# NetOp Remote Control

## Version 6.5

# User's Manual

*When you're expected to be in two places at once!*

**Printed in Denmark**

**Document Revision: 2000062**

**Please send any comments to:**

**Danware Data A/S**

**Kongevejen 62**

**DK-3460 Birkerod**

**Denmark**

**Fax: Int +45 45 90 25 26**

**E-mail: danware@danware.dk**

**Internet: http://www.danware.com**

## Warranty

Danware Data A/S warrants the quality of the physical material of the user package, that is manual and CD-ROM. If these items are defective, we will exchange them at no cost within 60 days of purchase from Danware Data.

## Disclaimer

Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of any faults with the enclosed programs and/or documentation.

## License

Danware Data A/S retains the copyright to the user manual. All patent, copyright and other proprietary rights in and to the programs will remain with Danware Data A/S or its licensers.

Your purchase gives you the right to copy and use the programs as described on your *Danware License Certificate* included in your package.

Please save your *Danware License Certificate* and your original CD-ROM. They serve as your legal right to use the software. You may also need them in order to receive future updates to the product.

Please be careful not to install or run the software on more PCs than your Danware License Certificates permits you to do.

The programs may be copied for backup purposes only, and only as long as the above mentioned rules are adhered to.

## Trademarks

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this manual are trademarks of their respective manufacturers.

# Contents

# Chapter 1
# An Introduction to NetOp

## 1.1 About this manual

Your NetOp Remote Control manual contains documentation and technical information covering the different NetOp modules available - The NetOp Guest and Host, NetOp Gateway, NetOp Access Server, and NetOp Log Server.

*Note: Chapters containing information regarding NetOp modules you do not have should be ignored. If you wish to receive more information about the NetOp family of products, and licensing please contact your local NetOp distributor or Danware Data A/S.*

This manual is intended for a first time user of NetOp, however it contains valuable technical information and references that may be used by any user of the program - from novice to advanced.

Please use the table of contents to refer to the chapter division implemented as it might differ from previous releases of the NetOp Remote Control manual.

You should also note that the README.TXT supplied on your NetOp installation CD-ROM may contain important last minute information and should be read through before you start using the program.

The following typographical conventions are used throughout this manual:

Text in SMALL CAPITALS represents keys on your keyboard (a '+' indicates that keys should be pressed simultaneously). For example, SHIFT, ALT, or CTRL.

**Bold text** represents text you are to type at particular prompts, fields, etc.

*Italics* represent strings from the user interface.

## 1.2 NetOp Remote Control

Welcome to NetOp Remote Control, a Danware Data product for remote control of PCs over a wide variety of communication standards.

The term "remote control" refers to the interaction between the Guest, Host and possibly other modules that make up NetOp. By installing the Guest program on a PC it will be able to communicate with a PC running any of the Host modules and remote control it.

A user at the Guest PC (or the controlling PC) will be able to view the screen of the Host, transfer keystrokes and mouse actions that will be executed on the Host, or utilize many of the tools provided by NetOp. In a sense using NetOp will enable you to control a PC as if you were sitting right in front of it, even though it might be located on the other side of the globe.

NetOp Remote Control allows for a wide range of communication standards and operating system combinations.

The following is a overview of communication standards that may be used by the NetOp Remote Control program.

### Windows or OS/2 operating sytems

TCP/IP, UDP/IP, IPX, NetBIOS, Infrared (98/2000 only), Windows modem, Serial, Direct Cable connection (serial null modem), and ISDN (CAPI).

### DOS operating systems

IPX, NetBIOS (with both taking advantage of the NetOp for DOS program's extremely low TSR memory requirement).

## 1.3 Examples of use

The world of computing and networking contains many factors that should be considered when implementing almost any program into any environment. Different types of operating systems, communication protocols, security and access privileges set by administrators combined with the actual needs of end users create a complex spectrum of considerations that arise when any change or migration occurs.

The NetOp family of products was designed with that knowledge in mind. It offers compatibility and flexibility that allows for easy implementation and usage on almost any network, with almost any combination of operating systems and communication protocols.

Here are some examples of possible NetOp implementations:

## Support

Use NetOp to provide qualified help for users anywhere. With NetOp a help provider or help desk support engineer can take over a user's computer to perform maintenance, repairs, give on-line demos and provide fast efficient help without ever leaving his office, cutting down on travel expenses and valuable hours spent at end-user sites. With NetOp's *Help Request* feature systems administrators can ease and streamline support in larger organizations.

## Using Your office computer from home or when on the road

With NetOp you can access your computer at work from anywhere on the globe. NetOp's advanced communication functionality allows you to connect in one of several ways to the important data on your office workstation while maintaining high security standards. You can either dial-in directly or use the NetOp Gateway to browse for all available Host PCs on your LAN or WAN. You can exchange data, read your e-mail, initialize applications, retain full access to all network resources all from the comfort of your own home or while traveling.

## Remote Configuration and Network Maintenance

Use NetOp to remotely configure servers and workstations. Software implementation on a large scale can be done completely from within the comfort of an IT department. No matter what the operating system is or the communication protocol, NetOp can help deploy, install, and maintain software, configure systems, transfer configuration files, and maintain security. For example you can configure an OS/2 Lotus Notes Server from a Windows 2000 PC.

## Development and Testing

NetOp is ideal for testing multi-user programs on a network. NetOp's ability to simultaneously remote control multiple PCs provides the ultimate tool for the programmer who needs to test multi-user applications. For example: it allows you to act as a workstation

operator in one window, while monitoring activity on a Database Server on another, all done simultaneously!

## 1.4 The NetOp Modules

NetOp consists of the following modules , integrated together to provide your organization with the ultimate remote control solution, though not all are necessary to initiate a remote control session the “add-on” modules can prove to be a powerful tool in managing remote control activity for any particular environment.

*Note: This is a general overview of the products. They will be discussed in depth as you read further on.*

### The NetOp Guest

A Windows application that allows a PC to remote control any other PC, which is running the Host program. It provides for the interface used to view the Host PC’s screen, and other handy utilities providing for complete control over the Host.

### The NetOp Host

A Windows application that allows the PC on which it is running to be remote controlled by another PC running the Guest program.

### Log Server

The NetOp Log Server acts as a logging mechanism for NetOp traffic.The NetOp Log Server can provide the system administrator with valuable security information such as who controlled who, when, what actions were taken, and all of this done from one central point on a Network or any other environment with NetOp implemented.

### Access Server

The NetOp Acess Server provides the ultimate tool for centralized remote control security by maintaining the NetOp security profile of any company on one central network PC.

This eliminates the need to individually maintain passwords, access profiles, etc. on a multitude of Hosts and Guests. ALL security settings (user authentication, passwords, Host names, Host groups, and so on) are stored on the Access Server.

*Note: An Access Server can also act as a Log Server.*

### Gateway

The NetOp Gateway will accept incoming calls or redirect outgoing calls (NetOp Remote Control requests) via modem, ISDN, IPX, NetBIOS, TCP/IP or Infrared and route these calls to their intended destination.

The NetOp Gateway allows for up to10 dial-in/out points for NetOp traffic.

## 1.5 The NetOp family of products

The following is a brief description of the NetOp product range. When planning your NetOp implementation it is important to know the features available for each product so as to ensure that you experience a smooth and trouble free installation and configuration process.

*Note: The following section is only an overview, functionality and configuration methods will be discussed in depth in later chapters.*

### Cross platform support:

NetOp offers comprehensive cross-platform support for your remote control environment. For example: NetOp Remote Control modules can be integrated into a NetOp for OS/2 environment. A Windows module can use a NetOp for OS/2 Access Server, Log Server, or Gateway. A NetOp Remote Control Guest can also remote control an OS/2 Host (and vice-versa). A Windows Guest can also be integrated with NetOp for DOS modules (running the RemPC v4.3x program), with limitations applying. NetOp's ability to remote control version 4.3x RemPCs gives you the ability to remote control DOS PCs on your network from your Windows PCs. There are two main reasons for providing this type of cross-platform capability. The first reason being of course the flexibility that it provides, making NetOp easy to implement in almost any environment, and on almost any network. The second reason is to protect your investment in the product, making upgrades easier to perform, and ensuring reliable and flexible integration between all computers.

### NetOp Remote Control Version 6.x

NetOp Remote Control can be installed on Windows 2000, Windows NT (3.51 , 4.0), Windows 98, Windows 95 and Windows 3.1x. The Guest is capable of remote controlling Windows 2000, Windows NT (3.x,4.0), Windows 98, Windows 95, Windows 3.1x, OS/2, and DOS. NetOp supports all high resolution graphics and uses advanced state of the art techniques to obtain optimal performance. This is accomplished without replacing a single driver.

As mentioned previously NetOp supports a wide array of communication standards - TCP/IP, UDP/IP, IPX, NetBIOS, Serial (Direct connect with null-modem cable, analog modem, ISDN modem), Infrared, Windows modem (TAPI), and ISDN (CAPI).

## Additional features of NetOp Remote Control

In addition to the standard remote control functionality NetOp offers advanced features to help you take full advantage of the products:

Integrated bidirectional file transfer, remote reboot, chat mode, print redirection and interactive request for help just to mention a few. NetOp also offers a high level of security. In addition to the traditional security features such as password protection, a view only feature, user notification, and Callback security, NetOp offers a comprehensive centralized logging and security system through the use of the Access Server, and Log Server. Both of these modules can enable system administrators to completely supervise and audit all remote control activity from a central location. NetOp also offers integration with Windows security management.

To furthermore increase the capability of NetOp, the Gateway module allows access to any NetOp Host on a network through one central point, enabling a user to dial in using a dial-up interface to browse a LAN using the IPX, IP or NetBIOS protocol. A Gateway can run on almost any type of PC from a high-end server to a non-dedicated PC offering the highest possible flexibility.

## NetOp for OS/2 version 5.x

NetOp for OS/2 offers Host module capability on OS/2 ver. 1.3, 2.x, Warp, Warp Connect and version 4.0. NetOp for OS/2 supports all high resolution graphics and uses advanced techniques to obtain optimal performance, yet still consumes only a minimal amount of system resources. It offers all of the functionality and backwards compatibility available with NetOp Remote Control 5.x, plus communication over the same standards (NetOp for OS/2 also includes APPC). The OS/2 version also offers the Log Server, Access Server, and NetOp Gateway functionality.

