delete a command from the list, select it and click . To change the position of a command, select it and click  to move it up the list, or  to move it down.

Conversions

FTP Server Type

An FTP profile is used to read the lists of files from the server. The format of these lists depends on the system. Esker supplies pre-defined profiles, but you can create new ones (see **FTP Profiles**). Select a profile associated with this FTP session.

Data Type

The data type is used to convert the messages from the server. Select the data type of the commands exchanged with the server.

Data Transfer

Data transfer can be binary or in ASCII format. Select Binary to transfer the files without conversion. Select ASCII to convert the carriage returns and line feeds between Windows and UNIX.

Note:

You can change the type of conversion after the connection has been made.

Local data type / Remote data type (ASCII mode)

You can choose another character coding on the local and/or remote machine, so that the conversions take place correctly.

Changing a connection

You can at any moment view or modify the connection parameters of a session, connect according to these parameters, or disconnect.

► Viewing or modifying the connection parameters

Select Session > Connection > Configuration. The dialog that appears is identical to the connection dialog used when starting an emulation session.

► Connecting or disconnecting the configuration

Select Session > Connection to connect according to the parameters defined in the dialog (Configuration option).

Select Session > Connection > Disconnection to disconnect the current session.

Security gateway

You can configure a security gateway to protect the exchanges during an FTP session. The Esker container manages customization of the security gateway. Refer to the Esker Viewer chapter of the Application Access manual to find out how to configure a security gateway.

Display parameters

When you establish a connection (the server is available and the user name and password are correct), the tree structure of FTP server directories appears.

If you specified an initial directory in the configuration, the tree-structure is displayed from this directory.


Browsing remote file systems

You can browse remote file systems using the standard Windows method. Directories appear as yellow folder icons. An open folder indicates the current directory in the directory tree (left pane). The files appear as paper sheet icons. Click a directory to open it and move around inside it.

Display server directories and files as icons or lists

Select the option of your choice from the View menu: Large Icons, Small icons, List or Details menu. These options are also accessible from the context menu displayed when you click on the mouse right button in the right-hand window. You can also use the buttons proposed in the toolbar by default.

Display source file

Select View > Source. You can also click  on the toolbar.

Filters





You can apply particular filters in order to display only certain files. This limits the list of files by selecting only those of use for the session (for example, a single type of files, or all types of files except some).

► Apply filters to the files

Select Session > Connection > Commands > Filter. A dialog appears.

There are two areas in the dialog box:

- Include filters lets you enter filters for the file type(s) to display. For example, if you add “*.txt” to the filter area, only the files with the extension .txt will be shown.
- Exclude filters lets you enter filters for the file type(s) you don't want to display. For example, if you add “str*” to the filter area, the files beginning with “str” won't be shown.

Click  to add a filter,  to delete a filter, or  and  to change the order of the filters in the list.

Interactive File transfer

File transfer can be performed between:

- A remote FTP server (whose directory tree is accessible from an instance or session of the FTP ActiveX component) and your PC (whose directory tree is accessible from Windows Explorer).
- Two remote FTP servers (on which each of the directory tree structures is accessible from two FTP ActiveX instances or sessions).

To perform the file transfer, you can:

- Copy and paste the files via the clipboard.
- Drag and drop the files.

File transfer between PC and server

To transfer files between the PC and the FTP server:

- Open an FTP connection on the server: the server directories and files are then available from Tun FTP.
- Open Windows Explorer to display the PC's directories and files.
- Use one of the following methods to transfer files.

File transfer between servers

To transfer files between two FTP servers, open an FTP session for each server. Then, use one of the following methods to transfer files between the sessions.

► Copy/paste a file or set of files

Copy and Paste are available in the Tun FTP:

- Edition > Copy or Paste.
- Right-click and select Copy or Paste.
- Keyboard short cuts Ctrl-C to copy and Ctrl-V to paste.
- Toolbar buttons.

From the source window, select the source file(s) and copy into the clipboard.

In the target window, select the target directory and paste the file(s) from the clipboard.

Notes:

You can select an entire directory and transfer it.

To select multiple files, press and hold <Shift > (to select consecutive files) or <Ctrl > (to select non-consecutive files).

► Drag and drop a file or set of files)

Drag and drop is available in Tun FTP. From the source window, select the file(s) and drag them to the target directory.

► Displaying progress of transfer

During the transfer operation, a dialog appears to inform you of how the operation is progressing.

Click Cancel to cancel file transfer.

After a transfer, the Transfer terminated message appears.

For more information on the status of the transfer, click Details.

Type of transfer

File transfer is performed in binary mode by default. Click the button to transfer files between the two machines exactly as they are (with no conversion filters).

To account for differences between the end-of-line characters in the DOS and UNIX systems, select ASCII mode to change the CR/LF character to LF or vice-versa, depending on the direction of the transfer. In ASCII mode, format conversion is performed in accordance with the formats of the local and remote data. Select these formats in the list boxes above the directory trees.

► Modifying transfer mode

Select Session > Connection > Configure, and click the Conversions tab. Select the file transfer mode.

Other actions

Apart from transferring files, you can perform other actions from the context menu:

- Save: Saves the selected files or directories to the local drive or a network drive.
- Delete: Deletes selected files or directories. Confirmation is requested before the files or directories are deleted.
- Rename: Changes the name of the selected file or directory.
- Open: Opens a file in a text editor or starts the program if it's an executable file.
- Source: Displays the contents of a directory as a file list (for example, as the output of the UNIX command “ls -l”).

UNIX commands sent to the server

You can send UNIX commands to the server from this dialog.

Enter the UNIX command that to send to the server in the command line and click Send. The list of UNIX commands you can use depends on the system you're working on. To view this list, click Command List. The command list appears in the lower part of the dialog.

Note:

Commands followed by an asterisk (*) are not implemented.

Example of UNIX command

On a SCO-type server, you can set the file permissions of the files on the FTP server using the command “umask xxx,” where xxx is the octal code for the file permissions to assign. When you enter the command “umask 111” on the command line, you set the file permissions to 666 (that is, -rw-rw-rw-).

Macros

File transfer from Tun FTP application can be controlled automatically using macros. Macros can be used to open an FTP connection, send commands to the server, download or save files to your machine or the server and close the FTP connection.

Macros can be created and run with FTP in the following way:

- Create and run macros written in VBScript or JScript. Use the macro management tool supplied in the container.
- Run macros written with EScript.

Notes:

Macros written in VBScript are saved in files (or function libraries) with extension VBS. Macros written in JScript are saved in files (or function libraries), with extension JS. Files with extension VBS and JS can contain several macros (or functions), and each of these macros can be run separately. Macros written in EScript are files with extension MAC. MAC files contain only one macro per file.

FTP API

Writing an FTP macro in VBScript or JScript language requires familiarity with the properties, methods and events of the FTP API ActiveX component. FTPAPI.HLP documents this API, and it is available in \Pc2host\Win32\DOCS\MISC on the CD-ROM.

► Creating a new macro

Select Tools > Macros. The macro manager opens. You can create a new macro or a new macro library from the Notepad text editor or by using the macro recorder proposed by Esker.

Encrypting a string

String encryption is useful to include a password in a macro, for example. Copy the encrypted password to the macro, rather than the password itself. Tun FTP uses a simple encryption tool.

Select Tools > Macro > Encrypt a string.

Running a macro in EScript

You can run a macro written in EScript (single macro in a file with extension MAC), as Tun FTP is compatible with this language.

From the container, select File > Open. Then, select Macro Tun FTP (.mac) and choose the .mac extension file of your macro.

FTP profiles

The FTP profile used by a session is stated in the FTP server type field of the Conversions tab in the FTP connection dialog.

Definition

The purpose of the profiles is to give the user a mechanism authorizing access from the FTP client application to non-standard servers. An FTP profile determines from the data returned by the FTP server which information (or fields) is to be displayed in the client application graphic interface. The graphic interface can display the following information:

- File name.
- File type.
- File size.
- Last modified date.
- File attributes.
- File owner.
- Group the file belongs to.
- Number of links to the file.

A profile is a sequence of character strings comprising a series of field descriptors and field separators.

Notes:

In the rest of this chapter, line designates each element in the file list returned by the server. Depending on the type of server and line separator used, a single element can be returned on one or more lines.


Similarly, blank designates the “space,” “tab” and “Enter” characters.

Some information, which is irrelevant to a particular FTP server, can be left blank. Only the name and type of file are obligatory. A line is ignored if the file name or type is omitted.

The file size must correspond to the profile's numeric base (for example, only base 10 numbers).

► **Displaying the format of the list of files**

If you use an incorrect server profile to connect to an FTP server, the remote directory may appear empty. Check the format of the file list used on the server and make sure the profile used is compatible.

To view the format, select Display > Source, or click  on the toolbar. The server file list is shown as it appears on the server (as output of the UNIX “ls” command, for example).

You can also obtain information on the server type by sending the SYST command to the server (see UNIX commands sent to the server).

Creating a new profile

Esker supplies the main standard profiles used for FTP transfer. However, you can create new profiles if you need a particular configuration.

► **Creating a new FTP profile**

In the Windows registers base, create a new Profile key under entry:

HKEY_LOCAL_MACHINE\Software\Esker\Tun\8.00\FtpX

The Profile key can contain the following strings:

Name	Name of profile
Profile	String describing the profile
UNDEFINEPDSprofile	String describing the MVS profile
Type	Type of server 1 for MVS (multiple profile management), 2 for UNIX (link management), 0 for the other types of server.
Logincommand	Commands to be executed at connection (binary field ending in double zero)
BlockSize	Size of a block (DWORD). By default equal to 1.
Base	Numerical base of the size (DWORD). By default equal to 10.

Name	Name of profile
ListSeparator	Separator for the LIST command (binary field ending in zero). By default 0D0A.
NameListSeparator	Separator for the NLST command (binary field ending in zero). By default 0D0A.
CaseSensitive	Case sensitivity (1 if yes, 0 if not). Parameter used to find out whether a file with the same name already exists on the server. By default equal to 0.

Field Descriptor

The FTP client using the field descriptor sequence scans each line of the directory list sent by the FTP server. Each field descriptor in the sequence corresponds to a field in the lines to be scanned. A field descriptor can include the following items:

- Field descriptor codes.
- Field descriptor modifiers.
- Field descriptor tests.

Field descriptor codes

The letters A, B, D, F, G, L, S, U, and I show the type of field descriptor information:

A	File attributes
B	File size (number of blocks)
D	File date and time
F	File name
G	The group which owns the file
L	Number of links to the file
S	File size (number of characters)
U	The user who owns the file
I	Skips the field (default value)

Notes: Field descriptor letter codes are not case sensitive.

If the same field descriptor code appears several times in the profile string, only the value of the last descriptor counts.

S indicates the file size as given by the server. B corresponds to the same size multiplied by the value of the Block-Size parameter in the profile configuration.

Example:

A standard UNIX directory list line looks like this:

```
-rw-r--r-- 2 rootsystem 890Sep 12 15 :24 passwd
```

It contains the following fields:

- File attributes (file type and access rights).
- Number of links to the file.

- User who owns the file.
- Group which owns the file.
- Number of bytes stored in the file.
- Month of the last modification.
- Day of the last modification.
- Time (or year) of the last modification.
- File name.

A simple profile can be created to deal with this kind of FTP server:

```
A, L, U, G, S, D: D: D, F
```

The field separators used are the comma (“,”) which removes the spaces in front of the next field descriptor; and the colon (“:”) which concatenates the values of several field descriptors in the same field (in this case, the date and time of the last modification).

Field Descriptor Modifier

By default, the line returned by the server is scanned from the current read position up to the first blank encountered. You can change field descriptor default behavior by appending a modifier. Three types of modifiers are possible:

- Length modifier.
- Character set modifier.
- Pattern string modifier.

Length modifier is used for fields in which the number of characters is known. This modifier is an integer equal to the size of the field. The field doesn't have to end with a blank character and may even contain blanks. For example, you can use the field descriptor A10 when the scanned lines have an attribute field of exactly 10 characters. A length of 0 means an unlimited length: The rest of the line is then used for the field (including blanks). If no length is indicated, the field will only contain the string corresponding to the descriptor up to the first blank.

Character set modifier is used when the character set appearing in the field is known. The following syntax applies:

- Authorized characters are included in brackets. For example, [aAZ] means the characters “a,” “A” and “Z” are authorized in the field.
- Unauthorized characters are preceded by a caret: The field can then contain any character except the ones in brackets. For example, [^aAZ] means that the characters “a,” “A” and “Z” are excluded from the field.
- An interval may be defined by placing a dash between the interval bounds. For example, [A-Z] means that the characters “A” through “Z” are authorized in the field and [^0-5] means that the characters “0” through “5” are excluded from the field.
- The backslash character is an escape character for special characters (\t is a tab character, \] is a square bracket, \- is a dash, \\ is a backslash).

A length modifier may follow the character set modifier. In this case, the field ends either at the first scanned character which is not part of the character set or when the given length is reached.

Examples of character set modifiers are:

[0-9]	Decimal number
[0-9a-fA-F]	Hexadecimal number
[^\t]	Every character excluding blanks and tab characters
[rwx\~]9	UNIX simple access rights (read, write and execute)

Pattern string modifier is used to match a string in the scanned line. The complete pattern must appear in the scanned line at the current scan position for the field to be recognized.

A pattern string modifier is indicated between braces. If the pattern string is to contain a closing brace, it must be preceded by a backslash. For example, to test whether a line received by some MS-DOS FTP servers corresponds to a subdirectory or not, you can use the pattern string modifier {<DIR>}

Typically, a pattern string modifier is used in conjunction with a field descriptor test mark.

Field Descriptor Test Mark

You can add a test to a field descriptor ({+|-|*|!|/} et !). There are five types of test:

- + the string processed is a file (File positive test mark)
- - : the string processed is ignored (File negative test mark)
- * : the string processed is a link (UNIX)
- | : the string processed is a file name (AS400)
- / : the string processed is a sub-directory

The file positive or negative test marks are used to determine whether or not the scanned line is an ordinary file line (that is, a recognized type). For the file positive test mark, if the scanned field doesn't match the field descriptor, the scanned line is considered to be a non-ordinary file line. For the file negative test mark, if the scanned field matches the field descriptor, the scanned line is considered to be a non-ordinary file line.

The symbolic link test reveals if the scanned line is a link to a file or directory on the UNIX platform. If the scanned field matches the field descriptor, the line is considered as a symbolic link line to a file or directory.

Note:

The symbolic link test for UNIX servers only works with type 2 profiles. See "Creating a new profile."

The file name test reveals if the scanned line matches an AS400 file name. If the scanned field matches the field descriptor, the line is considered a file name line.

The subdirectory test mark is used to determine whether or not the scanned line is a subdirectory line. If the scanned field matches the field descriptor, the line is considered as a subdirectory line.

Before scanning, every line is considered as a non-ordinary file line. After the scan, lines that are not subdirectory or ordinary files, or links, or filenames are omitted. If the scan results in an empty file name, or the . and .. file names, the line is also omitted.

An exclamation mark ("!") means that the next field descriptor scans the information sent by the server at the same position in the string as the current descriptor. So if an exclamation mark follows a field descriptor, the current field is rescanned with the next field descriptor. This allows several successive field descriptor tests to be performed on the same fields until one is positive (the remaining tests are then skipped).

Field separators

The field separators are: “,” “;” “:.” A field separator must separate two field descriptors. By default, a field descriptor matches all the characters of the scanned line up to the first blank character encountered or the end of the line. Field separators can change the way the line from the server is scanned:

- A comma deletes the spaces and tabulations before the field descriptor it precedes.
- A colon (:) also matches contiguous blanks but concatenates several field descriptors in the same output field. The field descriptors on either side of the colon must use the same field descriptor code.
- A semi-colon changes the scan direction (by default, the lines are scanned from left to right).

In the following example, the attributes field and the links field are scanned from left to right. Then, the file name, modification date and time (concatenated), size, group and finally user fields are read in the other direction from the end of the line:

```
A, L; U, G, S, :D:DD, F
```

Note:

When the line is scanned from right to left, the concatenation is not read completely in this direction. In fact, the colon always precedes the field it concatenates in the direction left->right. To express D (“D”) concatenated with D (“:D”) concatenated with D (“:D”), we obtain scanning from left to right “D:D:D,” and from right to left “:D:DD.”

Profile examples

Example 1

The standard UNIX attributes can be defined using the following sequence of three field descriptors:

```
A[d]l! A[\-]l+ A[rwx]9
```

A[d]l!: If the first character scanned is “d,” the line is recognized as a directory. The attribute field (“A”) takes the value “d.” The next field descriptor rescans the current field (“!”).

A[\-]l+: If the first character scanned is “-,” the line is recognized as a file. The attribute field (“A”) takes the value “-.”

A[rwx]9: The remaining attributes cover 9 characters and use the letters “r,” “w,” “x” or “-.” The attribute field (“A”) takes the value “rwxr--r--.”

Example 2

This profile example is for a UNIX server that returns a directory list in the following format:

```
-rw-r--r--_2_root_system_890_23_Sep_12:15:24_my_passwd
```

The corresponding profile is: a[\-]l+!a[l]l*!a10,l,u,g,s,d:d:d,f0

The profile scans the line as follows:

- a[\-]l+: If the first character scanned is “-,” the line represents a file and the attribute field takes the value “-.”
- !: The line is scanned with the next descriptor starting from the same character as the current descriptor, that is, the first character in the line.
- a[l]l*: If the first character is “l,” the line is a symbolic link (UNIX) and the attribute field takes the value “l.”
- !: The line is scanned with the next descriptor starting at the same character as the current descriptor, that is, the first character in the line.
- [d]l/: If the first character is “d” the line represents a directory and the attribute field takes the value “d.”
- !: The line is scanned with the next descriptor starting at the same character as the current descriptor, that is, the first character in the line.
- A10: The attribute field takes as its value the first ten characters scanned from the current point (the start of the line), namely “-rw-r--r--.”
- ,: Removes the space between “-” et “2.”
- l: Link = “2.”
- ,: Removes the space between “2” and “root.”
- u: User = “root.”

- ,: Removes the space between “root” and “system.”
- g: Group = “system.”
- ,: Removes the space between “system” and “890.”
- s: Size = “890.”
- ,: Removes the space between “890” and “23.”
- d: Date = “23.”
- :: Concatenates the following field.
- d: Date = “23 Sep.”
- :: Concatenates the following field.
- d: Date = “23 Sep 12:15:24.”
- ,: Removes the space between “24” and “my.”
- f0: File name = “my passwd”; the 0 means the rest of the line must be assigned to the file name field. This accounts for file names with spaces. If “f” had been used in the example instead of “f0,” the file name would have been “my.”

However, in some cases the server doesn't return the user name:

```
-rw-r--r--_2_____system_1320_23_Sep_12:15:24_mypasswd2
```

The above profile wouldn't work in this case as there's no user and therefore all the values are shifted left. The user field is assigned the group value, the group field is assigned the size value, etc. The problem is solved by using the following profile:

```
a[\\-]1+!a[1]1*! [d]1/!a10,l;u,g,s,:d:dd,f
```

In this profile, the scan is reversed after the semi-colon that is when the link field is scanned. The user is thus scanned last: It's no longer important whether there's a user or not. On the other hand, this particular profile won't accept file names with spaces like the previous profile. Notice, that if “f0” had been kept in the profile with the reverse scan, the rest of the line (scanned from right to left) would have been assigned to the file name and the other fields left empty.

Profile checking

To check your profiles you can use the following JavaScript page and replace “a[\\-]1+![1]1*! [d]1/!a10,l;u,g,s,:d:dd,f” with your profile and “-rw-r--r-- 2 root system 890 23 Sep 12:15:24 passwd” with your server's directory list format:

```
<HTML>
<HEAD>
<TITLE>FTP profile checking </TITLE>
<script language="JavaScript">
function TestProfile()
{
s = Gui.TestProfile("a[\\-]1+![1]1*! [d]1/!a10,l;u,g,s,:d:dd,f,"
"-rw-r--r-- 2 root system 890 23 Sep 12:15:24 passwd")
window.alert(s);
}
</script>
</HEAD>

<BODY BGCOLOR="#808080" LEFTMARGIN="0" TOPMARGIN="0" SCROLL=no>
<a href=JavaScript:TestProfile()> Profile test </a>
<OBJECT ID="Gui" HEIGHT=0% WIDTH=0% CLASSID="CLSID:D9B8A3A7-29B9-11D1-88DD-
444553540000">
</BODY>
</HTML>
```


File transfer with FTP clients

The FTP protocol (File Transfer Protocol) is used for transferring files from one machine to another. The FTP client establishes a connection with the FTP server to transfer data (in the direction client/server or vice versa). A PC may be the FTP client or the server or both.

FTP uses two main transfer modes, binary and ASCII. In binary mode, the bits in the files are transferred without modification and the file and its copy are exactly identical. This means that the receiving machine can re-read the file in its original form, which isn't necessarily the case for two machines with different architectures (for example, a UNIX server and a Windows PC). ASCII mode allows files to be transferred from a UNIX environment to a Windows environment and vice versa with the correct management of carriage return and line feed characters.

By implementing the FTP client protocol, Tun Net allows a PC to become a FTP client and exchange files with a server.

Tun Net and FTP

Tun FTP offers an easy-to-use graphical interface to FTP, the standard File Transfer Protocol used to transfer files between servers and TCP/IP clients. Tun FTP is a client program. There are two ways to use Tun FTP:

- Interactive mode uses a graphical interface similar to Windows Explorer: The user can select files and destination servers with the mouse.
- Programmed mode is used to automate file transfer tasks in written procedures.

Tun FTP and NIS

Tun FTP is enhanced by access to the NIS server through the NIS Browser included with Tun applications. This functionality lets you view the network's FTP configurations that are defined on the NIS server. The administrator must have previously configured the NIS server and defined the FTP Configurations resource table using the NIS browser. See "The NIS Browser" for comprehensive instructions on that application's use.

Starting Tun FTP

Run the program by clicking Tun FTP in the Network Resources Access group (Start > Programs > Esker Tun under 32-bit Windows). When you start Tun FTP, a dialog appears.

The dialog invites you to connect immediately to an FTP server.

NIS configuration

To use an FTP configuration that's accessible through the NIS, click Cancel to quit this dialog box and choose File > Open NIS Connection from the main menu. Then double-click the desired resource to activate it.

Direct configuration

To define your own FTP configuration, complete the Tun FTP Config dialog as follows:

Configuration Name

Enter the configuration name in the first field. By default, Tun FTP stores the parameters of the connections in a log file (wftp.ini). The name used to save the configuration is composed of the host name and the user name. This makes

it easier to establish a connection with the most frequently used FTP servers without having to supply the same information each time. To select a configuration from the log file, open the list of configurations, select one and click OK. To create a new configuration, click New: All the fields are then cleared and the new configuration values can be entered.

Note:

The configuration files don't hold the password.

Host

Enter the name or IP address of the FTP server.

User

Enter the name of the account whose access rights to use to access the server.

Password

Enter the user's password.

Anonymous Login

If you check this, the name “anonymous” is automatically placed in the User field, and the password prompt is replaced by a prompt for the user's e-mail address.

Options

Options opens a dialog for additional connection parameters.

Home Directory

Enter the name of the default server directory.

Account

Some servers require an account number in addition to the user name and password. Enter this number here. If a password is required for access to the account, a dialog appears for this purpose.

FTP Service Number

The default FTP connection always uses TCP/IP port number 21. Some non-standard servers may use a different port. If this is the case, change the default.

Comment

Enter a description, which is displayed instead of the configuration name. You can provide a descriptive title for an FTP connection in addition to the server and user names.

Stay under the Home Directory

Check this to treat the user's home directory as the “root” directory in the remote file system when you open an FTP connection with a particular user account. It's then impossible to access public directories such as /tmp.

Host Type

Specify the remote host and data types (if known) in these fields.

- FTP Server Type is used to scan directory lists received from the server. The format of the directory lists is system-dependent.
- FTP Server Type can be chosen from among the predefined main server types, or a new FTP Server Type can be defined (see further on: Defining Server Profiles).
- Data Type is used for converting the character string messages received from the server during the FTP session.

Data Transfer

Specify the default data transfer type for the connection. You can change these values once the connection is opened. If you select Binary, the files are transferred as they are with no conversion.

If you select ASCII, Carriage Return and Line Feed conversions between DOS and UNIX are performed. In addition, you can specify the local and remote data types. The default values are standard and are suitable for most purposes: If either machine is known to have a different character standard then you specify this and the relevant conversions are performed during file transfer.

Connection

After completing the required fields, click OK to connect. If the server is available and the user information is correct, the Tun FTP file manager screen is displayed.

Local

The top half of the window is a graphical representation of the PC file system, similar to that of Windows Explorer.

Remote

The file system on the remote machine (displaying the home directory of the account used for the connection).

History

Lists the command “dialog” between the PC and the server. Double-click in this area to enlarge the display of exchanged commands.

Status bar

Message area showing the results of the most recent command.

Multiple connections

Tun FTP runs in MDI (Multiple Document Interface) mode. This means that you can open simultaneous sessions on different servers, assuming that you've allocated enough TCP connections in your kernel (see “TCP/IP Configuration on a UNIX host” in this manual for more details).

Closing a session

Close a file transfer session by choosing File > Close Connection.

Using a firewall

Choose Options™Firewall from the main menu to implement a firewall. You can then only access an outside server by passing through a gateway machine of the Proxy type, which acts as a security filter to protect the local network.

To configure the gateway, check Use a Proxy server (SOCKS protocol). Enter the name or IP address of the server (only enter a name if your system uses a DNS). You can also choose the server from the drop-down list box: The list contains the servers registered in the host table (hoststab) and on the NIS server (NIS resources are shown in yellow).

Enter the port number for the SOCKS protocol (typically, this is 1080, the default value).

To avoid using the gateway for local network communications, check Do not use for local addresses.

You can apply the firewall settings to all Tun applications on your machine by checking Use these settings for all Tun applications. To reapply general settings to all Tun applications, click Restore general settings.

Interactive mode

Navigation

Tun FTP has the “look and feel” of Windows as you navigate through the file systems on local and remote machines.

File structure representation

A yellow folder icon represents directories, with the current directory shown as an open folder.

An icon that looks like a sheet of paper represents files: Its appearance varies depending on the file type (as in Windows Explorer).

File information such as size and date of creation appears next to file icons. To view more details of files, choose Options > File Details. You can also choose Options > File Sort to restrict the display to a particular file type, and sort files.

Directories first

Since directories are displayed before files, click a directory to view its contents.

Double-click remote directories to send explicit requests to the FTP server, or highlight the directory and click Refresh to send the request.

When the directory has been read, all its files are displayed. The directory tree remains displayed on the left side of the window. You can hide it by choosing Options > File Details and unchecking Tree: This increases the size of the file window.


Due to the large number of FTP requests, refreshing a remote file system takes longer than refreshing a local file system.

Simple transfers

Here's one way to transfer a file from one machine to another:

Select the file on the source machine (highlight the file).

Select the target directory on the destination machine.

Click Copy (). Transfer progress displays.

When the file transfer is completed, the status window disappears and the target file system display is refreshed.

Note: If the file name is incompatible with the format used by the destination system, a dialog box lets you rename the file.

Transferring several files

To transfer a number of files at the same time, hold Shift to select adjacent files, and Ctrl to select non adjacent files.

Transfers using “drag and drop”

You can also transfer files using the mouse (drag and drop):

Select the files to transfer.

Keep the mouse button pressed when you've selected the last file, and move the cursor to the icon of the destination directory.

Release the mouse button.

A dialog box will ask you to confirm the transfer.

If you accept, the transfer takes place as described above.

Transferring directories

To transfer a directory, select it in the right pane and drag and drop it to its destination.

Transfers between servers

You can easily transfer files between servers using “drag and drop”. To do this, open simultaneous FTP connections on the servers and drag and drop the files from one connection window to the other.

Applying Filters

-
- B** File transfer is performed in binary mode by default. Click to transfer files between the two machines exactly as they are (with no conversion filters).
 - A** To account for differences between the end-of-line characters in the Windows/DOS and UNIX systems, select ASCII mode to change the CR/LF character to LF or vice-versa, depending on the direction of the transfer.
-

Additionally, in ASCII mode, format conversion is performed in accordance with the formats of the local and remote data. You select these formats in the corresponding list boxes above the directory trees.

File management

The file management buttons perform the following functions:

Delete File(s)

Click Delete to remove selected files. By default, you're asked to confirm your choice. Clear Options > Confirmation to stop the confirmation requests.