## NetOp for DOS

The group of NetOp for DOS modules consists of individual modules for modem, ISDN (CAPI Interface), and network (IPX/NetBIOS).

### NetOp for DOS (network)

Network remote control of DOS, Windows and OS/2 from a DOS program. Supports NetBIOS and Novell/IPX network protocols with extremely low memory requirements (only 3 to 6 kb of RAM). Supports standard VGA graphics for OS/2 and some SVGA for DOS/Windows. The NetOp for DOS (network) program also offers peer-to-peer file transfer, and the ability for Hosts to be controlled by NetOp Remote Control for Windows and NetOp for OS/2 Guests.

### NetOp for DOS (modem)

Modem remote control of DOS and OS/2 PCs from a DOS program. As it's network counterpart it uses very little memory, and offers the file transfer feature. The NetOp for DOS (modem) program also includes chat, and a remote reboot feature.

### NetOp for DOS (ISDN)

Remote control of DOS/Windows over ISDN (CAPI) from a DOS program. Supports any ISDN adapter with a CAPI 1.1 interface. Also includes an advanced drag and drop file transfer feature.

## Custom Solutions

Should our current line of standard products not satisfy your needs, please inform us.

If what you miss is not already planned for upcoming versions, the Danware expertise can be made available to provide a customized solution for you.

# Chapter 2
# Installation

## 2.1 Summary

This chapter describes the necessary steps for installing the NetOp software on your computer.

Installation of all NetOp modules is described. In case your NetOp licensing does not include all modules, please disregard the sections that describe installation of modules you do not have.

It is very important that you read through the README.TXT file located on your distribution CD-ROM. This file contains important information, which is not in this manual.

## 2.2 Prerequisite Tasks

### 2.2.1 Technical Requirements

For details regarding technical requirements please refer to Table 12-1 in chapter 12 ‘Appendix’.

### 2.2.2 Checking Your Package

Your package should contain a manual, a registration card, the NetOp software CD-ROM and a license certificate.

NetOp packages consist of one or more of the NetOp modules: The Guest, the Host, the Gateway, the Access Server and the Log Server. Depending on the type of license you have purchased you will be able to install one or more of these modules. For more information regarding licensing please contact Danware Data A/S, or you local distributor.

## 2.3 Installation

To start the NetOp installation process insert the NetOp CD-ROM into your CD-ROM drive, the main NetOp installation screen should then appear automatically.

*Note: If you have chosen not to automatically run AUTORUN.INF files or if the installation screen does not appear, start the program: D:\SETUP.EXE (where 'D:' represents your CD-ROM drive letter).*

Follow the on-screen instructions by selecting the appropriate language. The installation program will then prompt you to either navigate to the installation menu, view related documentation and product information.

*Note: The NetOp documentation is available in PDF (Portable Document Format) format. To view the NetOp documentation in PDF format you must install the Acrobat Reader (TM) program included on your NetOp installation CD-ROM.*

From the installation menu you may either choose to *Install NetOp* which will then start the NetOp installation program or to *Create Install Disks*, which will then prepare the main NetOp installation program on 3.5" disks. Choose this option if you wish to install NetOp on PCs that do not have a CD-ROM drive.

## 2.3.1 Installing the Guest module

After choosing to *Install NetOp* from the main installation menu, the NetOp installation program will start. Follow the on-screen instructions to install the NetOp Guest module.

## 2.3.2 Installing the Host modules

After choosing to *Install NetOp* from the main installation menu, the NetOp installation program will start. Follow the on-screen instructions to install the NetOp Host module. Depending on the license number entered NetOp will either install a standard Host, an Access Server, a Log Server or a Gateway. For more information regarding licensing please contact Danware Data A/S or your local distributor.

## 2.3.3 Actions performed by Setup

Setup uncompresses the NetOp files to the directory specified by the user, and creates a Program Folder.

Furthermore setup performs the following:

Installs the file CTL3D.DLL and/or CTL3D32.DLL in the Windows\System directory (only if newer versions of the DLLs do not already exist).

Modifies the registry on Windows 9x, Windows NT and Windows 2000 PC's.

NetOp installs the VNETOP.386 device driver in [386enh] section of the SYSTEM.INI file on Windows 3.x systems.

On Windows NT and Windows 2000 setup installs additional device drivers and modifies the registry.

NetOp creates file associations for both DWC files (NetOp connection files), DWR files (NetOp recording files) and DWS files (NetOp script files).

NetOp installs a special NetOp port monitor to be used by the NetOp remote printing feature.

## 2.4 Silent Install

NetOp includes a silent install feature, which uses a special source file to help install and setup the NetOp modules. This SETUP.ISS source file can be accessed quickly and easily making it a particularly useful feature with large installations. For information regarding the silent installation process and the SETUP.ISS file please refer to Section 12.2 'Silent Install and NetOp Deployment'.

## 2.5 NetOp Deployment Utility

NetOp Deployment Utility (NDU) is a separate NetOp program which helps you to configure and deploy NetOp Host or other NetOp modules. The program runs on Windows 2000 or NT. Using push technology, it can deploy onto networked Windows 2000 and NT PCs even though NetOp has not previously been installed. It can also deploy onto Windows 2000, NT, 98 and 95 PCs where a NetOp Host version 6.x is running. This includes reaching non-networked PCs via e.g. Modem.

To install the NetOp Deployment Utility insert the NetOp CD-ROM into your CD-ROM drive, and the main NetOp installation screen will then appear automatically. Select *English*, then *NetOp Deployment* and *Install.*

For more information, please refer to Section 12.2 'Silent Install and NetOp Deployment'.

# Chapter 3
# Quick Start

## 3.1 Summary

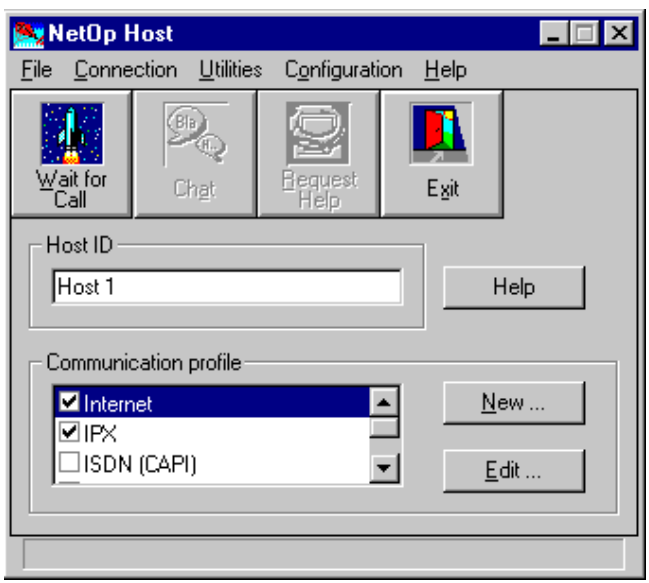
This chapter presents a brief guide that should enable you to get started with NetOp. After reading this chapter you should be able to set up the Guest and Host and start a remote control session.

## 3.2 The Host

To start the Host program, double click on the Host icon in the NetOp program folder or start the program NHSTW32.EXE (NHOSTW.EXE - Windows 3.1x PCs) from the NetOp directory.

The first time the NetOp Host is run the program will offer to guide you through configuration of your modem. Follow the on-screen instructions if dial-up capability is needed

You will then be presented a dialog as shown in the following figure:



In the *Communication profile* section use the check boxes to choose one or more interfaces from the list that the Host should use to communicate with the Guest. If you are in doubt about which profile(s) to choose, please consult your system administrator.

By default, the Host ID will be the Windows computer name. To change Host ID choose Program options from the Host's Configuration menu and select the Host name tab.

To start the Host, click the *Wait for call* button in the Toolbar (see the following figure). The Host will initialize and the selected communication profiles wait for incoming calls.


The Host will remember the setup information for future use. The next time the Host is run simply click *Wait for call* to initialize it.

To bypass the configuration phase and start the Host directly the next time it is loaded, choose *Program options* from the Host's *Configuration* menu, and enable *Wait for call at program startup* from the resulting dialog box.

## 3.3 The Guest

To start the Guest, double click on the Guest icon in the NetOp program folder or start the program NGSTW32.EXE (NGUESTW.EXE on Windows 3.1x PCs) from the NetOp directory.

The first time the NetOp Guest is run the program will offer to guide you through the configuration of your modem. Follow the on-screen instructions.

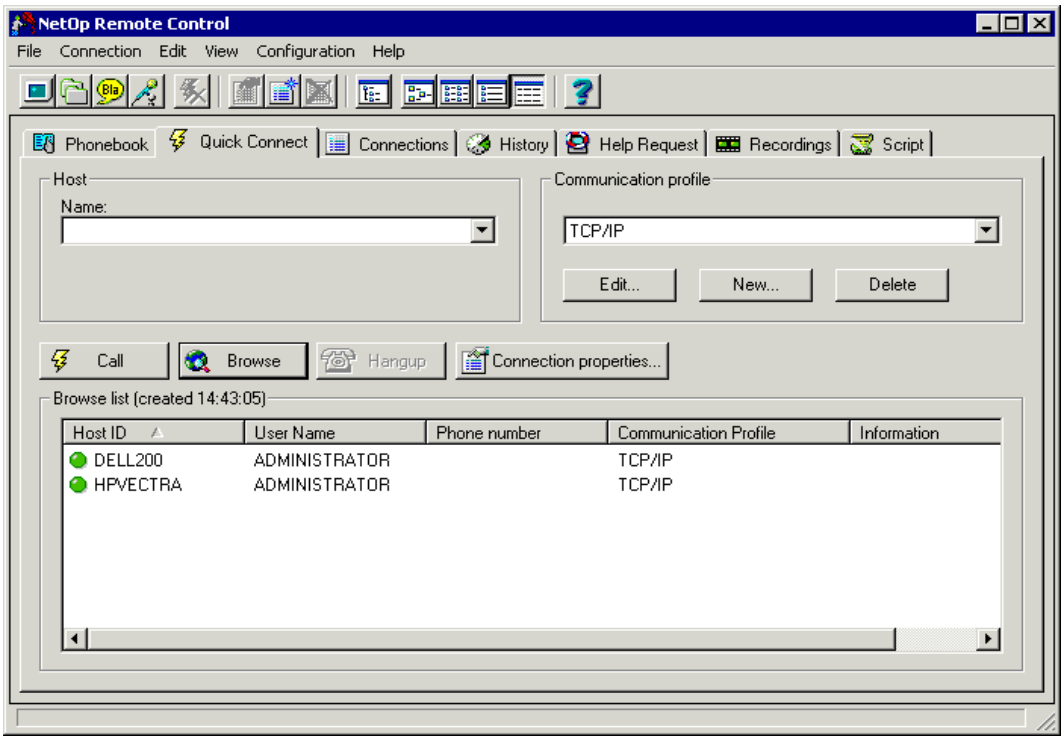
To start a remote control session do the following:

1. Click the *Quick Connect* Tab (see the following figure).

2. Select the appropriate communication interface from the *Communication profile* drop down list (if in doubt, consult your system administrator).