Rename File

You can change the name of a file by clicking Rename. A dialog prompts you for a new name.

View File

To see the contents of a selected file, click View.

File Details

To see all the attributes of a particular file (like size, attributes, date, name, or owner), select the file, and then click File Details.

UNIX commands sent to the server

You can send UNIX commands to the server from the Tun FTP window. To do that, choose File > Other Command and enter the UNIX command that to send to the server. The list of UNIX commands varies according to the system.

To view this list, enter the UNIX command help on the command line of the option File > Other Command. The list of commands appears in the lower part of the dialog. Double-click in this area to increase the size of the window.

Note:

Commands followed by an asterisk (*) are not implemented.

Example of UNIX command:

On a SCO-type server, you can set the file permissions of the files on the FTP server using the command "site umask xxx", where xxx is the octal code for the file permissions to assign. When you enter the command "site umask 111" on the command line of the option File > Other Command, you set the file permissions to 666 (that is, -rw-rw-rw-).

Automated file transfer

Tun FTP contains an integrated macro language that you can use to replace keystrokes and mouse-clicks and manage file transfer sessions automatically. You can run a macro from within Tun FTP, or associate a macro with the program icon in Windows so that it's executed automatically when the program is started.

Enter the following command line in the Properties of the program icon:

```
C:\...\TUN\TCPW\WFTP32.exe -Mmacro_file
```

in 32-bit Windows,

where macro_file is the name of a file with a ".mac" extension that contains connection and transfer instructions.

To execute a macro from within Tun FTP, choose File > Execute Macro, and enter the name of a macro.

Macro example

Below is an example of a macro (winftp.mac) that prompts you for your login information, makes a connection, then transfers all the files with a ".bat" extension in the \Tun\Tcpw directory to the /tmp directory on a UNIX server:

```
# Display the Message Window
ShowMessage

ReadVar "Enter the host name" HOST
IfEqual "" %HOST exit
ReadVar "Enter your user name" USER
IfEqual "" %USER exit
ReadPasswd "Enter your password" PASSWD
IfEqual "" %PASSWD exit

ClearMessage
verbose "on" -s
debug "off"

#Connection

login %HOST %USER %PASSWD
IfError ERROR
lcd "\\tun\tcp"
cd "/tmp"
mput "*.bat"
logoff

Echo "Macro has finished" -b "Message"
exit
```

```
Label ERROR
Echo "Connection Error" -b "Error"
exit
```

Language description

Instructions consist of valid commands followed by parameters, with one instruction per line. The command name is always the first word on a line.

In this manual, commands are composed of capital and small letters to make them easier to read. However, case makes no difference to the program. For example, ReadPasswd, READPASSWD, and readpasswd are all interpreted in the same way.

Lines beginning with the character # are considered as comments.

The macro language is only capable of handling strings of characters (any characters with ASCII values between 0 and 255) delimited by double quotes. For example: "Tun Net is a communications software package".

Variables

You can define an unlimited number of variables to store character strings. These variables can then be used instead of command parameters.

Variables must be preceded by the character % when they're used in instructions:

```
Login %HOST, %USER, %PASSWORD
```

When variables are defined and assigned, the % character isn't used:

```
Set variable "abcde"
```

If an instruction calls a variable that hasn't been defined, the macro-language interpreter looks at the DOS environment to see if it's been *set* there instead. If the variable remains undefined, an empty string is used.

List of instructions

Below is a list of the available Tun FTP commands with a brief description of each. The exact syntax is described in the last chapter of this manual.

Tun FTP commands	Description
aget	Initiate file transfer from the host machine to the local machine in ASCII mode
append	Add the contents of a local file to the end of an existing file located on a remote host
aput	Transfer files from the local machine to the host machine in ASCII mode
ascii	Change default transfer mode into ASCII mode
bget	Copy a file from the host machine to the local machine in binary mode
binary	Change the default transfer mode into binary
bput	Transfer a file from the local machine to the host machine in binary mode
cd	Change current directory on the host machine
ClearMessage	Erase all messages in the execution window
debug	Write a .LOG file with messages sent to FTP
delete	Delete a file on the server
Dos	Execute a DOS command
drive	Select a new current drive on the local machine
Echo	Display a character string in the execution window or in a specified message box
Exit	Unconditional exit from a macro

Tun FTP commands	Description
lcd	Change the current directory on the server
get	Copy a file from the server to the local machine
Goto	Unconditional branch to a label
HideMessage	Hide messages in the macro execution window
Host_text	Set the server's charset
IfConnected	Test whether or not the local machine is connected to a server
IfEqual	Test a variable or most recent FTP response for equality
IfError	Test the results of the most recent command
IfNoEqual	Test a variable or the most recent FTP response for inequality
IfNoError	Test the results of the most recent command
Label	Define a label
lcd	Select a new current directory on the local machine
local	Set word size on the local machine
login	Establish connection with a server
logoff	Close the current connection
mdelete	Delete one or more files on the server
mget	Copy one or more files from the server to the local machine
mkdir	Create a directory on the server
mput	Copy one or more files from the local machine to the server
option	Set an option
Pause	Wait one second
parent	Change to the parent directory on the server
put	Copy a file from the local machine to the server
ReadVar	Enter a character string in a dialog box and assign it to a variable
ReadPasswd	Enter a character string and assign it to a variable without displaying the characters
rename	Change the name of a file on the server
rmdir	Remove a directory on the server
Set	Define and assign a variable
Server	Execute a UNIX FTP command
ShowMessage	Display the macro-execution window
stat	Check whether FTP responds to commands (testing for possible disconnection)
text_codes	Set the text formats for the local and remote files
Title	Assign a title to the macro-execution window
verbose	Display or hide messages

Note:

If you're having trouble connecting to an FTP host using Tun FTP, read the next section for suggestions on how to deal with some of the differences in the way UNIX servers handle FTP.

Defining Server Profiles

Most servers are of the standard UNIX type. This section need only be read to troubleshoot connection problems with the predefined server types.

Directory Lists

If the wrong server profile is used to connect to a specific FTP server, the remote directory appears to be empty. First, check the format of the directory lists received from the server. There are two ways to view the directory lists.

The first way is to check Special Files in the Options > File Details. The second possibility is to use the -Z option in the Tun FTP command line. You can then consult the directory lists in the file DIR.DBG in the Tun FTP working directory. You might also be able to obtain information on the type of server by double-clicking the log window (at the bottom of the session window) or by typing the remote command SYST in File > Other Command.

Profile Section

To define a new profile server, create a new key

```
\HKEY_LOCAL_MACHINE\Software\Esker\Tun\8.00\Wftp
```

in the 32-bit Windows registry.

The profile section may contain the following settings:

Profile setting	Description
Name	The profile name
Dir	The field descriptor sequence
SubdirMark	The character used to separate directories in a path name
PathHeader	Cell Body
PathTrailer	The string to be appended to the end of a path name
FileHeader	The string to be inserted between the directory name and the file name
MaskHeader	The string to be inserted between the directory name and a file mask
DefaultMask	The string used as a mask if the server requires one
BlockSize	The number of bytes in a block

The default values for these settings are those used for standard UNIX FTP servers. SubdirMark, FileHeader and MaskHeader have the slash character as default. The PathHeader, PathTrailer and DefaultMask default settings are null. The BlockSize default setting is 512 bytes (not used for UNIX).

Field Descriptor

The FTP client using the field descriptor sequence scans each line of the directory list sent by the FTP server. Each field descriptor in the sequence corresponds to a field in the lines to be scanned. A field descriptor is a letter code:

F	File name
A	File attributes
D	File date and time
U	The user who owns the file
G	The group which owns the file
L	Number of links to the file
S	File size (number of bytes)
B	File size (number of blocks)

The other field descriptors refer to information that can be ignored. The same field descriptor code may appear several times in the sequence, in which case the corresponding fields from the scanned line are concatenated.

Field Separators

By default, a field descriptor matches all the characters of the scanned line up to (but not including) the first blank character encountered (or the end of the line). A blank character or a group of contiguous blanks is matched by a comma or a colon. A comma is used to skip the blanks and a colon is used to place blanks in the output field.

Example

A standard UNIX directory list line looks like this:

```
-rw-r--r-- 2 root system 890 Sep 12 15:24 passwd
```

It contains the following fields:

- File attributes (file type and access rights).
- Number of links to the file.
- User who owns the file.
- Group which owns the file.
- Number of bytes stored in the file.
- Month of the last modification.
- Day of the last modification.
- Time (or year) of the last modification.
- File name.

A simple profile can be created to deal with this kind of FTP server:

```
A,L,U,G,S,D:D:D,F
```

Note that the 3 fields of the scanned line corresponding to the date and time of the last modification have been concatenated using the sequence D:D:D.

Field Descriptor Modifier

You can change field descriptor default behavior by appending a modifier. Four types of modifiers are possible:

- Length modifier.
- Character set modifier.
- Pattern string modifier.
- String constant modifier.

The length modifier is used for fields in which the number of characters is known. The field doesn't have to end with a blank character and may even contain blanks. For example, you can use the field descriptor A10 when the scanned lines have an attribute field of exactly 10 characters. A length of 0 means an unlimited length.

The character set modifier is used when the character set appearing in the field is known. The character set is indicated between square brackets. A caret as the first character of the set means that the field may contain any character except the one(s) indicated in the bracketed group. An interval may be defined by placing a dash between the interval bounds.

The backslash character is an escape character: (\t is a tab character, \] is a square bracket, \- is a dash, \\ is a backslash). The character set modifier may be followed by a length modifier. In this case, the field ends either at the first

scanned character which is not part of the character set or when the given length is reached. Examples of character set modifiers are:

[0-9]	Decimal number
[0-9a-fA-F]	Hexadecimal number
[^ \t]	Every character excluding blanks and tab characters
[rwx\~]9	UNIX simple access rights (read, write and execute)

The pattern string modifier is used to match a string in the scanned line. The complete pattern must appear in the scanned line at the current scan position for the field to be recognized.

A pattern string modifier is indicated between braces. If the pattern string is to contain a closing brace, it must be preceded by a backslash. For example, to test whether a line received by some MS-DOS FTP servers corresponds to a subdirectory or not, you can use the pattern string modifier {<DIR > }.

Typically, a pattern string modifier is used in conjunction with a field descriptor test mark.

The string constant modifier is used to append a string constant to an output field. No scanning is carried out. The string constant is enclosed in double quotes. Double quotes in the string constant must be preceded by a backslash. For example, to insert a dot between the file name and extension when they are received separately from the server, you must use the modified field descriptor f".".

Field Descriptor Test Mark

Finally, you can append a test mark to a field descriptor. Three different test marks are possible:

/	Subdirectory test mark
+	File positive test mark
-	File negative test mark

The subdirectory test mark is used to determine whether or not the scanned line is a subdirectory line. If the scanned field matches the field descriptor, the line is considered as a subdirectory line. The file positive or negative test marks are used to determine whether or not the scanned line is an ordinary file line. For the file positive test mark, if the scanned field doesn't match the field descriptor, the scanned line is considered to be a non-ordinary file line. For the file negative test mark, if the scanned field matches the field descriptor, the scanned line is considered to be a non-ordinary file line.

Before scanning, every line is considered as an ordinary file line. After the scan, lines that are not subdirectories or ordinary file lines are omitted. If the scan results in an empty file name, or the . and .. file names, the line is also omitted.

An exclamation mark following a test mark indicates that the field will be rejected after testing (the field will be re-scanned using the next field descriptor).

Scan Direction

By default, each line is scanned from left to right but the scan direction can be changed by placing a semicolon before the field descriptor.

In the following example, the attribute field and the link field are first scanned from left to right, then the file name field, date field, size field, group field and finally the user field are scanned backwards from the end of the line.

A, L; U, G, S, D, F

Note:

Field descriptor letter codes are not case sensitive. Field descriptors can be separated by blanks (to make them easier to read). If several contiguous field descriptors have the same letter code, all but the first letter code can be omitted (if there's no ambiguity).

For example, the standard UNIX attributes can be defined by the following sequence of three field descriptors:

```
A[d]1/ [\\-]1+ [rwx]9
```

Compatibility

Profile field descriptor sequences from previous versions are fully compatible except for the \$DT field descriptor. The corresponding number of D field descriptors, separated by semicolons, must replace this field descriptor. For example, \$DT3 must be replaced by D:D:D.

The \$ sign placed in front of each profile field descriptor is now ignored.

If semicolons were used in a field descriptor sequence in an earlier profile, it's generally better to replace them with simple commas.

Using the FTP server

Tun Plus implements the full FTP server protocol. The FTP server function enables one PC to export one or more of its directories so that another PC or UNIX machine can read the files contained in them or write files to them. The FTP server function allows a UNIX machine to update files or retrieve files from the PC without the user of the PC having to perform any special operations.

Using the FTP server in a multi-user environment

You can connect to the multi-user server from a multi-user client PC (or from the Citrix/Microsoft TSE server machine itself) in administrator or user mode. The way you use the FTP server depends on the connection mode you use.

In Administrator mode, you can:

- Choose the start mode for the Esker FTPD service, and start and stop this service.
- Define one or more FTPD configurations. Define configuration rights for the ordinary user.

In User mode, you can do one of the following:

- Define one or more FTPD configurations.
- Only view existing configurations.

To use the FTP server in the multi-user environment, you must start the Esker FTPD service on the multi-user server and configure the FTP service with Tun FTPD.

FTP server configuration

Configuring the FTP server consists in specifying one or more directories on the PC, which the user can access from a client FTP application (for example, Tun FTP).

- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > Configuration > FTP Server.

If the FTPD server isn't already running, a dialog offers to start it. If connected as a user, contact the network administrator.

If connected to the server as administrator, the Limited access check box appears. This lets you give users the right to change or only view the FTPD configurations defined by the administrator.

If connected to the server as a user, you can do the following (depending on the access rights the administrator has given you):

- Define FTPD configurations: In this case, follow the instructions below.
- Only view existing configurations: In this case, following a warning message reminding you of your limited access rights, the same dialog as above appears except that Consult replaces Setup.

Notes:

If there are enabled FTPD directories, Tun FTPD proposes to run as a background task (if this isn't already the case) when you activate the dialog box.

Display this dialog by running Tun FTPD and selecting the Setup option in the system menu (select Start > Programs > Esker Tun > Network Resources Access > Local Server Startup > FTP in 32-bit Windows).