3. If you are going to reach the Host through a dial-up connection (modem or ISDN) enter the phone number in the *Phone number* field and leave the name field empty. For a network connection to the Host enter the Host name in the *Name* field. For NetBIOS and

## 3.3 The Guest




IPX this is the name that is displayed in the Host ID field in the Host main window. For TCP/IP enter the Host PC's DNS name or IP address in dotted-decimal notation.

(E.g. peter.danware.dk or 208.0.0.1).

Click the *Call* button.

Use the *Browse* button to browse for available Hosts on a network, and you will be presented with a list of available Hosts. If you have chosen to Browse using a dial-up protocol, the Guest will first dial the number entered, then connect to the Host or Gateway and finally browse.

To connect to a Host from the browse list, simply double click on it in the browse list.

# Chapter 4
# The NetOp Guest

## 4.1 Summary

This chapter describes the procedures for using the NetOp Guest. This is the NetOp module that is used to remote control a Host PC.

Areas covered in the chapter include: How to start the Guest, how to configure the Guest and operation during remote control sessions.

For instructions on how to install the Guest please refer to chapter 2, ‘Installation’.

## 4.2 Starting the Guest

To start the NetOp Guest do the following:

1. Open the program folder in which you installed NetOp.

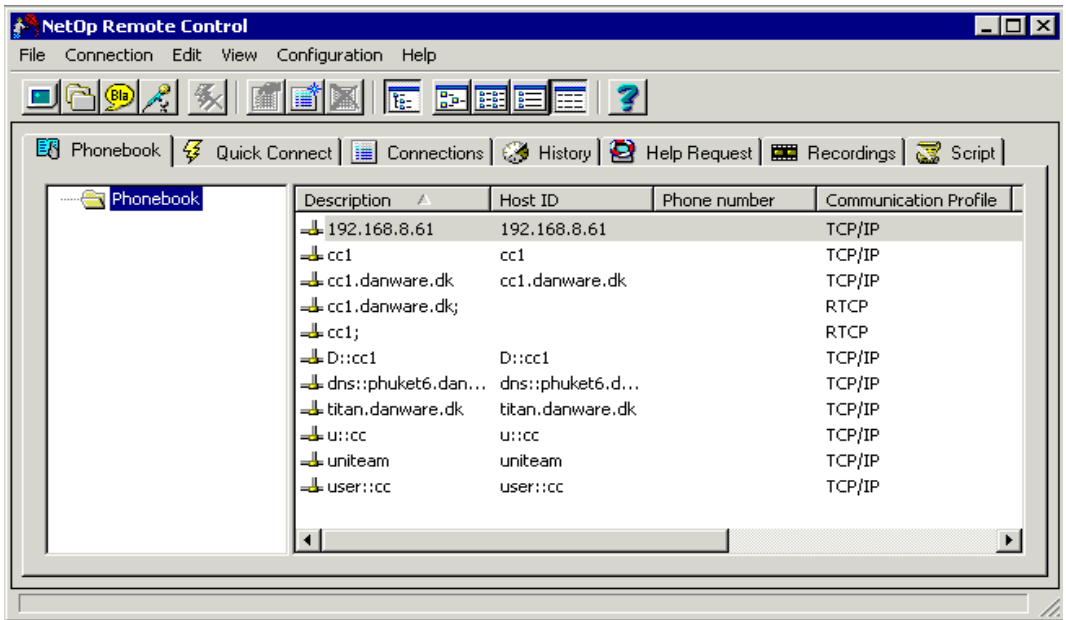
2. Double-click the Guest icon.

This will launch the NetOp Guest Program

The first time the NetOp Guest is run the program will prompt you to setup your modem, follow the on-screen instructions or select no if a modem is not to be used right now.

## 4.3 The NetOp Guest Interface Overview

The following figure shows the NetOp Guest user interface:




When connecting to one or more Hosts, the NetOp Guest Program will open new windows, one to remote control each Host. Multiple chats and file transfers can likewise be active. All these windows can be minimized and otherwise manipulated.

Furthermore the main window, or the ‘Guest Control Panel’ contains the following elements:

## 4.3.1 Menubar

The Guest program contains a Menubar where all NetOp options are available.

## 4.3.2 Toolbar

In the Toolbar (placed by default below the Menubar) shortcut buttons for the most common commands are available. The Toolbar can be placed anywhere within or outside one of the NetOp windows. Simply click anywhere within it’s limits and drag it around, holding the mouse button down.

## 4.3 The NetOp Guest Interface Overview

The following is a list of commands that can be executed from the NetOp Guest Toolbar.

### Remote Control

Click on the above icon to initiate a remote control session with selected Host(s).

### Transfer files

By clicking on the above icon you will start the NetOp file transfer utility, to use with the selected Host.

### Chat

Select this option to initiate a chat session with the selected Host.

### Audio Chat

Click on the above icon to initiate an Audio Chat with a selected Host.

### Hangup

Select this option to hangup all connections to the selected Host, including remote control, file transfer, chat and video chat.

### Tools

Use the above icons to (left to right): Edit the connection properties of a selected item in a particular tab, create new entries, or delete a particular entry.

### View Tools

Select the following Toolbar icons to initiate different views of items and entries:

(left to right)

View or hide the tree view folder

Display items using large icons

Display items using small icons

Display items in a list

Display detailed information about each item in the window.

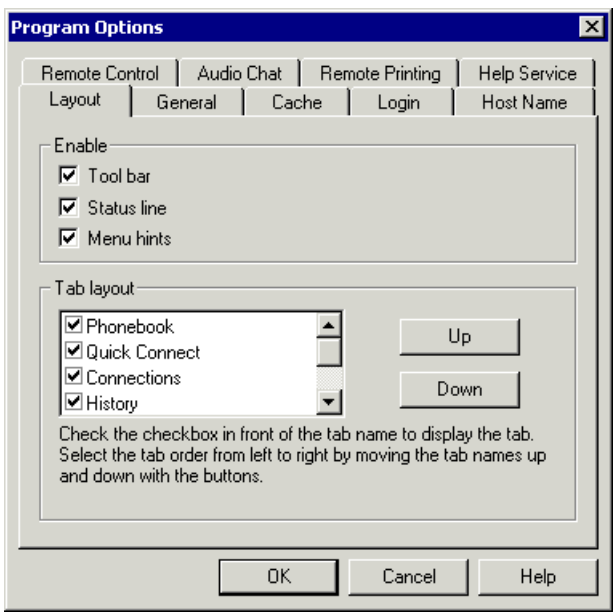
*Note: Some view tools may not be available for all tabs.*

# 4.4 Program Options

The *Program Options* dialog box is activated by choosing *Program Options* from the *Configuration* menu. The following sections describe how to control some of the elements in the Guest Control Panel.

## 4.4.1 Layout

The *Layout* Program Options tab is shown in the following figure.




This *Layout* tab of the Program Options dialog allows you to configure the layout of the Guest Control Panel. The following list describes the options available.

### Toolbar

Enable this option to display the Toolbar.

### Status Line

Selecting this option will enable a status line located at the bottom of the Guest Control Panel. Use this Status Line to view menu hints and other information pertaining to the Guest.

### Menu Hints

When this option is enabled the status line will display a description of the current menu item or Toolbar button.

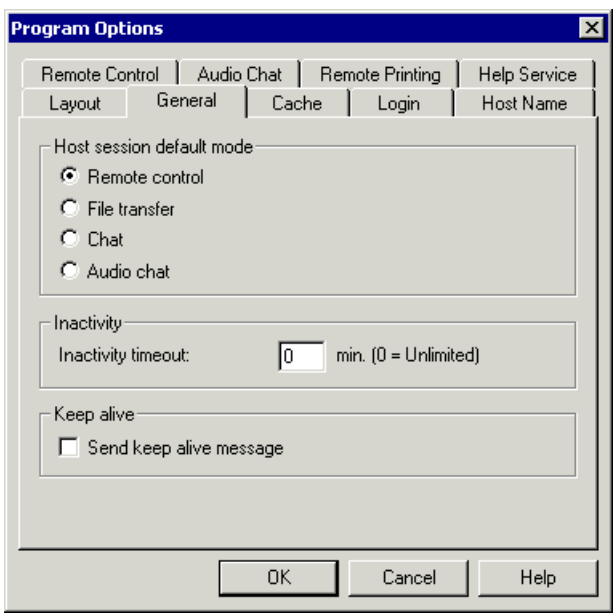
### Tab Layout

Use this option to specify which tabs you wish to enable in the main Guest Control Panel and their subsequent order. By checking or un-checking a particular tab you will either enable or disable it. Use the *Move Up* and *Move Down* buttons to specify the tab order from left to right.

All changes will take effect the next time the Guest program is started.

## 4.4.2 General

The *General* Program Options Tab is shown in the following figure:



## 4.4 Program Options

### Host session default mode

This option allows you to select the session type to be initiated when a Host is double clicked from any of the tabs. You may select from the following options: Remote Control, File Transfer, Chat, or Audio Chat.