Hide the Tun FTPD icon by checking Hidden Server. This reduces the number of icons displayed in the Windows environment when the keystrokes Alt-Tab or Ctrl-Tab are used.

Defining a directory

To define a directory to enable, click New.

Root Directory

Enter the full path name of the Windows directory that to make accessible to an FTP client.

User

Enter the name of the person to authorize to access the exported directory. You can use any character string as long as you communicate it to users who want to access the exported directory.

To provide unlimited access to the exported directory, check Anonymous Login. Consequently, anybody can log in without having to supply a password: They simply enter the user name anonymous.

Password

If access isn't anonymous, associate a password with the authorized user name.

Comments

Enter a brief (optional) description saying why you've exported this directory.

Anonymous Login

This gives unrestricted access to the exported directory. Anyone at all may log on to the server by entering the user name anonymous. The password isn't checked.

Read Only

This limits access to the exported directory to read only. This option is very useful if you allow anonymous logins. It stops users from writing to the exported directory.

Unix Compatible

If selected, the files in the exported directory are displayed in UNIX format. For example:

```
-r--r--r--1 root other 212544 Jun 1410:513270.exe  
-r--r--r--1 root other 130144 Apr 2812:153270.zip  
-r--r--r--1 ftp group 699582 Jun 1414:05euro.zip  
-r--r--r--1 root other 107631 Apr 2519:01httpd.Z
```

Otherwise, the files are displayed in Windows format. For example:

```
3270 EXE 212 544 14/06/95 10:51  
3270 ZIP 130 144 28/05/95 12:15
```

```
EURO ZIP 699 882 14/06/95 14:05
HTTPD Z 107 631 25/04/95 19:01
```

This can be useful for some FTP clients which expect to find a file list in UNIX format. The list, in this case, is interpreted and displayed differently on the screen.

Banner

Click to record texts that are displayed when users log in. The server banner is displayed during login before the requests for the user's identification and password. You can use the banner to supply information on the files in the exported directory, or indicate access restrictions.

Clients

Access to the FTP server can be restricted to a specific number of machines. Click Clients to create or modify the list of IP addresses or machine names authorized to access the exported directory. Machines that aren't in the list don't have access rights. If the list is empty, all connected machines are allowed access.

Private Configuration (except in Citrix/Microsoft TSE version)

Check this to define the exported FTP directory as a private configuration. This means that only the user who configured the FTP directory can export it.

FTP directories configured with this option appear in the list of FTP directories (enabled or disabled) with the comment Private. The other FTP directories appear with the comment Public.

In the list of FTP directories (enabled and disabled):

- FTP directories configured as public are visible to all the users. FTP directories configured as private are only visible to the users who defined them.
- If the Esker FTPD service is started (the FTPD server is running), the administrator can only enable and disable the export of FTP directories defined as public. Ordinary users cannot enable or disable any export of FTP directories.


If the FTPD server was started without the Esker FTPD service (Tun FTPD is started from the Network Resources Access group), the administrator can enable and disable the export of FTP directories defined as public and those defined as private. Ordinary users can only enable or disable the export of directories configured as private.

Defining users' rights in a multi-user environment

In the main Tun FTPD screen, select or clear the Limited Access check box to define users' configuration rights:

- If unchecked, users can declare, modify or delete FTP directories and export them.
- If checked (the default), users can only view the existing FTP directories.

Exporting

To export a FTP directory, select it from the list of directories, and then click . This directory can now be accessed from a client machine if the FTPD server is running.

Execution of the FTP server

The directories and files exported by the FTP server are only accessible to another machine if Tun FTPD is running.

- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > Local Server Startup > FTP.

Note:

The server is running when the program's icon appears in the taskbar.

If you use Tun FTPD regularly, you can copy the program to the Windows Startup Program Group.

Statistics

To view Tun FTPD server statistics, select Tun FTPD > Stat (on the task bar). Alternatively, click Stat in the Tun FTPD configuration dialog box.

The dialog displays information on the requests made by other machines to your FTPD server and also current operations. To view real time update, click Refresh.

Transferring files

To carry out file transfer using Tun FTPD, run the program on another machine, supplying the name and password of the user

VT320 Terminal Emulation

Tun VT320 is a terminal emulation program running on the Windows platform that offers DEC VT320 emulation using standard *telnet* services. If you require a more complete terminal emulation package, with a much larger selection of terminal types, you might consider using Tun EMUL (included in Tun Plus).

Tun VT320 and NIS

Tun VT320 is enhanced by access to the NIS server through the NIS Browser included with Tun applications. This functionality lets you view the servers on the network that are defined on the NIS server. The administrator must have previously configured the NIS server and defined the Servers resource table using the NIS browser. See “The NIS Browser.”

Using Tun VT320

Run the program by clicking Tun VT320 in the Network Resources Access group (Start > Programs > Esker Tun 32-bit Windows).

Enter the name or IP address of the host to connect to, or select it from the scrolling list by clicking the down arrow next to the Host Name field.

This list shows the servers that are declared in the **hosts** file and on the NIS server (NIS Server resources have yellow icons).

Multiple connections

Tun VT320 runs in MDI (Multiple Document Interface) mode. This means that you can open simultaneous emulation sessions on different servers, assuming you've allocated enough TCP connections in your kernel.

Closing sessions

Close a terminal emulation session by choosing File > Close Session. Choose File > Close All Sessions to close all the sessions at once: All open connections are closed when you exit the program.

Terminal options

Changing the display

Choose Settings>Display settings to change the display characteristics of an emulation session.

Screen

Screen size

The default setting for Tun VT320 emulates 80 x 25 screens. You can change this using the Columns Used and Lines Used fields. This is useful for emulating other terminals that use different dimensions (for example, 132 columns or 43 lines).

Typically, Tun VT320 simultaneously memorizes only 25 lines. Change this value in the Lines Memorized field. This lets you scroll the emulation screen backwards using the vertical scroll bar. The maximum value for this field is 2048.

Note:

SystemPC is best suited for 80 columns; Sys132PC works best for 132 columns.

Display Scrollbars

Use the vertical and horizontal scroll bars to access parts of the screen that aren't currently visible. Lines Memorized determines how many lines are stored in the vertical scroll bar's buffer. This is only available if Dynamic Sizing is inactive.

Cursor Coupling

Horizontal Cursor Coupling and Vertical Cursor Coupling let you enable or disable cursor coupling in either direction. Cursor coupling scrolls the screen so that the cursor is always visible. If either box is unchecked, it's possible to move the cursor beyond the view of the terminal window.

Display IME Window at Cursor Position

This opens a window at the cursor position that lets you send Japanese characters. Since it's only useful on Japanese machines, the option is grayed on other types of machine.

Terminal centering

Check Center terminal to center the terminal window in the emulation window. When centered, you can put a frame around it. To do that, check Frame terminal.

Terminal Font

Font Used

You can change the character font used in the terminal display to a font available in Windows. Only non-proportional (fixed) character fonts are available for emulation. We strongly suggest that you use SystemPC and System132, two fonts delivered with Tun VT320 that provide full character sets, including semi-graphic characters, in sizes from 2 to 20 points.

Dynamic Sizing

Select this to always have a full terminal screen in emulation. If you use SystemPC and Sys132PC, you can change the size of the emulation window, and the font size changes accordingly, whether in 80 or 132 columns (with 25 lines).

Attributes

Click this tab to change character style and foreground and background colors.

Use the mouse to select the attribute (normal, reverse video, highlight, etc.) to change, then choose the foreground and background colors. To change the normal character style, select the option desired, italic, bold, or underline, or a combination of all three.

Saving your changes

Click Apply to apply any changes you've made to the current session. To use the same display context the next time you open an emulation session, click Save (in the main Display Settings window). This records the current display options for future connections. Click Load to load previously saved settings.

Emulation options

Choose Settings>Options to change other aspects of the VT320 emulator.

Screen options

- Choose the startup screen size: This can be the maximum possible size, Maximized, the size of the screen on leaving the Previous session, reduction to Icon, or the Default Size indicated on the Terminal Font and Size tab in the Settings > Display Settings dialog box.
- Choose a full-screen display without menus, or other display controls.
- Choose the default screen size for the opening of a new session.

National keyboard

You can change the default keyboard to a different national type. Only the relevant keys are changed; the terminal keys remain the same. Select Auto to use the keyboard type installed in Windows.

Customize

Use this tab to choose a full-screen display without menus.

Session Options

Choose Settings > Session to change the session preferences.

Telnet

This tab lets you change the emulated server in the current session and the port number.

Terminal Setup

- Select a Cursor Style. Choose from a rectangular block or an underlined stroke.
- Set Autowrap Mode to Yes to induce automatic carriage returns if the body of the text is wider than the screen.
- Select the VT Default Character Set, either Dec Graphic or ISO latin-1.
- Select the character used by the BackSpace Key: BackSpace or Delete. This option takes into account the various uses of the backspace key on different host systems. For example, a SUN machine uses the delete character (0x7f) instead of a backspace character ((0x08). Most other machines (SCO, RS/6000, HP...) use the standard backspace key.
- Enter the Number of lines on terminal to be displayed on the emulation window.
- Define the actions associated with the Cursor Keys by selecting a mode in the list: Cursor, Application, or default mode.

Firewall

The firewall option makes connections to the outside safe. Click Options>Firewall.

In the Firewall configuration dialog, check Use a Proxy server.

Enter the name or IP address of the server. Only enter a name if you use a DNS. You can also choose one from the drop-down list (click the down arrow to the right of the field). The list contains the names of the servers listed in the server table (hoststab) and on the NIS server (NIS resources have yellow icons).

Also enter the SOCKS port number (usually the default value 1080).

To avoid using the firewall for local connections, select Do not use for local addresses.

The firewall configuration can be applied to all Tun applications: To do that, check Use these settings for all Tun applications. To reapply the general configuration to all Tun applications, click Restore global settings.

Copy Option

Choose Edit>Copy Option to control CR/LF Conversion, the wait state (useful when Clipboard contents are very large), and rectangular selection of emulation screen areas.

The Wait State (expressed in milliseconds) delays the clearing of the clipboard during a voluminous paste operation. This avoids creating a bottleneck in the communication channel.

Executing Remote Commands

Tun RSH (Windows **R**emote **S**hell) is based on the standard TCP/IP services SHELL (514) and REXEC (512). It was designed to allow users to run simple commands (*lpstat, who, ls, finger...*) or start procedures (backup, SQL requests, man...) on remote servers. The command results may be:

- Viewed in a window.
- Stored in a file on the PC.
- Placed in the Windows clipboard.

Servers may be accessed with or without a password. In the latter case, configure the UNIX host to give the user access rights. See “TCP/IP configuration on a UNIX host” in the manual “Installing and configuring Tun.”

The advantage of running a remote shell command, rather than opening a telnet session, is that connection with the server is only maintained during the execution of the command. It's closed when the command is finished. The program is economical in terms of system and network resources.

With Tun RSH, you can execute commands on one or more remote servers and view the results in a window, without establishing either a telnet or emulation session. In addition, Tun Net's Remote Shell program is completely customizable: You can easily configure frequently used commands.

Tun RSH and NIS

Tun RSH is enhanced by access to the NIS server through the NIS Browser included with Tun applications. This functionality lets you view the network's servers that are defined on the NIS server. The administrator must have previously configured the NIS server and defined the Servers resource table using the NIS browser. See “The NIS Browser.”

Using Tun RSH

Run the program by clicking Tun RSH in the Network Resources Access group (Start > Programs > Esker Tun 32-bit Windows).

When Tun RSH starts, the screen clears and the main application window appears, maximized.

To execute a remote command, first select a server. Choose File > Open Connection:

Host

Enter the name or IP address of the server, or select it from the list (this list contains the servers declared in the hosts file and on the NIS server).

User

Enter the name of the account whose rights to use to access the server. By default, this field already contains the name used during the previous connection.

To be prompted for your password after each command, select the REXEC option. If no password is necessary, clear the REXEC check box. In this case, the UNIX host must be configured correctly to allow access.

When the connection is established, the remote shell screen appears. It contains a button bar which is empty when the program is first started, and two main windows:

- Command Panel: For entering non-interactive commands.
- Result Panel: Displays the results of remote commands.

Multiple connections

Tun RSH runs in MDI (Multiple Document Interface) mode. This means that you can open simultaneous Command Panels on different servers. The Result Panel remains common to all executed commands.

Closing sessions

Sessions automatically close when exiting the program File > Exit.

Command execution

Type a command in New Command, then click Do to send the request.

If the connection information is correct (Host name, User name, etc.) the results of the command display in the Result Panel. An error message displays if there is a connection problem.

Command recall

Show List displays the commands that have already been executed. Use the mouse to select a command from the list instead of retyping it.

Result Panel

By default, command results display in the graphic Result Panel. You may save the information to a disk file or the Windows Clipboard (Options > File or Options > Clipboard). Save As (to a file) and Copy (to the Clipboard) perform the same functions.

Erase the results in the Result Panel after each new command, or append the results of one command after another by choosing Options > Auto-clear.

Customizing Tun RSH

Tun RSH includes a macro to record frequently used commands and sequences.

Defining a macro in Tun RSH

Choose File > Create Macro to define a new macro:

Macro name

Enter a name for the macro to associate it with a button.

Result

Select a destination for the command results, by default, the Result panel. If File is chosen, the File Name field is activated and you can enter the name of the file to write the results to.

Macro

This window lists commands to execute (on one or more servers). Enter the name of the host, the user and the command to be executed. If access to the host normally requires a password, check Rexec.

Click OK. The macro is registered in the lower part of the dialog. OK becomes Execute. You can then decide whether to execute the macro immediately, save it or add it to the toolbar as a button. If you execute the macro immediately, a dialog appears save it.

Adding commands to a macro

To add a new command to the list, click Add, and fill in the Host name, User name, and Command fields.

After adding the commands, save the macro file (with a .MAC extension) by clicking Save As. The name you give it is used when the macro is recalled from within the program.

Tun RSH Macro files created in this manner can be added as buttons to the menu bar (under File). To do this, click OK and select Add Button in the macro editor. The button uses the macro name as a title. There's a limit of eight buttons.

Once defined, the command buttons appear automatically during subsequent program execution. You can change the contents of the menu bar at any time by choosing File > Modify Macro Button or File > Delete Macro Button.

Macro execution

The easiest way to execute macros is to associate them with buttons. You can also choose File > Load Macro to open a macro. Run it by clicking Execute in the Edit Macro dialog.