### Inactivity timeout

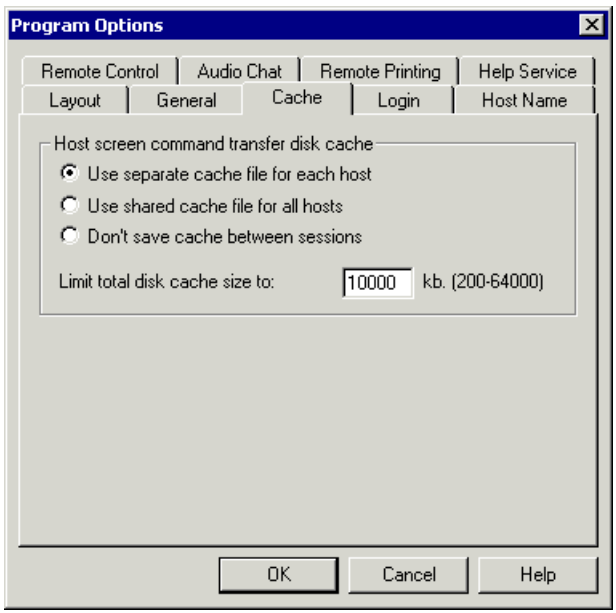
NetOp disconnects from a Host, if there is no activity for more than the specified number of minutes. Activities include keystrokes, mouse events and file transfers. Video display changes and audio signals are not considered “activity” in this sense, and NetOp will disconnect even though there are screen changes. Choose ‘0’ to specify no timeout.

### Send Keep alive message

NetOp uses a non-polling communications technique. In a sense this means that if there is nothing to send between Guest and Host (e.g. keystrokes from Guest to Host or screen changes from Host to Guest) nothing will be sent. By checking this options you will be sure that a connection timeout will occur if there is a bad or unstable connection between the Guest and Host. This option should be unchecked if you want to take advantage of the CAPI short-hold-mode feature or if communicating through e.g. an ISDN router that should be shut down if there is no activity to save cost.

## 4.4.3 Cache

The *Cache* Program Option Tab is shown in the following figure:




### Use separate cache file for each Host

Use this option to save the Host's screen cache locally, creating a new file for each Host.

### Use shared cache file for all Hosts

Use this option to save the Host's screen cache locally, using the same file for all Hosts. This reduces the total cache size on the disk but may also hinder performance.

### Don't save cache between sessions

Use this option when you do not wish to save screen cache on the Guest's hard drive.

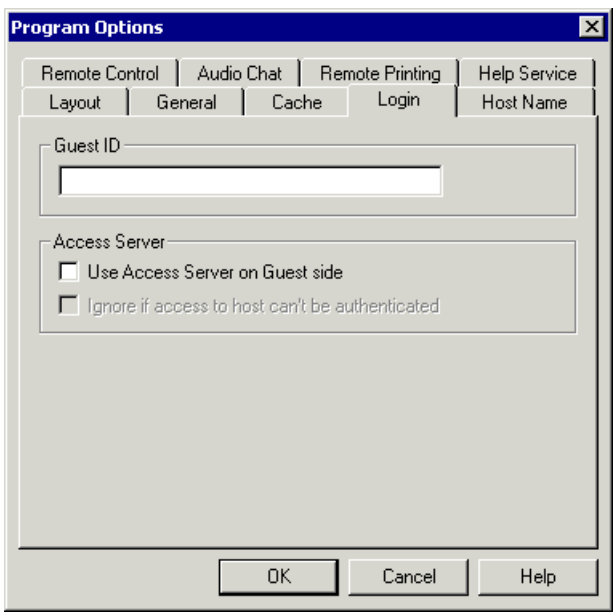
### Limit total disk cache size to

Use this section to determine the maximum size of the screen cache. The default size of the cache is set to 10000kb.

The default location for the cache files is a subdirectory to your main NetOp directory called 'Cache'. You can specify a different location by using the `CachePath=` entry in the `[Guest]` section of the NETOP.INI file.

## 4.4.4 Login

The *Login* Program Option Tab is shown in the following figure:




This section of the program options dialog is used in conjunction with the NetOp Access Server (See Chapter 9 'The Access Server').

### Guest ID

Enter an ID for the Guest machine. Use this option in conjunction with the *Use Access Server on Guest side* option. This will authenticate a Guest on an Access Server, or

when a Guest identifies itself to a particular Host. This ID is also used when using the log feature either when logging locally or when logging on a Log Server.

### Use Access Server on Guest side

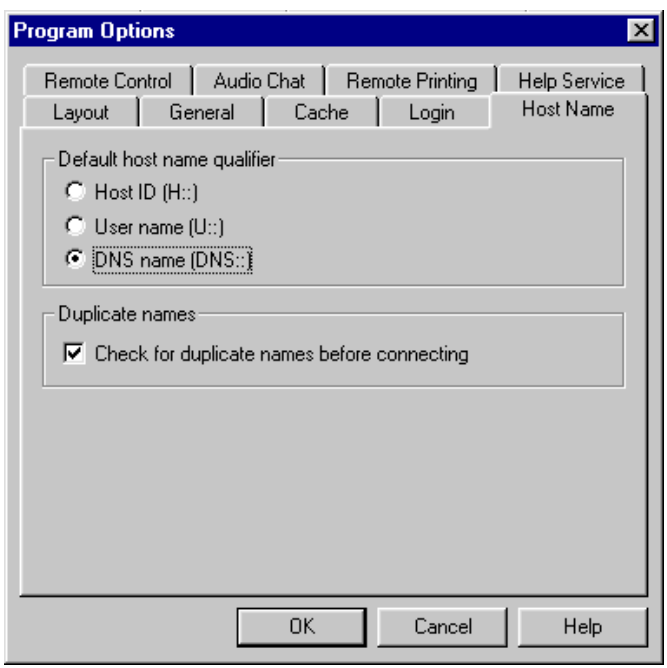
Enable this option if you want the Guest to use an Access Server for authentication before controlling Hosts. Upon restarting the Guest, it will search for an Access Server and will have to login. The Access Server will control authentication and Guest access rights for the Guest, assuming it is present on the server.

### Ignore if access to Host can't be authenticated

Enable this option if you wish to remote control Hosts that require the Guest to be authenticated by an Access Server while still allowing you to remote control PCs that do not require the Guest to be authenticated.

## 4.4.5 Host Name

The *Host name* Program Options Tab is shown in the following figure:



## 4.4 Program Options

Three types of name qualifiers are available when trying to initiate a session with a Host. These name qualifiers offer different methods for calling the particular Host, either by its Host ID, User Name, or DNS Name. In this dialog you may change the default name qualifier.

### Host ID (H::)

Select the option “H::” to implicitly prefix “H::” to what users type in the Guest’s Name field. If a user enters “Bill”, it will be interpreted as “H::Bill”, and the Guest will try to connect to a Host with the HostID “Bill”. However, if a name qualifier was explicitly entered, like “U::Bill”, the default name qualifier will be ignored. The explicit name qualifier will be used instead.

### User Name (U::)

Select the option “H::” to implicitly prefix “U::” to what users type in the Guest’s Name field. If a user enters “Bill”, it will be interpreted as “U::Bill”, and the Guest will try to connect to a Host, where the user Bill is logged in. However, if a name qualifier was explicitly entered, like “H::Bill”, the default name qualifier will be ignored. The explicit name qualifier will be used instead. If you are using this qualifier with TCP/IP, and the Guest and Host are on different subnets, you must manually add the Host’s IP address to the Guest’s IP broadcast list.

### DNS Name (DNS::)

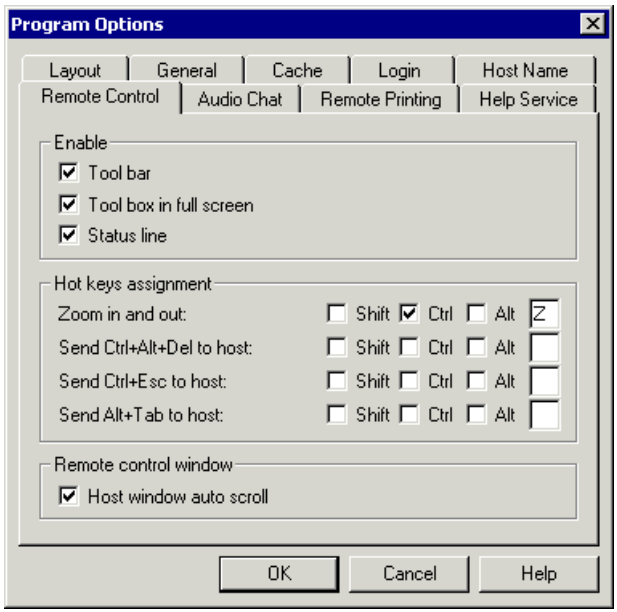
Select the option “DNS::” to implicitly prefix a “DNS::” to what users type in the Guest’s Name field. If a user enters “Bill”, it will be interpreted as “DNS::Bill”, and the Guest will try to ask its IP name server for an address for Bill. However, if a name qualifier was explicitly entered, like “U::Bill”, the default name qualifier will be ignored. The explicit name qualifier will be used instead.

### Check for duplicate names before connecting

Since the same users might be logged in to different PCs at the same time a situation might be encountered where duplicates exist when using e.g. User Name as a qualifier. When selecting this checkbox the Guest will display a list of duplicate Names if any are encountered.

## 4.4.6 Remote Control

The *Remote Control* Program Options Tab is shown in the following figure:




### Toolbar

Enable this option to display a NetOp Toolbar containing the most common NetOp commands and options in the Remote Control Screen. All actions executed from the Toolbar will apply only to the corresponding Host.

### Toolbox in full screen

Enable this option to display a NetOp Toolbox containing the most common NetOp commands and options when the Host is viewed in full-screen mode. All actions executed from the Toolbox will apply only to the corresponding Host.

### Status Line

Selecting this option will allow you to view a status line for each active Remote Control Window. The Status Line will be placed at the bottom of the Host window and will contain the following information (from left to right):

1. Menu hint - A brief description of the menu entry or Toolbar button currently under the mouse.

2. Mouse mode

3. Keyboard mode

4. Time connected. Shows the total time connected to the Host PC in the active window.

If the active Host PC is controlled via a dial-up connection, the status line will show two status lamps. For a serial/modem connection the lamps will be turned on when receiving data (RD) and transmitting data (TD). For an ISDN connection the lamps will be turned on when there is activity (receiving or transmitting) on B channel 1 (B1) and B channel 2 (B2).