Opening Tun RSH in button mode

If run with the option -b, Tun RSH opens in button mode. Only the pre-configured command buttons display.

In this case, the only Tun RSH menu options available are File and Help.

All the buttons in the above example are one-line macros created using these procedures. Clicking a command button executes the associated macro.

Remote Command Server

This module is not available in the Tun Plus for Citrix/Microsoft TSE version.

Tun Net and RSHD

A PC can act as a server and allow remote commands to be executed from another PC or a UNIX machine. Tun Net enables a PC to act as an RSH server: One or more machines can be authorized to access it and execute remote commands.

When the Remote Command Server (Tun RSHD) is run on a host PC, it opens two sockets of the port and rexec types. It then remains in listening mode for requests from an authorized RSH client.

Remote authorized users can then execute commands on a PC running the RSH daemon.


Setup

- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > Configuration > Remote Command Server.

If the RSHD server is already running, you can choose Configuration from the program's system menu. To start the RSHD server, choose Start > Programs > Esker Tun > Network Resources Access > Local Server Startup > Remote Command. A dialog appears.

Declare authorized users or machines. Right-click Tun RSHD and choose User or Machine.

Adding a new user

To add a new user, click  or right-click anywhere in the Users windows and choose the New. A dialog appears.


Complete Local Name and Password. A warning message displays if you try to validate the dialog without these fields. Local Name identifies the remote user, as displayed in the Users window:

Remote Name is optional. It adds additional information on, for example, the authorized user's remote machine, as shown above, but it can also be used as an added restriction. If no Remote Name is provided, Tun RSH doesn't implement Remote Name restrictions.

Confirmation is required for the obligatory password.

Current Directory is the default directory in which the authorized user's remote command is executed.


Adding a new machine

Click  and enter the name of the machine or its IP address in the highlighted field beneath the new machine icon. The button bar is inactive until this step is completed.


Note that you can use the wildcard character (*) if you enter an IP address, for example, 194.123.*. Click in an empty part of the dialog box window to validate your entries. The buttons become active again.

The authorized user can then execute remote commands from an authorized PC using Tun RSH or a UNIX machine.

Properties of a machine or user

To examine or modify the Properties of a machine or user, select an icon and click .

Removing a machine or user

To remove a machine or user from the list, select it . Confirmation is always required.

The authorized user can then execute remote commands from an authorized PC using Tun RSH or a UNIX machine.

Options

Click Options. A dialog appears:

Domain Name

Enter the name of the domain from which other users may access the PC running the RSH daemon. You don't have to complete this, but doing so means that authorized users won't have to enter their full IP addresses.

End of Command

In normal circumstances, the second option Timeout is sufficient. When another PC sends a command to the host PC, Tun RSHD waits for the timeout value, in seconds, before it interrupts the connection.

If you select Wait for command to end, Tun RSHD waits until the command has been fully executed before closing the link. However, there's always a risk that, if the command hasn't finished, or there's a problem with the network, the RSH server will be blocked.

This could occur, for example, if the client sent the command *dir /p* to the server and the current directory on the host PC was packed with files. As far as the server is concerned, since it has interrupted the link, any further keyboard activity isn't acknowledged. In this case, you, as the user of the PC host, must stop the server by pressing Alt-Ctrl-Del.

If you select Timeout, the server closes the connection at the end of the timeout, whether or not the command has finished.

Click OK to validate your selection.

Examples

The following are examples of commands executed from a UNIX machine on a PC running Tun RSHD:

```
rsh pcrshd "dir c:\windows > c:\test.txt"
```

This command copies the contents of the directory *c:\windows* on the PC *pcrshd* to a file (on the same PC) called *c:\test.txt*. The user name in this case is the one used to log on to the UNIX machine. This user name, as well as the name of the UNIX machine, must be authorized on the PC "pcrshd".

```
rsh pcrshd "dir c:\windows" > /tmp/test.txt
```

This command is similar to the previous one, except that the destination file is located on the UNIX machine (the redirection operator *>* isn't included in the quotation marks, indicating that the destination file is local).

```
rsh pcrshd -l john dir
```

This command executes a "dir" command on the PC "pcrshd" in the name of the user "john" (local PC name). The remote name of this user must be the one used to log on to the UNIX machine. If no remote name is specified, the command from the user "john" could be carried out using any UNIX login ID.

Remote Backup (32-bit Windows)

Tun TAR for 32-bit Windows provides remote backup in a working environment similar to Windows Explorer.


Remote backup involves two operations: saving files to an archive; and restoring files from an archive.


To use remote backup, you need: A backup device attached to a UNIX server (tape, hard disk, diskette); the command to run the backup or restore job.

Running the application

Select Start > Programs > Esker Tun > Network Resources Access > TCP-IP Utilities > Tape Archive.

Tun TAR opens in backup mode by default (there's a Save To field and a Backup button at the bottom of the screen).

To change to Restore mode, choose File > Restore from the main menu or click Restore Mode  in the toolbar (with a blue arrow pointing upward).

To change back to Backup mode, choose File > Back Up from the main menu or click Backup Mode  in the toolbar (with a red arrow pointing downward).

Managing archives

You can manage the available archives directly from Tun TAR. To create new archives, or change or delete existing archives, choose File > Archive.

The dialog box shows the archives already declared: It lists the archive name, the server it's stored on, the user name used to access it and the backup device used. Each type of archive is represented by an icon:



hard disk.



tape.



floppy disk drive.

If the NIS server is active, the existing NIS archives appear in the archive list. See “The NIS Browser.” If the archive is an NIS archive, it has a yellow icon.

Adding an archive

To add an archive to the list, click Add. A dialog appears:

Archive

Enter the name for the archive.

Name

Enter the name or IP address of the server that the backup device is attached to.

User

You access the server to perform backup operations on the device under a UNIX user name. Enter it in this field.

Protocol

Two communication protocols are used to back up data on the server or receive backed up data from the server.

- RSH lets you perform a backup or restore without a password. You can only use this protocol if the UNIX server has been configured for it: The server must recognize the names of the PC and user performing the operation.
- The REXEC protocol doesn't require previous configuring on the UNIX server: However, you must enter a password each time you perform an archive operation.

Command

You use a UNIX command to transfer characters between the PC and the backup device. The command can be:

- cat
- dd
- or another command if neither of these work.

Example:

```
cat >/dev/rmt0
```

where /dev/rmt0 is the backup device.

```
dd of=/dev/rmt0 obs=200b
```

where obs is the number of bytes read from or written to the backup device.

The cat is by far the most simple and universal. However, it might be the case that it doesn't work on some servers with certain backup devices. In this case dd is a suitable alternative.

In rare cases, the commands cat and dd don't work. You then have to use specific backup and restore commands.

Choose the backup device command to use.

If you choose dd, enter the number of bytes written to, or read from, the backup device in the Block Size field.

If you use a different command, enter the command name for each operation (backup or restore) in the Backup and Restore fields.

Device

Enter the name of the backup device in the Path field (for example, /dev/rmt0). If necessary, look the name up in the documentation for your UNIX server.

Choose the type of medium you're backing up to: Hard Disk, Diskette, or Tape. This displays the appropriate icon for the archive in the archive list.

If you're using a tape, enter the time it takes to rewind in the Rewind Delay field. This is the time Tun TAR waits before performing the backup operation. It gives the tape time to rewind, if necessary.

Modifying an archive

In the Archives dialog, select an archive to modify and click Modify. Refer to the instructions in "Adding an archive" and modify the relevant fields.

You can't modify an NIS archive from Tun TAR for 32-bit Windows. You can, however, view the settings of an NIS archive by clicking View when you select an archive.

Deleting an archive

Select an archive to delete and click **Delete**.

Creating a group of files

Tun TAR for 32-bit Windows backs up and restores groups of files on a UNIX server. A group of files is a selection of the files on the PC you're performing the archive operation from. The files are backed up on (or restored from) the same remote device.

To create a group of files, must select the directories and files in the group. You can select the files directly (by clicking the check boxes beside them) or use filters.

Selecting files

Tun TAR uses tree view (directory hierarchy) and list view (directory contents) displays just like Windows Explorer. Display the directories and files and check those to include in the group.

If you only select a part of a directory, the directory check box is selected but grayed. If checked normally (not grayed) you've included all the subdirectories and files in the group of files.

Example:

In the following example, two subdirectories of the "Tun" directory are selected, "Mail" and "SQL." All the subdirectories and files of "Mail" are selected; and only some of the files in "SQL."

The "SQL" directory check box is selected but grayed. Since all the files in the "Mail" directory are selected, the directory check box contains a check mark and isn't grayed.


File filters

You can use file filters to select files on the basis of different criteria such as:

- Date of last modification.
- File names and types.

You can apply filters at two levels:

- Drive level: The criteria apply to all the directories in the directory tree.
- Directory level: The criteria only apply to the selected directory. They have higher priority than drive level criteria.

To apply drive level file filters, choose Options > General File Filters. To apply directory level file filters, first select the directory in the tree view (it's then highlighted), and choose Options > Directory File Filters, or click .

A dialog appears if you choose Options > General File Filters:

The same dialog displays for directory level filters except for the title "Directory File Filters : xxx," where xxx is the directory name.

To apply filtering on the file time stamp, check Date of Last Modification and enter the dates: Respect the date format indicated (it depends on your Windows configuration).

To show or hide files or types of files in the list view (right pane), enter the details in Include Files: You can use wildcard characters (* for a string of characters and ? for a single character). Separate the file names with semi-colons (;).

Example:

You only want to see files with the extension ".doc" in the application window: Enter ".doc" in the Include Files field.*

To exclude files or types of files from the right pane, enter the details in Exclude Files: You can use wildcard characters (* for a string of characters and ? for a single character). Separate the file names with semi-colons (;).

Example:


You don't want to see files whose extension ends with "xt" in the application window: Enter ".xt" in the Exclude Files field.*

If file filtering (date, inclusion, or exclusion) is applied at directory level, the color of the directory icon changes from yellow to green.

Saving a file set

Once you've selected the files to group, you can perform the backup and quit the application. However, if you later want to perform an archive operation on the same group of files (for example, if you regularly back up the same files), it's recommended to save the files as a set.

You save the files as a set in a file with the extension “.tfs” (Tar File Set). You can also link an archive name with this file. The archive is then automatically selected when Tun TAR loads the file set.

To save a file set, select the files to include in the set and choose File > Save (or File > Save As to save an existing file set under a different name). You can also click . Use a file name with the extension “.tfs.”

Backing up files

By default, Tun TAR opens in backup mode. If you're in restore mode, change to backup mode. You have to select two files to perform a remote backup: the set of files to back up and the backup archive.

Selecting an existing file set

You can open an existing file set (see “Creating a file set”). Do one of the following:

1. Choose File > Open. In the dialog, select the file (with the extension “.tfs”) whose contents to save. Click Open.
2. If you've created a shortcut for Tun TAR on the desktop, you can use the drag and drop feature. Select the .tfs file in Windows Explorer and drag and drop it to the Tun TAR shortcut icon.

You can change the files in the group. You can use file filters to do this.

Backing up a new file set

You can create a new file set when you're backing up files. Follow the instructions in the section “Creating a file set.” You can save the configuration on the local machine and re-use it for future archive operations.

Selecting the backup archive

Choose the archive where to back up the files in Save To.

If the archive to use isn't in the list, you have to create it. Proceed as described under the heading “Adding an archive” in the section “Managing archives.”

It may be the case that when you open a file set the name of an archive appears in the Save To field. This happens if the archive name was saved in the selected .tfs file. Check the archive is the one to use for the backup operation. If it isn't, select a different one as described above.

Performing the backup

When you've selected the files and the archive, click Backup to start the backup operation. A confirmation message appears.

The message shows the overall size of the selected files. Click Yes to start the backup. If you don't want this confirmation message to appear at the start of every backup operation, change the settings (see “Settings”).

Depending on the type of archive selected, you might be asked for a password. This is true for archives that use the REXEC protocol. In this case, enter the user's password for the UNIX server the backup device is attached to. See “Adding an archive” in the section “Managing archives.”

You can view the backup log by splitting the Tun TAR window with the split bar at the bottom. A progress indicator shows the progress of the operation.

Note:

During backup, make sure none of the files being backed up is modified.

Saving the catalog locally

You can save the catalog of the backup you've just made locally. This means you have a local copy of the file list in the archive when you do a restore operation. You don't have to load the catalog from the archive to select the files to restore.

To save the catalog locally, choose File > Save catalog.

Select the directory where to save the catalog, enter the catalog file name with the extension .tcf, and click Save.

Canceling the backup

You can cancel a backup operation that has already started. To do that, click Cancel. A confirmation message displays.

Click Yes to confirm the cancellation, or No to continue the backup.

Restoring files

By default, Tun TAR opens in Backup mode. To change to Restore mode, choose File > Restore. Like backing up, restoring involves two elements: the archive containing the files, and the file set to restore.

Selecting files to restore

To select the files to restore, you must load the archive catalog to view the files in the archive.

If you saved the catalog for the previous backup locally (see “Backing up files” and “Saving the catalog locally”), you can use the local catalog file to select the files to restore. To do that, choose File > Open catalog.

Select the .tcf catalog file to consult.

If you don't have a local copy of the backup file catalog, select the archive to restore files from and click Load catalog (see the next section: Selecting an archive).

The hierarchy of the files backed up in the archive appears in the left pane.

Select the file(s) to restore from the archive.

Selecting the archive

Choose the archive you need for the restore from the Restore From list box at the bottom of the application window.

If the archive you need isn't in the list, you must create it. Follow the instructions given in “Adding an archive” in the section “Managing archives.”

Performing the restore

When you've selected the files to restore, click Restore to start the operation. A confirmation message appears.

Click OK to start the Restore operation. If you don't want this message to appear at each restore, change the program settings (see “Settings”).

You could be asked for a password, depending on the type of archive selected. This applies to archives that use the REXEC protocol. In this case, enter the user password for the UNIX server the backup device is attached to. See “Adding an archive” in the section “Managing archives.”

By default, you can't overwrite a file on the local disk when restoring. You can change the default by choosing Options > Settings. You can also request a confirmation message for the overwrite. If you do, you'll see a confirmation message:

Click OK or All to replace the selected file(s). The restore operation will then begin.

You can view the restore log by splitting the Tun TAR application window in two horizontally. Click the split bar and open the log. A progress indicator shows the progress of the operation.