### Hot Key Assignment

**Zoom in and out**

Specify which key combination will switch between full screen mode and windowed mode. The default value is CTRL+Z (z for zoom). To change the zoom Hotkey enable the *Shift*, *Ctrl* and *Alt* check boxes, depending on which of those keys you wish to use as part of the Hotkey combination. Enter a letter (A-Z) in the key field (the right most field).

Certain keystrokes can not be intercepted on the Guest, in this section you can define Hotkeys for the most common of these keystrokes.

**Send Ctrl+Alt+Del to Host**

Use this function to transmit the CTRL+ALT+DEL key combination to the Host. This function is used to perform special operations on Windows NT. To boot the Host PC do *not* use this Hotkey, but rather the Restart command (see section 4.16.8, ‘Restart Host’).

**Send Ctrl+Esc to Host**

Use this function to transmit the CTRL+ESC key combination to the Host. This function is used to activate the start menu on Windows 95/98/2000 and NT 4.0 PCs.

**Send Alt+Tab to Host**

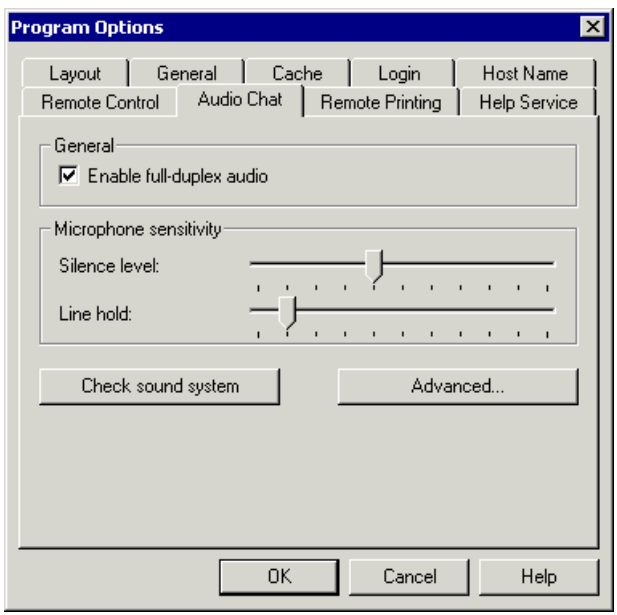
Use this function to transmit the ALT+TAB key combination to the Host. This function is used to switch between windows on Windows PCs.

### Host window auto scroll

Scrollbars will be added to the Remote Control Window on the Guest if the Host screen resolution is larger than the window. To see all parts of the Host screen the scrollbars can be operated manually. If Auto Scroll is enabled , the Remote Control Window will scroll automatically as the mouse approaches any of the window's four edges. The mouse will not move on the Guest screen but instead the Remote Control Window is scrolled in the direction of the mouse movement. If the mouse is moved fast out of the Remote Control Window, the window will not be automatically scrolled.

## 4.4.7 Audio Chat

The *Audio Chat* Program Options Tab is shown in the following figure:



### Enable Full Duplex

Select this option to enable full duplex sound for use with the NetOp Audio Chat feature.

Using Full-duplex enables a user at the Guest to talk to and hear a user at the Host PC at the same time. If this option is enabled NetOp will detect whether full-duplex is available and then use it.

*Note: Please consult your audio hardware documentation to verify that the particular sound device being used supports the full-duplex sound option.*

### Silence Level

The silence level thumb adjusts the Audio Chat silence level which refers to the audio level threshold that must be reached before a particular sound is picked up and used by the NetOp Audio Chat feature.

If full-duplex is not available or not used, NetOp must arbitrate the ownership of the microphone because Guest and Host can not talk at the same time (similar to a walkie-talkie) i.e. The Guest must stop speaking before the Host can speak and vice-versa. For NetOp to release the ownership of the microphone it must be able to detect silence, which can not be completely attained because of background noise. Experiment with the thumb, by placing it in a position where nothing is sent when you are not talking, and everything is sent when you are talking.

If full duplex is used the silence thumb can be set in a low position so the microphone is turned on all the time. If you are communicating over a slow line (e.g. modem) you might want to experiment with the thumb to limit the bandwidth.

### Line Hold

Use this option to configure the amount of audio data sent as “one-unit” across a communications link. For example, if a user is engaged in a normal vocal Audio Chat, the line hold will probably be set to medium or low allowing for both Guest and Host modules to interact with each other without long delay times. The line hold will be set to high if a user wishes to transfer a continuous piece of audio data over the link requiring a continuous stream of information for smooth play.

### Check Sound System

Use this option to check the current sound system installed on your PC for use with the NetOp Audio Chat feature.

*Note: Before initiating NetOp Audio Chat please make sure that you have configured all sound components and device drivers. For more info please consult your audio device hardware documentation as to available drivers and features of your particular audio device.*

### Advanced

Pressing the *Advanced* button will bring up the following dialog box:


### Record / Playback Preferred Device

This option allows you to select both audio input and output devices. By default NetOp will use the most suitable devices available, in case a PC has more than one sound device installed you may choose one from either the Record or Playback drop down list.

### Audio Compression

The sound NetOp picks up during an Audio Chat can be compressed using an audio compression codec. The list shown in the above figure presents the compression codecs installed on your computer that NetOp can use.

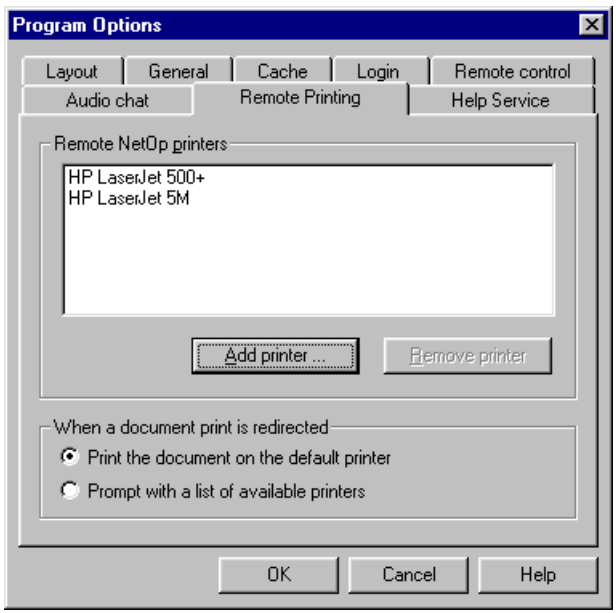
An audio compression codec must be present on both Guest and Host for it to function. Use this option to specify the order in which NetOp will search for a compression codec that can be used when an Audio Chat is started.

Use the *Move Up* /*Move Down* or *Use Defaults* buttons to organize the list of audio compression codecs as desired. If no compression is preferred (better quality but higher bandwidth) then select one of the *'No Compression'* codecs in the list.

*Note: A 'no compression' codec will be used if NetOp can not find any compression codec that can be used between the particular Guest and Host.*

## 4.4.8 Remote Printing

The *Remote Printing* Program Options Tab is shown in the following figure:




The NetOp Remote Print facility allows a Guest to send a print job to a Host where it will be printed locally and vice-versa. This dialog allows you to configure the NetOp Remote Printing options.

### Add Printer

This option will allow you to add a Windows printer which is used as NetOp printer. A NetOp printer appears to Windows to be a local printer, but the print jobs routed to it are redirected to the other end of your NetOp connection and printed on one of the Windows printers defined there. A NetOp printer uses a port named "NetOp:", where other printers use ports named for example "COM1:" or "LPT1:" The NetOp: port is installed when you install NetOp.

Once you have clicked the *Add Printer* button, NetOp will launch Windows' Add Printer Wizard and wait for you to press the Ready button when you are done with the Windows

Wizard. You can do exactly the same without starting NetOp at all., if you start manually from Printers in the Control panel or from Printers in the Start menu

To add a NetOp Printer please follow these guidelines, which assume you have started Window's Add Printer Wizard in one of the three ways described earlier. This Wizard is slightly different on different Windows versions, so on your computer, the items below may not appear exactly as listed.

1. Configure the printer to be a local printer. This is sometimes stated as managed by *My Computer.* Windows must believe that this is a local printer, and must not be aware that NetOp takes the print jobs and redirects them. If there is a checkbox referring to plug and play, make sure you uncheck that box.

2. In the Available Ports dialog select the port named "NetOp:" (On 95/98 this is item 3, not 2).

3. Select the printer manufacturer and model which matches the printer you want to print on. That printer is not physically attached to the computer you are running the Add Printer Wizard on, but to the computer in the other end of the NetOp connection. (On 95/98 this is item 2, not 3).

4. Give the printer a name you can easily recognize. One idea is to append "Netop" to the automatically generated name. It might not make sense for you to have this printer as your default printer, since it only works when there is a NetOp connection active.

5. The printer may not be shared.

6. If you select to print a test page, make sure a NetOp connection is active.

7. Click on the *Finish* button.

When a print job is sent to the NetOp Printer on the one end of a NetOp connection, it will be redirected to the other end, where it will be printed physically.

### Print the document on the default printer

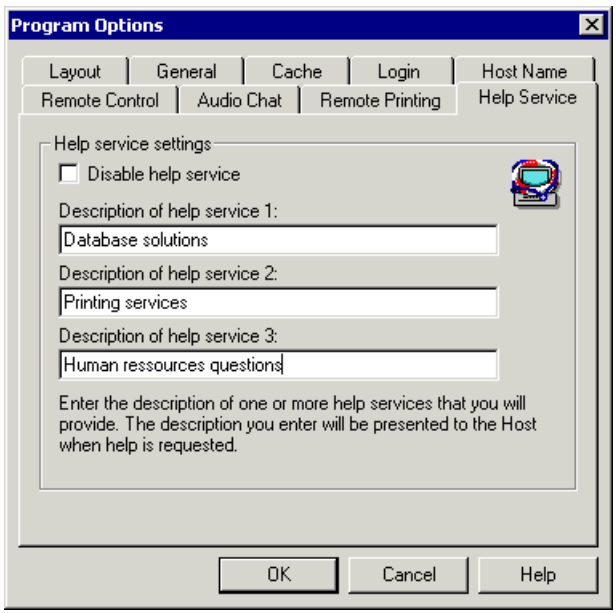
By selecting this option, any print job redirected through a NetOp printer to a Host will automatically be printed on the Host's default printer.

### Prompt with a list of available Printers

By selecting this option, the Guest will prompt its user with a list of available printers on the Host, when ever a print job is redirected. The user at the Guest can then select the printer that should be used for the particular job.

## 4.4.9 Help Service

The *Help Service* Program Option Tab is shown in the following figure:




NetOp contains an advanced *Help service* feature, which is designed to ease the process of providing on-line support. It is possible for a NetOp Guest to register as a *help provider*. Hosts can then request help from the registered providers. The Help service is available on networks as well as on dial up connections, directly or via gateways.

In the *Help Service* Program Options Tab it is possible to enter three *Help services* that will be offered by the particular Guest. Leave all three *Help Services* empty or check the *Disable help service* check box to turn help service off.

A Help service could be the name of a specific application this Guest wishes to provide support for. Or it could be the name of the person providing the support. Whenever a Host activates the *Request Help* function it will be presented with a list which contains all help services registered by any Guest. For more information regarding Help Service please refer to section 4.10 ‘The Help Request Tab’.

## 4.5 Guest Control Panel Tabs

The NetOp Guest Control Panel Contains a Phonebook, Quick Connect, Connections, History, Help Request, Recordings, and Script tabs. Some basic organizational rules apply to the management of these tabs.

### 4.5.1 Directory Window

The directory window is available in the Phonebook, History, Recording, and Script tab.

The left window pane (or directory window) contains the hierarchical list (tree structure) of the different directories created by the user. Use the directory window to group PCs or recordings after e.g. geographical or organizational position. Directories can be collapsed or expanded by double clicking on the directory icon with the mouse. It is possible to resize the Phonebook directory window or hiding/showing it by clicking the *Tree View* icon in the Toolbar.

To add a directory, right click anywhere within the directory window pane and choose '*create new folder*'. After you have entered the new folder name it will be created in the location specified. It is possible to cut, copy, paste, and rename directories by right clicking, and selecting either one of the options presented (or by using the menu).

To view objects in a particular directory simply click on it, the Hosts, Scripts or Recordings will then be showed in the listing window pane.

### 4.5.2 Listing Window

The listing window presents the Hosts, Recordings, or Scripts entered into the particular folder in the directory window pane by the user. (Similar to windows explorer).

To connect to a Host in the listing window simply double click on it (except in the Connections Tab). You may also start an session of your choice by selecting a corresponding button from the Toolbar, the icon will be selected until it is clicked again, this will end the particular session.

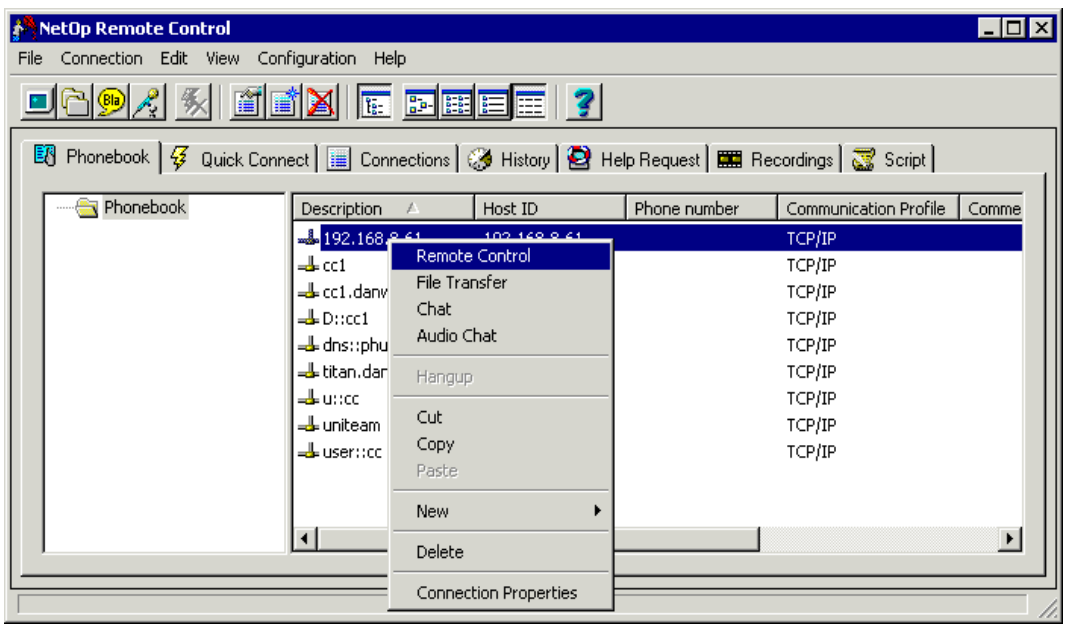
The listing window also contains a column header (available when detailed view is selected) which allows the user to arrange the different objects by either description, Host ID, User name, phone number, or communication profile, recording duration, time, etc. To arrange Hosts recordings or scripts by a particular category simply click on the corresponding tab, a small arrow will show the direction (either up or down) in which the column is organized.

You may also choose different views of Hosts by selecting the corresponding icon in the Toolbar (Large icons, small icons, details, etc.).

*Note: You may copy, cut, and paste files from the Guest Control Panel into any location on your computer (using Windows Explorer or any other similar application). This allows for easy access to phonebook entries, session recordings, or script files.*

## 4.6 The Phonebook

The Phonebook is activated by choosing the Phonebook tab from the main Guest dialog. The *Phonebook* tab is presented in the following figure:



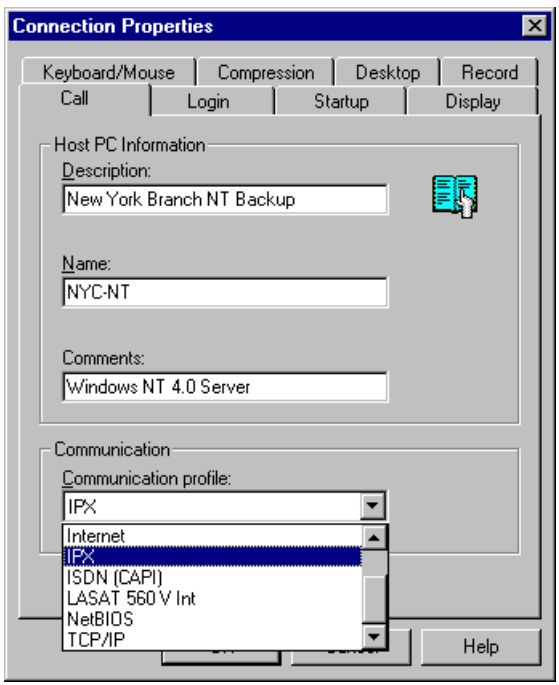

### 4.6.1 Adding Hosts

To add a Host to a particular Phonebook directory, simply right click anywhere within the Host listing window pane then choose *New* then *Phonebook entry* (or click on the corresponding icon in the Toolbar). The following multi - tabbed dialog will then appear.

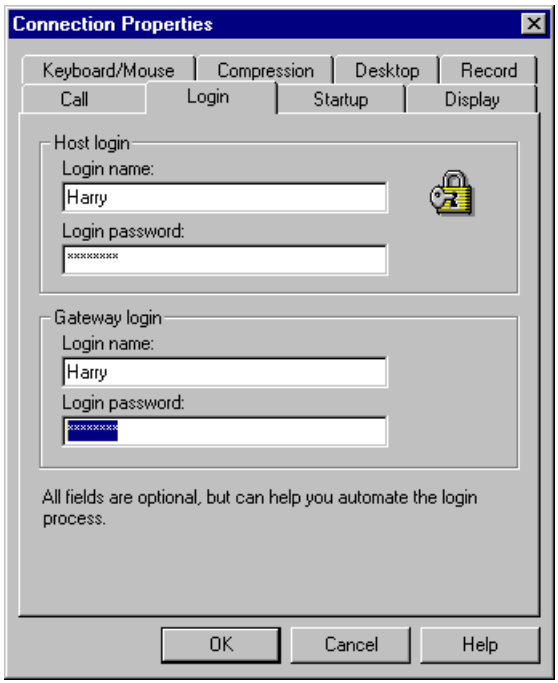
Enter a description in the *Description* field. This is the string that will appear next to the element in the list.

## 4.6.2 Call

Depending on which communication profile you have chosen, the dialog will contain just a *Name* field (network communication devices) or a *Phone number* and a *Name* field (dial-up communication devices). Use the *Comments* field to enter your personal notes, the contents of this field is not used by NetOp.




Select a communication profile from the *Communication profile* drop down list. Use the reserved *<any initialized communication>* to communicate with the Host PC using any of the communication profiles which were initialized at startup (see section 4.13, 'Communication Profiles'). Depending on which communication profile you have chosen, an icon will represent the specified Host.




## 4.6.3 Login

The above dialog is designed to speed up connections to Hosts requiring password authentication or Gateway authentication (See section 4.21 'Security').

By filling in the Host/Gateway password you will not be prompted to re-enter them when initializing the connection.

For more information regarding the other tabs please refer to section 4.14 'Connection Properties'.