Canceling the restore

You can cancel the restore operation after it's been started. Click t Cancel while the restore is still being done. A confirmation message appears.

Settings

You can change the backup and restore settings for Tun TAR. To do that, change to the mode (backup or restore) for which to set the settings. Then, choose Options > Settings.

Backup mode settings

In backup mode, you have the following options:

Confirm Backup

If you select this option (the default), a confirmation message appears before backup operations.

Close application on completion

If you select this option (by default, it's not selected), Tun TAR closes automatically after completing the backup operation.

Absolute/Relative Path

Select the path description to include in the backup: Absolute if to back up the files on the UNIX machine with their full path (example: C:\Docs\readme.txt), Relative if to include the relative path, relative, that is, to the current directory (example: readme.txt).

Saving the archive catalog

This option is selected by default. It means the archive catalog is saved at the start of the archive file. The catalog is then quickly loaded during a restore operation: You don't have to browse the backup file.

Restore settings

To restore settings, in restore mode, select Options > Settings.

Confirm Restore

This option is selected by default. A confirmation message precedes the start of the restore operation.

Close application on completion

If this option is selected (by default, it's not), Tun TAR closes automatically after the restore.

Original Location

This option is selected by default. When it's selected Tun TAR restores the selected files to their original location on the PC.

New Location

If this option is selected (by default, it's not), you must specify a location (target directory) for the restored files. By default, the Use Directory Names is checked: The files are restored to the target directory with the original subtree (if applicable). If you don't want to restore the backed up subtree below the target directory, clear this check box. The files are then restored directly to the target directory and no directory hierarchy is used.

Enter the target directory for the restore in the field beside the Browse button. Click this button to browse directory hierarchies and select a directory. This dialog appears:

Choose the target directory and click OK.

Allow Overwrite

By default, a restore doesn't overwrite existing files. You can select this option and specify the overwrite options. Overwriting, by default, is only authorized for older copies of the file (Overwrite Old Files is selected). You can overwrite all the files, irrespective of their dates, by selecting Overwrite All Files.

In each case, a confirmation message is displayed. Uncheck Confirm Overwrite to hide this confirmation message.

Printing

You can print the contents of the current file set and log.

Print Setup

Choose File > Print Setup to select the print settings for the jobs you print from Tun TAR.

Select the printer in the Name list box. Click Properties to change the printer's properties, if necessary.

Select the paper size and source (in the Size and Source fields) and the orientation (Portrait or Landscape).

Printing

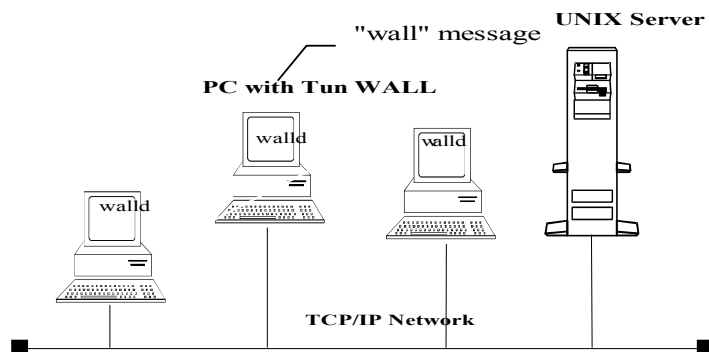
To print the contents of a file set, click the upper part of the window with the file set (left pane) and choose File > Print Selected Files. If the option is inactive, it's because no files are selected or you haven't clicked in the right place.

To print the current log, click the lower part of the window (where the log appears) and choose File > Print Report. If the option is inactive, it's because the lower part of the window is inactive (you haven't clicked in it).

When you've chosen an option, complete the dialog, if necessary (see "Print Setup" above), and click OK.

WALL and WALLD

WALL (Write to all) is a utility for sending messages to some or all of the other PCs and UNIX servers on the network. You might want to warn the other users immediately, for example, of particular events (stoppage of a server, closure of a DBMS, backups....) Users who want to receive messages sent by Tun WALL must have Tun WALLD running on their machines.



Sending a message

Run the program by clicking WALL in the Network Resources Access group (Start > Programs > Esker Tun in 32-bit Windows.)

Message composition

Subject

Enter the subject of the message in this field. This isn't obligatory but it gives the recipients a general idea of the message.

Message

The message area is designed to hold short messages only.

Transmission mode

Tun WALL uses the UDP protocol to communicate with Tun WALLD installed on other PCs.

However, Tun WALL can also send messages to UNIX servers using the standard RPC protocol.

You have the choice of sending messages to PCs running Tun WALLD (UDP protocol), UNIX servers (RPC protocol), or both types of system.

When you send a message, choose the protocol used by the recipients from the Options menu.

- Walld (UDP): Recipients are on PCs.
- Walld (RPC): Recipients are on UNIX machines.
- Walld (UDP & RPC): Both types of recipient.

Selecting recipients

By default, all the users with Tun WALLD running on their machines receive the message (the default protocol is UDP).

You can send the message only to selected recipients.

To do that, choose Options > Choose Recipients from the main menu.

Depending on the protocol you've chosen, the recipient list includes:

- Only PCs with Tun WALLD running (UDP).
- Only UNIX machines (RPC).
- Both UDP and RPC servers.

When you choose both protocols as in the above screenshot, the Walld and RPC columns show the type of server used:

Walld	Rpc	Server type
x	-	PC running Tun WALLD, version 8.50 or earlier.
-	x	UNIX machine.
x	x	PC running Tun WALLD, version 8.60 (RPC port 700).

Click the server (PC or UNIX) to send the message to.

To select consecutive servers, hold the Shift key down when you click. To select servers that aren't consecutive in the list, hold the Ctrl key down when you click.

You can select all the names by clicking Select All. Click Clear All to clear (deselect) all the names.

Click OK when you've finished. If you didn't select any servers in the list, the default, Send to all is used.

The chosen recipients are listed instead of Send to all.

Click Send to send the message to the selected users. The message is immediately displayed on the selected machines.

The information area

The lower part of the window provides information on the message's reception: That is, if the message was received by the recipients and if a reply is being prepared.

Read	Answer	
-		Received but not acknowledged
x	-	Read and acknowledge
x	x	Read with answer pending

A “-” in the Read column indicates that the message was received but wasn't acknowledged (read) by the recipient.

An “x” in the Read column and a “-” in the Answer column indicates that the message was and acknowledged (read) by the recipient. He or she isn't preparing an answer to the message.

An “x” in both the Read and Answer columns indicates that the message was received and acknowledged (read) by the recipient and that he's preparing an answer.

Receiving a message

You can only receive messages if the Tun WALLD server is running on your PC. Run it by clicking WALLD in the Network Resources Access group (Start > Programs > Esker Tun in 32-bit Windows).

When you send a message with Tun WALL, A dialog appears on the recipient machines with Tun WALLD running. After reading the message, the recipient can acknowledge it by clicking OK or answer by clicking the Answer button. If you send a message from a UNIX machine (RPC message), the same dialog appears on users' machines with Tun WALLD running, only the Answer button is inactive (grayed).

Answering a message

Click Answer to acknowledge reception of a message and answer it directly. Use the dialog box that's displayed to write and send your answer.

The answer is only sent to the sender of the original message.

Tun Accessories

This module is not available in the Tun Plus for Citrix/Microsoft TSE version. The Tun Accessories available are:

- Tun TFTP
- TIME

Tun TFTP

Tun TFTP can operate simultaneously in Client and Server mode. By default, Tun TFTP functions in client mode only. By using the option `-s` on the command line, you can run Tun TFTP in both client and server mode. With the command line options `-s` and `-h`, you can run Tun TFTP in server mode only.

- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > TCP/IP Utilities > TFTP.

NIS configuration

To access an already defined TFTP configuration, select Read Through NIS in the context menu (right-click the Tun TFTP icon in the taskbar). A dialog appears.

Select the TFTP configuration of your choice.

New configuration

To configure Tun TFTP, select the Configuration in the context menu (right-click Tun TFTP in the taskbar). A dialog appears.

The dialog shows the default settings. These values are suitable for the majority of cases. In the above example, an error message will be displayed three times after a delay of 5 seconds, and will be repeated 3 times. You can change these values to suit your needs.

Check Show error messages if to be informed of any possible errors (for example, if a file is being transferred in background mode). This option is recommended in Client mode. In Server mode, however, it's better not to select it since any unsuccessful access to the TFTP server provokes an error warning.

Read/write

To use Tun TFTP, choose Read/Write from the context menu (right-click the Tun TFTP icon). A dialog appears.

Type of transfer

Select the type of transfer desired: Read to transfer a file from the remote host, or Write to send a file to the remote host. The Wait for end of transfer check box indicates that the transfer is performed in synchronous mode: In this case, the dialog box remains on the screen for the duration of the operation. If the check box isn't selected, the transfer is performed in asynchronous mode. The dialog box is cleared from the screen at the start of the transfer operation and another transfer can immediately be started.

There's a risk that you won't be informed of possible errors if a file is being transferred and the Wait for end of transfer and Show error messages check boxes (in the settings dialog box) aren't selected. Therefore, if the Wait for end of transfer is unchecked, check Show error messages.

Remote host

Enter the name or the IP address of the remote machine.

Source file/Destination file

You must know the source and destination file names of the file to send or receive. Enter these with the full file path names and click OK to start the transfer. The transfer is only performed in binary mode.

Security

The fact that there's no user authentication means that the network administrator has to take special measures to protect the system from inexperienced or mischievous hands. There's a danger that a remote intruder could obtain host system files (for example, /etc/passwd) or overwrite existing files.

If there's a risk, restrict access to a subtree of the host file system, or run the Server in safe mode with the option -s.

On the UNIX server, you can set the "rwx" permissions appropriately for other groups to control access.

TIME

To use the TIME utility:

- In 32-bit Windows, select Start > Programs > Esker Tun > Network Resources Access > TPC/IP Utilities > Time Client.

Configuration

To configure Tun SNTP, choose Setup from the context menu (right-click Tun SNTP on the taskbar). A dialog appears.

The edit fields contain the default values (suitable for most cases).

Default parameters

To copy the server's date and time to the PC, complete the default parameters in the dialog box.

Enter the name or IP address of the server.

Next select the type of protocol used by the server (UDP/Time or SNTP).

Enter the frequency with which the server is to be queried for the time (in seconds). If the frequency is zero, the server isn't queried for the time automatically. If the frequency isn't zero, for example 3600 seconds, the date and the time on the PC is automatically updated (every hour in this case).

Error parameters

The lower half of the dialog box displayed is similar to that of the TFTP program.

Click OK for the parameters to take effect. If you selected a server, your PC copies the date and time of this server.

Read date and time

To read a server's date and time, choose Read date and time from the context menu (right-click the Tun SNTP icon in the taskbar). A dialog appears.

NIS

You can also set the time by using the NIS Browser > Servers table. Click a server icon with the right mouse button. If a Time/SNTP server is running on that particular host, the menu option Time / Sntp > Time is activated and gives the same results. See "The NIS Browser"

Tun Accessories and NIS

The Tun Accessories are enhanced by access to the NIS server through the NIS Browser included with Tun applications. This functionality lets you view the servers and TFTP configurations on the network that are defined on the NIS server. The administrator must have previously configured the NIS server and defined the Servers and TFTP Files resource tables using the NIS browser. See “The NIS Browser.”

References

INDEX

WADM2.EXE	Tun NET administrator.
WADM2_32.EXE	
WALL.EXE	Communication utility for sending short messages.
WALL32.EXE	
WALLD.EXE	WALL agent.
WALLD32.EXE	
WFTP.EXE	File transfer using FTP services
WFTP32.EXE	
WFTPD.EXE	FTP server.
WFTPD32.EXE	
WLPD.EXE	Sharing PC printers.
WLPD32.EXE	
WMOUNT.EXE	Drive mounting utility.
Wmnt32.EXE	
WNFSD.EXE	NFS server.
WNFSD32.EXE	
WNISS.EXE	Network Information Service application.
WNISS32.EXE	
WPING.EXE	Connection test using UDP and ICMP protocols.
WPING32.EXE	
WRSH.EXE	Command execution on a remote server using RSH or REXEC.
WRSH32.EXE	
WRSHD.EXE	Remote command server.
WRSHD32.EXE	
WSNTP.EXE	Time applet: Sets PC time to the selected host's time.
WSNTP32.EXE	
WTAR.EXE	Backup and restore on remote devices.
WTAR32.EXE	
WTFTP.EXE	File transfer using the trivial file transfer protocol.
WTFTP32.EXE	
WUMOUNT.EXE	Drive unmounting utility.
WUmnt32.EXE	
WVT320.EXE	Terminal emulation in DEC VT320 mode over TELNET services.
VT320_32.EXE	

Note:

If you use the Citrix/Microsoft TSE version of Tun, only the WADM2_32.EXE, WALL32.EXE, WALLD32.EXE, WFTP32.EXE, WFTPD32.EXE, WLPD32.EXE, WMNT32.EXE, WNFSD32.EXE, WPING32.EXE, WRSH32.EXE, WTAR32.EXE, WUMNT32.EXE and VT320_32.EXE files are available. The options relative to the NIS feature are not operational.

WADM2

Tun NET Administrator.

Syntax

wadm2_32 in 32-bit Windows

Description

WADM2.EXE (WADM2_32.EXE) is the Network Resources Access administration program for the Tun NFS, Tun LPR, Tun FTPD, Tun NFSD, Tun LPD, Tun RSHD and Tun NIS applications.

WALL

Communication utility for short messages.

Syntax

wall32 [-m] in 32-bit Windows

Description

WALL.EXE (WALL32.EXE) is a communication utility for short messages for users on the same network.

The command line option for WALL.EXE (or WALL32.EXE) is:

-m Maximizes screen at startup.

WALLD

WALL agent.

Syntax

walld32 [-h] [-q] in 32-bit Windows

Description

WALLD.EXE (WALLD32.EXE) is the daemon that receives messages sent by WALL.

The startup options for WALLD.EXE (WALLD32.EXE) are:

-h	Hides the program icon.
-q	Displays the program icon if the program has been run with the parameter -h.

WFTP

File transfer using standard FTP services.

Syntax

```
wftp32 [-c"config"] [-k"Niskey"]
[-m"macro_file"] [-t"number"]
in 32-bit Windows
```

Description

WFTP.EXE (WFTP32.EXE) offers an intuitive graphical interface to the standard file transfer protocol (FTP) over TCP/IP.