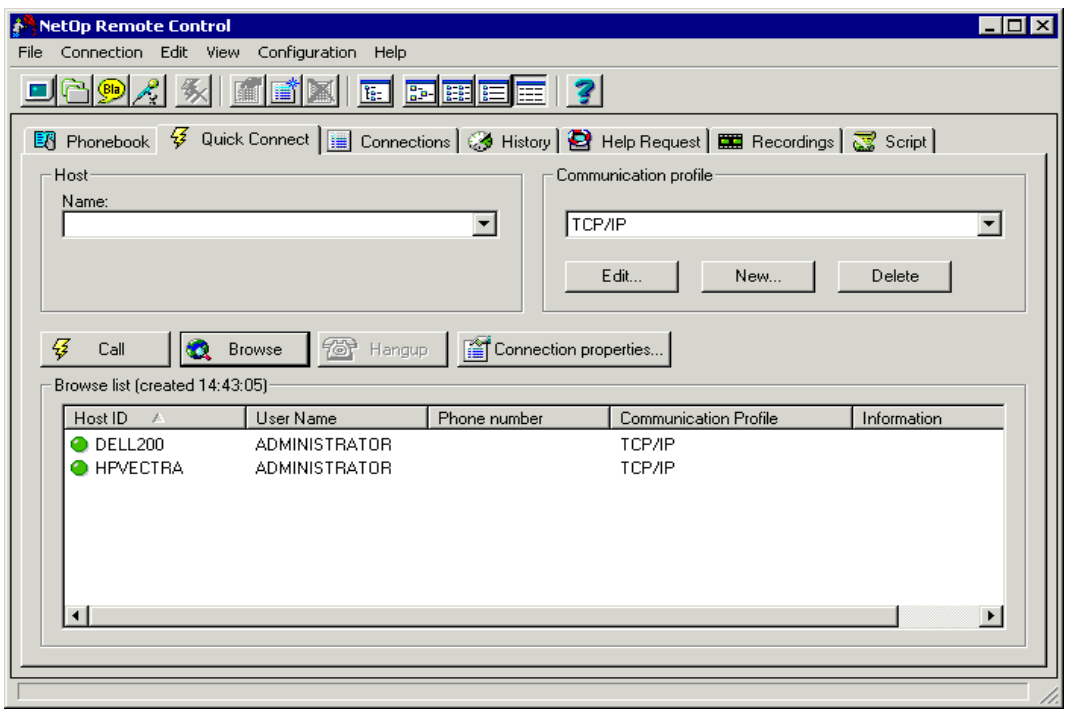
Once you have created a new Phonebook entry it will be saved in the corresponding directory on your drive as an *.DWC file (or NetOp connection file). Besides using the Phonebook utility within NetOp to connect to the Host you may also click on it's corresponding DWC file (which is associated with the NetOp Guest Program). This will then start the NetOp Guest program and automatically connect to the specified Host. You may also transfer *.DWC files between Guest PC's for sharing of Phonebook resources.

*Note: DWC files will only work if NetOp version 6.x or above is installed.*

By default the Phonebook folder is located as a subdirectory to the NetOp directory called '*phbook*'. To use a Phonebook at another location (e.g. shared on a server) specify this in the NETOP.INI file (See section 12.3 - The NETOP.INI File), in the entry `PhoneBookPath=` in the `[Guest]` section. The NETOP.INI file should be in your Windows directory.

## 4.7 Quick Connect

The following figure shows the *Quick Connect* tab:



## 4.7 Quick Connect

There are three main parts to the Quick Connect Tab:

**The Host**

**The Communication Profile**

**The Browse List**

Specify communication information necessary to reach the Host by selecting it from the *Communication profile* drop down list.

Depending on which communication profile you have chosen, the *Host* section of the dialog box will contain either a *Name* field (network) or a *Phone number* and a *Name* field for dial-up and Outgoing Gateway connections.

### Network (IPX, NetBIOS, TCP/IP (UDP))

Enter the name of the Host in the *name* field. Activate the drop down list to see a list of previously entered Host names.

### Dial-up (Modem, ISDN, TCP/IP (TCP), IrDA) / Gateway

For ISDN and modem, enter the phone number in the *Phone number* field, leave the *Name* field empty. If you are going to call the Host via a NetOp Gateway enter the Gateway's phone number in the *Phone number* field and enter the name of the Host in the remote network in the *Name* field, or leave the *Name* field empty.

For TCP/IP (TCP), enter the IP address in the IP address field instead of the telephone number and treat the name field as above. For infrared, there is only the name field.

You can select the reserved profile *<any initialized communication>*, this tells NetOp to look for Hosts on any of the communication profiles (if any) that were selected for initialization at startup in the *Initialize communication* dialog box (see section 4.13.1., 'Initialize communication'). If a Host is already being controlled the communication device used by this communication will also be available via the *<any initialized communication>* profile.

If no profiles are initialized yet *<any initialized communication>* will not appear in the list.

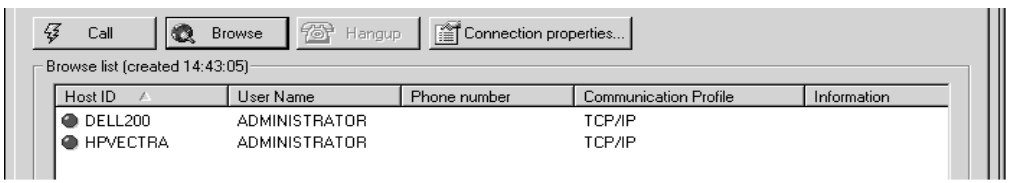
Use the *Connection Properties* button to activate the Connection Properties dialog box, this lets you change various options related to the Host PC. See section 4.14, 'Connection Properties' for a detailed description of this.

Pressing the *Call* button executes the default action, you may also choose another type of session by using the Toolbar, or Menubar.

## 4.7.1 Browsing for Hosts

NetOp includes a browse facility which lets you scan the network for available NetOp Host PCs.

Choose a communication profile from the *Communication profile* drop down list and activate the *Browse* button. The Guest will now scan the network using the specified communication profile and present a list of available Host PCs (see the following figure):




Choose the reserved communication profile name *<any initialized communication>* to browse for PCs on all initialized communication profiles. If you enter a string in the name field before browsing, the Guest will find Host PCs starting with this string. For instance you can enter a *p* to find all Host PCs with names starting with the letter p.

To browse a remote network through a NetOp Gateway, choose the communication profile needed to access the Gateway (typically a modem profile) and enter the phone number of the Gateway in the *Phone number* field, then click *Browse*.

The browse list will then show you available Hosts.

Hosts on the browse list will be represented by one of the following icons

**A Green Light** - The Host is ready to be remote controlled.

**A Red Light** - The Host is already controlled by another Guest

**A Yellow Light** - Status unknown.

If you browse using a dial-up communication profile, the *Hangup* button will be activated. The Hangup Button is used to hangup the connection instead of connecting to one of the Hosts on the list. The Hangup button is disabled when a connection is started to one of the Hosts in the list. When the connection to this Host is terminated, the connection is automatically hung up.

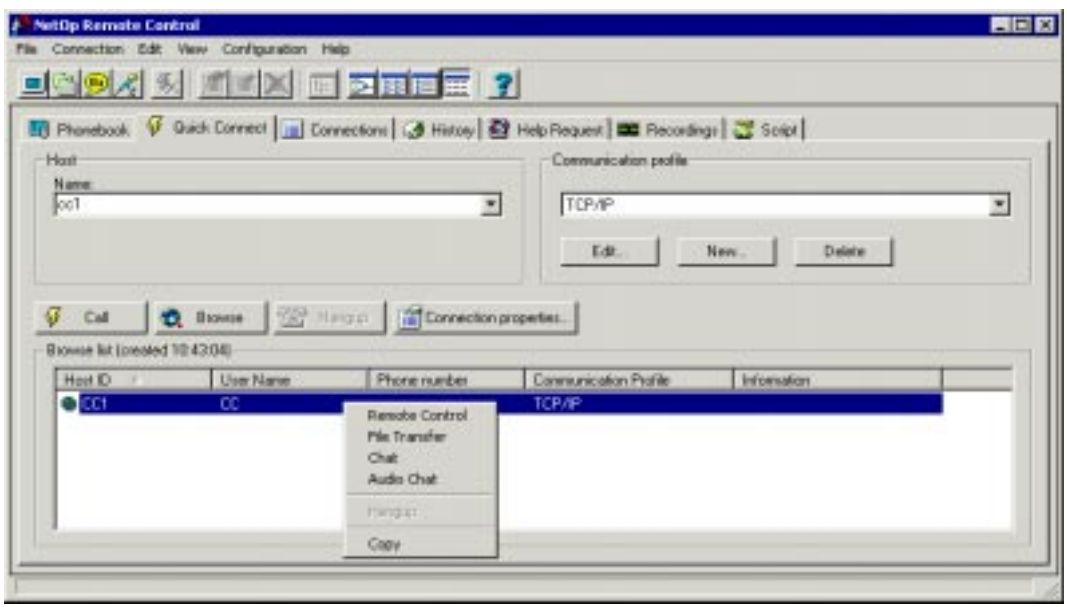
## 4.7 Quick Connect

The browse list includes a column header, which allows for arrangement by either Host ID, User name, Phone number, or Communication Profile.

You may also select different views of the browse list (Small/Large Icons, details, etc.) From the corresponding icon in the Toolbar.

To connect to a Host PC on the list, select it with the mouse or by using the arrow keys and activate the *Call* button. You can also connect to a PC by double clicking on its name with the mouse. This will initiate the default action set in the Connection Properties (See section 4.14.1).

You may also Right-Click on a Host from the browse list to select a particular action to initiate (see the following figure):




To save the browse list select the PCs you want to save. Select *Copy* from the popup menu that appears, when you right click in the browse view. You can now paste the files to the phonebook, the desktop or to any other folder.

## 4.7.2 Calling through an Outgoing Gateway

To make a call using NetOp's outgoing Gateway functionality you must select a Gateway communication profile (for more information regarding Gateway communication profiles please refer to Section 11.6 'Gateway Profile').

The phone number needed to reach the remote Host must be entered in the *Phone Number* field. You may also enter a Host name in the Host name field (optional if the call is to be routed through an Outgoing Gateway to an Incoming Gateway).

After pressing the Call button the user will be presented with a list of Outgoing Gateway Device Groups available on the network (unless a default device group has been selected in the *Gateway* communication profile) as shown in the following figure:


After selecting a device group to route the call, the Guest will be connected to either the remote Host or incoming Gateway at the other end of the Outgoing Gateway.

In a sense a 'Gateway' communication profile will simulate a dial-up connection from a Guest that is only connected via a networking profile. The actual dial-up connection will be made "transparently" on the Outgoing Gateway.