The startup options are listed below:

-c"config"	Configuration name.
-k"Niskey"	Launches the program from a NIS configuration.
-m"macro_file"	Launches the program from a NIS configuration.
-h	Hidden mode (used with -m)
-t"number"	Tests a profile identified by its number.

WFTPD

FTP server.

Syntax

```
wftpd32 in 32-bit Windows
```

Description

WFTPD.EXE (WFTPD32.EXE) enables a PC to act as an FTP server.

WLPD

PC printer sharing.

Syntax

```
wlpd32 [-rcmd] in 32-bit Windows
```

Description

WLPD.EXE (WLPD32.EXE) lets a PC share its printer with other machines on the network.

The command line option for WLPD.EXE (WLPD32.EXE) is:

-rcmd frees the RSH port if printer sharing doesn't use it, so as to use this port with other programs.

WMOUNT

Drive mounting utility.

Syntax

```
wmnt32 [-c"name"] [-d"disk"] [-k"Niskey"]
[-n"name"] [-p"password"] [-r"directory"]
[-u"user"] [-v] [-w]
```

in 32-bit Windows

Description

WMOUNT.EXE (WMNT32.EXE) mounts network drives.

The command line options for WMOUNT.EXE (WMNT32.EXE) are:

-c“name”	Configuration name for the mount (excludes the use of -w and -k, used with -r).
-d“disk”	Name of the local drive to mount (for example, -dE).
-k“Niskey”	Mounts a drive from an NIS resource (excludes the use of -r and -n).
-n“name”	Mounts a drive from a saved NFS configuration (excludes the use of -r and -k).
-p“password”	Password (used with -u).
-r“directory”	Mount directory (for example, “\\pc01\temp” in Workgroups, “mechin:/temp” in NFS).
-u“user”	User name.
-v	Verbose mode.
-w	Workgroup path type (used with -r).

WNFSD

NFS server.

Syntax

wnfsd32 in 32-bit Windows

Description

WNFSD.EXE (WNFSD32.EXE) enables a PC to act as an NFS server.

WNISS

Network Information Service.

Syntax

```
wniss32 [-k“Niskey”] [-y14] [-y15] [-o“file”]
```

```
[-s“file”] [-v]
```

in 32-bit Windows

Description

The Network Information Service (NIS) lets you access and administrate network resources. The program provides an efficient, user-friendly graphic interface between the PC and the UNIX yp tables.

The command line options for WNISS.EXE (WNISS32.EXE) are:

-k"niskey"	NIS resource (excludes the use of -o and -s, must be used with -y).
-y14	The NIS resource is an application (excludes the use of -y15, used with -k).
-y15	The NIS resource is an object (excludes the use of -y14, used with -k).
-o"file"	Object path (excludes the use of -s and -k).
-s"file"	Path to a script or executable (excludes the use of -o and -k).
-v	Verbose mode.

WPING

Tests network connections.

Syntax

```
wping32 [-h"hostname"] [-k"niskey"] [-u] [-i]
in 32-bit Windows
```

Description

WPING.EXE (WPING32.EXE) tests connections between PC and servers by sending and receiving UDP or ICMP packets.

The command line option of WPING.EXE (WPING32.EXE) is:

-h"hostname"	Starts Tun PING and pings the host "hostname .
-k"niskey"	Starts Tun PING with a connection to an NIS-defined server.
-u	Selects UDP as the echo type
-i	Selects ICMP as the echo type

WRSH

Command execution on a remote server using RSH or REXEC.

Syntax

```
wrsh32 [-b] [-c] [-e"command"] [-f"file"]
[-h"server"] [-k"niskey"] [-m"macro_file"] [-t]
[-u"user"] [-p"password"] [-x] [-v]
in 32-bit Windows
```

Description

WRSH.EXE (WRSH32.EXE) executes commands on a remote server and displays the results in a graphic window. This application is based on the standard RSH and EXEC services.

The startup options are as follows:

-b	Toolbox mode.
-c	Output placed on the Clipboard (cannot be used with -f).
-e"command"	Command to execute (can be used with -u, -h and possibly -x, -c, -f, and -t).
-f"file"	Output written to file (cannot be used with -c).
-h"server"	Server name (used with -u).
-k"Niskey"	For connection to an NIS server.
-m"macro_file"	Macro to be executed with its path (.mac) (can be used with -t, -c, and -f).
-t	Exits wrsh after a command or a macro (can be used with -m or -e).
-u"user"	User name (used with -h).
-p"password"	Password (used with -u).
-x	"Rexec" protocol (the default is "RSH").
-v	Verbose mode.

WRSHD

Remote Command Server.

Syntax

wrshd32 in 32-bit Windows

Description

When the Remote Command Server (WRSHD.EXE (WRSHD32.EXE)) is run on a host PC, it opens two sockets of the port and rexec type. It then remains in listening mode for requests from an *authorized* RSH client.

Remote authorized users can then execute commands on a PC running the RSH daemon.

WSNTP

Sets the PC clock to the time on a UNIX host.

Syntax

```
wsntp32 [-?] [-a"interval"] [-h] [-k"Niskey"]
```

```
[-s] [-r"server"] [-t] [-v]
```

in 32-bit Windows

Description

WSNTP.EXE (WSNTP32.EXE) makes the time on the local PC correspond to that of the chosen server.

The startup options are listed below:

-?	Help with the parameters.
-a“interval”	Time interval (in seconds) between each setting of the time.
-h	Invisible mode (can be used with -a and -r or -k, can't be used with -s).
-k“Niskey”	Setting of the time on the PC from an NIS server.
-s	Visible mode.
-r“server”	Name or IP address of the server.
-t	“Time” protocol (the default is “SNTP”).
-v	Verbose mode.

WTAR

Backup and restore on remote peripheral devices.

Syntax

```
wtar32 [-a“archive_name”] [-d“target_path”]
[-k“Niskey”] [-m“macro_file”] [-p“macro_file”]
[-t]
```

in 32-bit Windows

Description

Based on the standard SHELL service, WTAR.EXE (WTAR32.EXE) performs file backup and restore operations using remote resources.

The startup parameters are as follows:

a“archive_name”	Name of the archive to use.
-d“target_path”	Target path for the restored archive (can be used with -m).
-k“Niskey”	Use an NIS archive at startup.
-m“macro_file”	Macro file to execute (can be used with -d and -t).
-p“macro_file”	Same as -m (obsolete, included for backward compatibility).
-t	Terminates wtar after execution of a macro.

WTFTP

File transfer using standard TFTP services.

Syntax

```
wtftp32 [-a] [-h] [-k“Niskey”] [-l“file”]
[-m“server”] [-r“file”] [-s“directory”] [-v] [-w]
```

in 32-bit Windows

Description

The implementation of the TFTP protocol is restricted to the transfer of one file at a time in synchronous mode. TFTP is often used for booting terminals simply and efficiently on sites with only a few terminals or for feeding system files to network devices.

The startup options for Tun TFTP are:

-a	Visible mode.
-h	Hidden server mode.
-k"niskey"	File retrieval from an NIS resource (can't be used with -r, -l and -m).
-l"file"	Local file name (used with -m and -r).
-m"server"	Remote server name (used with -l and -r).
-r"file"	Remote file name (used with -l and -m).
-s"directory"	Without this option, the TFTP server searches the files in its startup directory. This option allows to specify another directory than the TFTP server one.
-v	Verbose mode.
-w	Writes from the local to the remote machine (the default is from the remote to the local machine, used with -m).

WUMOUNT

Driver unmounting utility.

Syntax

```
wumnt32 [-d"disk"] [-k"niskey"] [-n"name"] [-v] [-x]  
in 32-bit Windows
```

Description

WUMOUNT.EXE (WUMNT32.EXE) uninstalls network drives.

The WUMOUNT.EXE (WUMNT32.EXE) command line options are:

-d"disk"	Name of the local disk to uninstall (for example, -dE).
-k"niskey"	Uninstalls a drive from an NIS resource (can't be used with -n and -d).
-n"name"	Uninstalls a drive from a saved NFS configuration (can't be used with -k or -d).
-v	Verbose mode.
-x	Deletes the NFS configuration (used with -n).

WVT320

Terminal emulation in DEC VT320 mode over standard telnet services.

Syntax

```
vt320_32 [-h"server"] [-s"service"]  
in 32-bit Windows
```

Description

This program gives Tun Net users access to basic terminal emulation functions, primarily for configuring UNIX hosts. The startup options are as follows:

- h "server" Name or IP address of the server. Connection is established immediately on startup.
- s "service" Service number used to establish the TELNET connection (by default 23).

Tun FTP macro commands

Index

aget	Initiate file transfer from the host machine to the local machine in ASCII mode.
append	Add the contents of a local file to the end of an existing file located on a remote host.
aput	Transfer files from the local machine to the host machine in ASCII mode.
ascii	Change default transfer mode to ASCII mode.
bget	Copy a file from the host machine to the local machine in binary mode.
binary	Change the default transfer mode to binary.
bput	Transfer a file from the local machine to the host machine in binary mode.
ClearMessage	Erase all messages in the execution window.
debug	Write a .log file with messages sent to FTP.
delete	Delete a file on the server.
Dos	Execute a DOS command.
drive	Select a new current drive on the local machine.
Echo	Display a character string in the execution window or in a specified message box.
Exit	Unconditional exit from a macro.
fcd	Change the current directory on the server.
get	Copy a file from the server to the local machine.
Goto	Unconditional branch to a label.
HideMessage	Hide messages in the macro execution window.
Host_text	Set the server's charset.
IfConnected	Test if the local machine is connected to a server.
IfEqual	Test a variable or most recent FTP response for equality.
IfError	Test the result of the most recent command.
IfNoEqual	Test a variable or the most recent FTP response for inequality.
IfNoError	Test the result of the most recent command.
Label	Define a label.
lcd	Select a new current directory on local machine.
local	Set word size on the local machine.
login	Establish connection with a server.
logoff	Close the current connection.
mdelete	Delete one or more files on the server.
mget	Copy one or more files from the server to the local machine.
mkdir	Create a directory on the server.
mput	Copy one or more files from the local machine to the server.
option	Set an option.
Pause	Wait one second.

parent	Change to the parent directory on the server.
put	Copy a file from the local machine to the server.
ReadVar	Enter a character string in a dialog box and assign it to a variable.
ReadPasswd	Enter a character string and assign it to a variable without displaying the characters.
rename	Change the name of a file on the server.
rmdir	Remove a directory on the server.
Set	Define and assign a variable.
Server	Execute a UNIX FTP command.
ShowMessage	Display the macro-execution window.
stat	Check if FTP responds to commands (testing for possible disconnection).
text_codes	Set the text formats for the local and remote files.
Title	Assign a title to the macro execution window.
verbose	Display or hide messages.

aget

Copies a file from the server to the PC in ASCII mode.

```
aget remote_file [local_file]
```

remote_file	Name of the file to transfer.
local_file	Name the file takes on the PC. If not given, the file has the same name as it did on the server.

ASCII mode converts UNIX LF characters into CR/LF in Windows.

See also: aput, bput, bget, ascii, binary, text_codes

append

Adds the contents of a local file to end of a remote file.

```
append local_file remote_file
```

local_file	Name of the local file to send. The current filter (ascii, binary, iso) is applied.
remote_file	Name of the file to which the local file is appended.

aput

Copies a file from the PC to the server in ASCII mode.

```
aput local_file [remote_file]
```

local_file	Name of the file on the PC.
remote_file	Name for the new file on the server. If not specified, the name is the same as it was on the PC.

This transfer mode converts Windows CR/LF characters into LF on the UNIX host.

See also: aget, bput, bget, ascii, binary, text_codes

ascii

Sets the transfer mode to ASCII.

```
ascii
```

When this command is executed, the put and get commands transfer files in ASCII mode (with conversion of LF to CR/LF and vice versa).

See also: binary, text_codes

bget

Copies a file from the server to the local PC in binary mode.

```
bget remote_file [local_file]
```

remote_file	Name of the file to transfer from the server.
local_file	Name for the new file on the PC. If not specified, the file name is the same as it was on the server.

This transfer mode doesn't perform any LF to CR/LF conversion.

See also: aput, aget, bput, ascii, binary

binary

Sets the transfer mode to BINARY.

```
binary
```

When this command is executed, the put and get commands transfer files in BINARY mode (without any conversion of LF to CR/LF or vice versa)

See also: ascii

bput

Copies a file from the PC to the server in binary mode.

```
bput local_file [remote_file]
```

local_file	Name of the file on the PC.
remote_file	Name for the new file on the server. If not specified, the name is the same as it was on the PC.

This transfer mode doesn't perform any CR/LF to LF conversion.

See also: aget, aput, bget, ascii, binary

ClearMessage

Erases any messages in the application execution window.

```
ClearMessage
```

See also: Echo

debug

Displays messages sent by the application to the FTP server.

```
debug on|off
```

Messages can be sent to the execution window and/or to a .log file according to the parameters passed to the verbose command.

See also: verbose

delete, mdelete

To delete one or more remote files.

```
delete "remote_file"  
mdelete file1 [file2....]
```

Dos

Execute a DOS program during the FTP session.

```
Dos "pif_file"
```

This command can be used to run .pif files that call .bat, .com and .exe programs.

drive

Changes the current local drive on the PC.

```
drive x:
```

Echo

Displays a message in the execution window or in a specific dialog box.

```
Echo message [-b [title]]
```

This command displays messages on the screen while the program is running.

-b Sends the message to the dialog box specified in the character string following the option ([title]).

See also: ClearMessage

Exit

Unconditional exit from the macro.

```
Exit
```

fcd, parent

Changes the current directory on the remote machine (foreign change directory).

```
fcd directory  
parent
```

The parent command is equivalent to "cd ..".

See also: lcd

get, mget

Copies one or more files from the server to the local PC:


```
get remote_file [local_file]
mget file1 [file...]
```

remote_file	The name of the file or files to transfer from the server.
local_file	The name for the new file or files on the PC. If not specified, the file names are the same as they were on the server.

This transfer mode uses the current conversion filter (as given by the commands: `ascii` and `binary`).

With `mget`, the files have the same names on the PC as they did on the server. You can also use wildcard characters (* and ?).

See also: `put`, `ascii`, `binary`, `text_codes`

Goto

Unconditional branch to a LABEL.

```
Goto label
```

See also: `Label`

Hide & ShowMessage

Show or hide messages during execution.

```
HideMessage
```

```
ShowMessage
```

These commands determine if messages are displayed while macros are running.

See also: `ClearMessage`, `Echo`

host_text

Sets the charset used by the server.

```
host_text serveur_charset
```

serveur_charset is the character coding used on the remote machine. Here's the list of recognized formats:

Dos

Windows

Iso-8859

Shift-Jis

Euc

Jis

Unicode

Ebcdic

Cp437

Cp850

Cp860

Cp861

Cp863
Cp865
Cp1250
Cp1251
Cp1252
Cp1253
Cp1254
Cp1255
Cp1256

IfConnected

Checks to see if the application is still attached to the server.

```
IfConnected label | exit
```

This command is used to test if the FTP connection is still valid. If confirmed, the program can branch to an exit command or to a LABEL.

IfEqual, IfNoEqual

Tests the value of a variable or the most recent FTP command for equality or inequality.

```
IfEqual "value" [Variable] label | exit
```

```
IfNoEqual "value" [Variable] label | exit
```

This command can be used as a conditional branch to a LABEL or an exit command.

Example:

```
mput *.bat  
IfEqual "226" OK  
Echo "Error" -b  
logoff  
exit
```

```
label OK  
Echo "Successful"  
logoff  
exit
```

See also: IfError

IfError, IfNoError

Tests the results of the most recent FTP command.

```
IfError label | exit
```

```
IfNoError label | exit
```

Example:

```
mput *.bat  
IfError ERROR  
Goto OK  
label ERROR
```

```
Echo "Error" -b
logoff
exit
label OK
Echo "Successful"
logoff
exit
```

See also: IfEqual

Label

Defines a label.

```
Label name
```

Labels are used to branch from IfError, IfEqual, IfConnected, and Goto instructions.

See also: Goto

lcd

Changes the current directory on the local PC (local change directory).

```
lcd directory
```

See also: fcd

local

Defines word size on the PC.

```
local size
```

login

Establishes a connection with an FTP server.

```
login hostname username passwd [service_no]
```

hostname	Name of the FTP server.
username	User's account name.
passwd	Password for the user's account.
service_no	Default service number (21).

You can replace any of the above parameters with variables in a macro.

IfError can be used to test the results of a login command.

See also: logoff

logoff

Closes a connection with an FTP server.

```
logoff
```

See also: login

mkdir, rmdir

Creates or removes a directory on the server.

```
mkdir directory
```

```
rmdir directory
```

put, mput

Copies one or more files from the PC to the server.

```
put local_file remote_file
```

```
mput file1 [file2...]
```

local_file	Name of the file or files to transfer from the PC.
remote_file	Name for the new file or files on the server. If not specified, the file names are the same as they were on the PC.

This transfer mode uses the current conversion filter, as given by the commands: `ascii`, `binary` and `iso`.

With `mput`, file names are the same on the server as they were on the PC. You can also use wildcard characters (`*` and `?`).

See also: `mget`, `get`, `aget`, `bput`, `bget`, `ascii`, `binary`, `text_codes`

option

Changes local FTP options.

```
option casehack|ask|pathack on|off
```

casehack	When on, converts default remote filenames to lower case.
ask	When off, doesn't prompt user during <code>mget</code> and <code>mput</code> operations.
pathhack	When on, strips paths of default remote filenames.

Pause

Waits for a period of time specified in seconds.

```
Pause nbsec
```

ReadPasswd, ReadVar

Reads a character string and assigns it to a variable.

```
ReadVar message variable [title] [-o|-y]
```

```
ReadPasswd message variable [title]
```

This command displays the text of `message` in a dialog box, and waits for the user to enter information (which is assigned to `variable`). The name of the variable must not be preceded by a `$`.

title	Assigns a title to the dialog box.
-o	Puts OK and Cancel buttons in the dialog box. The title of the selected button is stored in the variable.
-y	Only the message and the buttons Yes and No are displayed. The title of the selected button is stored in the variable.

ReadPasswd works the same as ReadVar, but the characters entered by the user aren't displayed.

See also: Echo

rename

Changes the name of a remote file.

```
rename remote_file new_file_name
```

Server

Executes a UNIX FTP command.

```
Server "command_name"
```

This statement executes a UNIX command on the FTP server (just like the Tun FTP option File\Other command). Some UNIX FTP commands have an equivalent in Tun FTP's macro language (for example, the UNIX commands RNFR and RNT0, which rename files, are equivalent to the Tun FTP macro command RENAME). Other commands that are system-specific don't have an equivalent. This statement is useful for those commands.

Example:

```
Server "Site umask 111"
```

runs the command site umask in a macro.

Set

Creates and assigns a new variable.

```
Set variable "string"
```

This command assigns a character string to a variable. The name of the variable mustn't be preceded by a \$.

See also: ReadVar, ReadPasswd

stat

Shows server status.

```
stat
```

text_codes

Sets the text format for local and remote files.

```
text_codes local_file_format remote_file_format
```

See also: get, aget, put, aput, ascii, binary, host_text

Title

Assigns a title to an application execution window.

```
Title "string"
```

See also: HideMessage, ShowMessage

verbose

Tells FTP whether to be talkative or not.

Network Resource Access

`verbose on|off [filename] [-s|-f|-b]`

-
- `on` Displays FTP messages.
 - `-s` Messages are displayed in the program execution window.
 - `-f` Messages are sent to the file given by filename. If no file name is given, messages are written to ftp.log by default.
 - `-b` Writes FTP messages in both the window and a file.
-

See also: debug

Index

A

Account (FTP), 54
ASCII (FTP), 54, 57
Automatic connection at startup (FTP), 53

B

Backing up files, 94
Backspace key (in telnet), 83
Binary (FTP), 54, 57

C

Citrix/Microsoft TSE (FTPD), 77
Citrix/Microsoft TSE (LPD), 49
Citrix/Microsoft TSE (NFSD), 41
Commands (FTP), 54, 57, 59
Connection
 Customization, 54, 55
 Disconnection, 55
Container, 53

D

Data Transfer (FTP), 54
Data Type (FTP), 54

E

Encryption (FTP macros), 58
EScript
 FTP, 58
Esker FTPD, 77
Esker LPD, 49
Esker NFSD, 41
Exporting an NIS configuration, 14

F

Field descriptors (FTP profiles), 59, 60
Field separators (FTP profiles), 59, 62
Files
 .js file, 58
 .mac file, 58
 .vbs file, 58
 /etc/exports file, 32
Filters (Tun TAR), 93
FTP
 Account, 54
 API, 58
 ASCII, 54, 57
 Automatic Connection, 53
 Binary, 54, 57
 Browsing remote file systems, 55
 Commands, 54, 57
 Connection settings, 53

Data Transfer, 54
Data Type, 54
Delete, 57
Details of transfer, 56
EScript, 58
Esker proprietary language, 57
File transfer, 56
Files display, 55
Filters, 55
FTP Port, 53
Initial directory, 54
Inter-server transfer, 56
JScript, 57
Macros, 57
Open, 57
Password, 53
PC-server transfer, 56
Profiles, 54
Proxy, 55
Rename, 57
Save, 57
Security bridge, 55
Server name, 53
Server Type, 54
Source, 57, 59
Source file, 55
String encryption, 58
SYST Command, 59
Timeout, 54
Type of transfer, 57
User, 53
VBScript, 57
FTP API, 58
FTP Connection
 Settings, 53
FTP files display, 55
FTP Filters, 55
FTP Language, 57
FTP Macro Language
 ascii, 119
 bget, 119
 binary, 119
 ClearMessage, 119
 debug, 119
 delete, mdelete, 120
 Dos, 120
 drive, 120
 Echo, 120
 Exit, 120
 fcd, parent, 120
 get, mget, 120
 Goto, 121
 Host_text, 121
 Label, 123
 lcd, 123
 local, 123
 login, 123
 logoff, 123
 mkdir, rmdir, 124
 option, 124

- Pause, 124
- put, mput, 124
- rename, 125
- Server, 125
- Set, 125
- stat, 125
- text_codes, 125
- Title, 125
- verbose, 125

FTP profiles, 58

- Field descriptors, 59, 60
- Field separators, 59, 62

FTPD, 77

- Anonymous login, 78
- Banner, 79
- Clients, 79
- Comments, 78
- Limited access (Citrix/Microsoft TSE), 77, 79
- Password, 78
- Private configuration, 79
- Read only, 78
- Root directory, 78
- UNIX compatible, 78
- User, 78
- Users' rights (Citrix/Microsoft TSE), 79

FTPD in Citrix/Microsoft TSE, 77

I

- Importing an NIS configuration, 14
- Initial directory (FTP), 54
- ISO8859, 51

J

- JScript (FTP macros), 57

L

- Log file (LPD), 50
- LPD, 45
 - Conversions, 51
 - Limited access (Citrix/Microsoft TSE), 50
 - Log file, 50
 - Print Manager Queue, 50
 - Public printer, 50
 - Statistics, 51
 - Timeout, 50
 - Users' rights (Citrix/Microsoft TSE), 51
- LPD in Citrix/Microsoft TSE, 49
- LPR
 - Declaring a remote printer, 45
 - Name, 45
 - Number of retries, 46
 - Printing in DOS, 46
 - Protocol, 45
 - Remote command, 46
 - Remote host, 45
 - Remote queue, 46
 - Timeout, 46

- User name, 46

M

- Macros
 - FTP, 57
- MDI, 81, 86
- Mounting NFS file systems in 32-bit Windows, 36
- Multiple Document Interface, 67, 81, 86

N

- NFS
 - Automatic settings, 34
 - Burst read/write, 34
 - Created file permissions, 34
 - Default local drive, 33
 - File names, 38
 - Firewall, 35, 39
 - Locks, 38
 - Lookup cache, 35, 38
 - Mapping, 38
 - Max locks, 38
 - Name, 32
 - NFS Administration, 32
 - NFS drive properties, 37
 - NFS file properties, 37
 - NFS Settings, 38
 - NFS version, 33
 - Nobody, 33
 - Password, 35
 - PCNFSD server, 33, 35, 39
 - Proxy, 35, 39
 - Read cache, 35, 38
 - Read size, 34
 - Reconnect at logon, 33
 - Remote host, 32
 - Remote path, 32
 - Retry multiplier, 34
 - Root, 33
 - Server cache, 34
 - Settings, 37
 - Share/lock, 33
 - Statistics, 37
 - Symbolic links, 33
 - Timeout, 34
 - Timezone offset, 38
 - Transport protocol, 33
 - Use lowercase, 34
 - Write size, 34
- NFSD
 - Authenticated users, 43
 - Authorized clients, 42, 43
 - Clients, 42
 - Comments, 42
 - Directory, 42
 - Export name, 42
 - Limited access (Citrix/Microsoft TSE), 41, 43
 - PC-NFS authentication, 43
 - Read only, 42

- Statistics, 44
- Unrestricted access, 42
- Unrestricted read, 42
- Users' rights (Citrix/Microsoft TSE), 43
- NFSD in Citrix/Microsoft TSE, 41
- NIS, 13, 110
- NIS administrator, 20
- NIS domain, 14
- NIS resources, 13, 15, 27
 - Address books, 26
 - Applications, 27
 - Data sources, 26
 - Emulation configurations, 26
 - FTP configurations, 25
 - Mail addresses, 26
 - Network drives, 24
 - Object paths, 27
 - Printers, 23
 - Servers, 22
 - TAR configurations, 25
 - TFTP files, 25
 - URL addresses, 26
 - Virtual data sources, 26
- NIS tables, 13, 20

P

- Password (FTP), 53
- PCNFSD, 33, 35, 39
- PING, 29
- Printing (Tun TAR), 97
- Profiles (FTP), 54, 58
- Protocols
 - LPD protocol, 45
 - REXEC protocol, 45
 - RSH protocol, 45
 - TCP protocol, 31, 33
 - UDP protocol, 31, 33
- Proxy (FTP), 55
- Proxy (NFS), 35, 39

R

- Restoring files, 95
- REXEC, 45
- REXEC protocol, 92
- RPC Protocol, 99
- RSH, 45
- RSH protocol, 92

S

- Screen (VT320), 81
- Script languages (FTP macros), 57
- Security bridge (FTP), 55
- Server Type (FTP), 54
- Servers
 - PCNFSD server, 33, 35, 39
- Services
 - Esker FTPD, 77

- Esker LPD, 49
- Esker NFSD, 41
- Settings (Tun TAR), 96
- Source (FTP), 59
- Source file (FTP), 55
- Statistics
 - LPD, 51
 - NFSD, 44
- Statistics (NFS), 37

T

- TAR archives, 91
- TCP, 31, 33
- Telnet VT320, 81
- Terminal centering (VT320), 82
- Terminal fonts
 - System132, 82
 - SystemPC, 82
- Timeout (FTP), 54
- Tun FTP
 - Applying Filters, 69
 - Executing macros, 70
 - File structure representation, 68
 - Macro language, 70
 - Multiple connections, 67
 - Simple transfers, 68
 - Transfers between servers, 69
- Tun NIS, 13
- Tun RSH, 85
 - Adding commands to a macro, 87
 - Button mode, 87
 - Command panel, 86
 - Macro, 86
 - Result panel, 86
- Tun RSHD, 89, 112
- Tun SNTP
 - NIS, 104
- Tun VT320, 81
 - Backspace, 83
- Tun WALL, 99
- Type of transfer FTP, 57

U

- UDP, 31, 33
- UDP Protocol, 99
- User (FTP), 53

V

- VBScript (FTP macros), 57
- VT320_32.EXE, 114

W

- WADM2.EXE, 108
- WADM2_32.EXE, 108
- WALL recipients, 100
- WALL.EXE, 108

Network Resource Access

WALLD.EXE, 108
WALLD32.EXE, 108
WFTP.EXE, 108
WFTP32.EXE, 108
WFTPD.EXE, 109
WFTPD32.EXE, 109
WLPD.EXE, 109
WLPD32.EXE, 109
WMNT32.EXE, 109
WMOUNT.EXE, 109
WNFSD32.EXE, 110
WNISS32.EXE, 110
WNTP32.EXE, 112
WPING.EXE, 111
WPING32.EXE, 111
WRSH32.EXE, 111
WRSHD32.EXE, 112
WTAR32.EXE, 113
WTFTP32.EXE, 113