### Browsing using an Outgoing Gateway

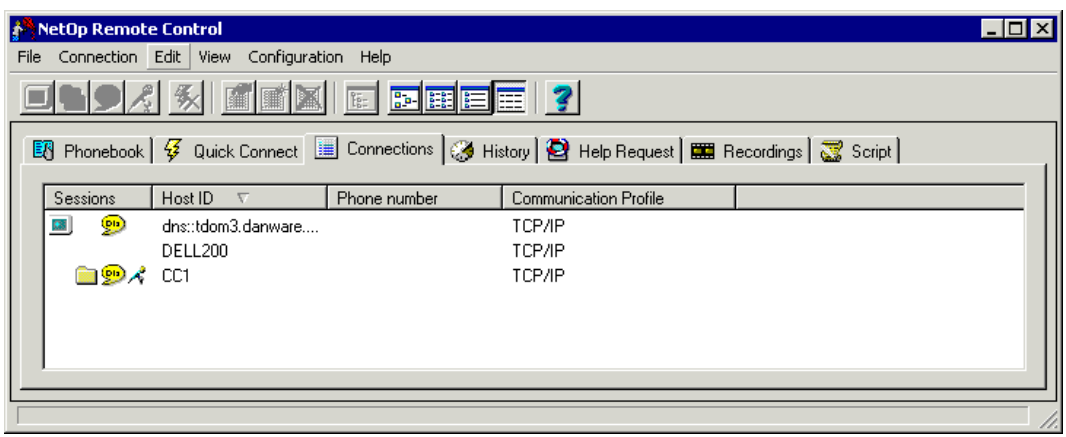
It is also possible to browse for Hosts using an Outgoing Gateway. Do this by selecting a *Gateway* communication profile, enter a phone number in the *Phone Number* field then press the *Browse* button. If the Host at the other side of the Outgoing Gateway is a standard Host, the Guest will automatically be connected to it. If the Outgoing Gateway connects to a regular (or Incoming) Gateway the browse list will be presented showing all available Hosts on the remote network.

To remote control a Host from the Gateway Browse list simply select it from the list.

For more information regarding Outgoing Gateway functionality please refer to Chapter 10 'The Gateway'.

## 4.8 Current Connections List

The following figure shows the *Connections* List Tab:



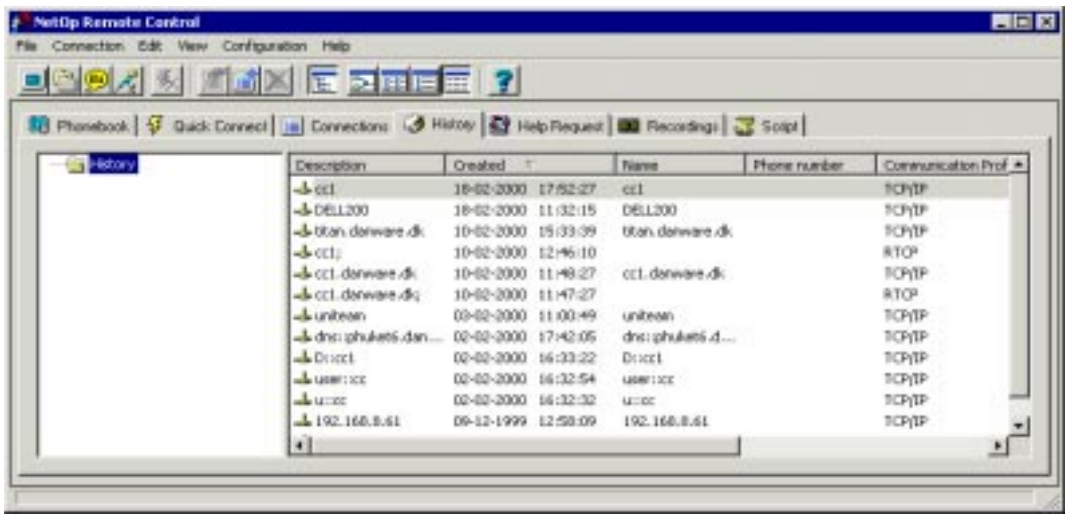

The *Connection* tab lists Hosts that are currently connected to the Guest. Using the Connections List it is possible to view all active connections and type of session initiated with each Host. The session type is represented by an icon (to the left of the Host ID). As in other tabs it is possible to select different views of the connections list by selecting the corresponding icon in the Toolbar.

A column header allows for organization by either session type, Host ID, phone number or communication profile.

As in the Phonebook it is possible to initiate remote control, chat, Audio Chat, and file transfer session with currently connected Guests. To do this select the corresponding icon from the Toolbar or Menubar.

## 4.9 The History List

The following figure shows the *History* List:




The History List presents the user with a list of Hosts previously connected to by the Guest. To reconnect to any one of the Hosts use the same procedures described in the Phonebook and connections sections. (Using the Toolbar or right clicking on the Host and selecting a particular action).

The History list stores the connection information of the Host at the time of last successful connection.

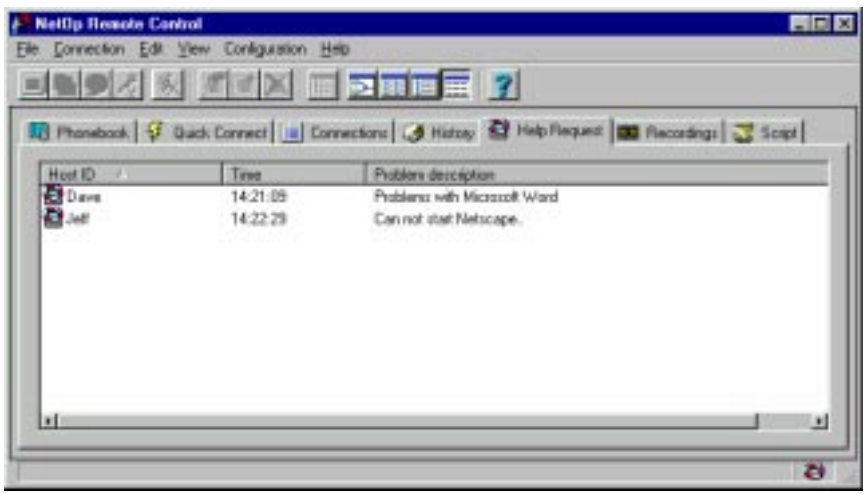
History entries are added to the root directory of the History list. A previous entry for the same Host will then be overwritten. You can create subdirectories to the History root directory and move the entries to prevent overwriting and save them for your records.

The same organizational methods that apply to the Phonebook apply to the History List. You may view the left window pane containing directories and subdirectories, and select different views and sorting methods. (Please refer to the Phonebook section 4.6 for more information.

By default the History folder is located as a subdirectory to the NetOp directory called '*History*'. To use a History folder at another location (e.g. shared on a server) specify this in the NETOP.INI file, in the entry `HistoryPath=` in the `[Guest]` section. The NETOP.INI file should be in your Windows directory.

## 4.10 The Help Request Tab

The following figure represents the *Help Request* tab:




NetOp contains an advanced *Help service* feature, which is designed to ease the process of providing on-line support.

It is possible for a NetOp Guest to register as a *help provider*. Hosts can then request help from the registered providers.

To register a Guest as a Help provider choose the *Help Service Tab* from the *Program Options* menu. In the resulting tab it is possible to enter three *Help services* (For more information please refer to section 4.4.8). Leave all three help services empty or check the *Disable help service* check box to turn off help service.

A Help service could be the name of a specific application this Guest wants to provide support for. Or it could be the name of the person providing the support. Whenever a Hosts activates the *Call Guest for help* function it will be presented with a list which contains all help services registered by any Guest.

When a request for help from a Host is registered, it can be viewed from the *Help Request* tab, it will also be accompanied by a sound alert and an icon in the Guest PC's system tray. Each line represents one request, with the Host ID, the time the request was made and a problem description entered by the Host user when the request was made. The list is continuously updated, requests are automatically removed if they have been serviced by a Guest or cancelled by the requesting Host user.

*Note: As in previous tabs it is possible to arrange the Help Requests by using the column header and use different views (such as small/large icons, details, etc.)*

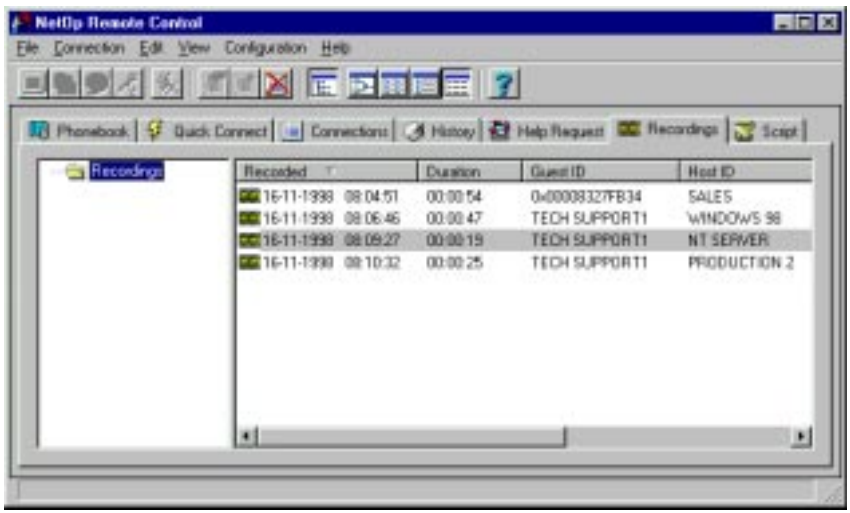
To answer a help request double click the line in the request window . This will initiate the default action (set in the *Connection Properties* See section 4.14.1) with the Host that made the request. You may also choose to select an option from the Toolbar or right click on the Help Request and select an action from the resulting menu.

Multiple Guests can provide help service simultaneously. They can even register the same help services. If for instance multiple Guest services register the service *Excel support*, this service will appear once on a Host's list of services. If the Host requests help from this service, the request will appear in the request window on all the Guests which registered *Excel support*. When one of the Guests answers the request, it will dynamically be removed from the list on the other Guests.

Please note that in order to receive help requests via any given communication device, that device must be initialized at startup. Refer to section 4.13.1, 'Initialize communication' for a description of this procedure.

# 4.11 Session Recording

The *Session Recording* tab is represented in the following figure:




The NetOp Guest program includes a Session Recording utility which allows the Guest to record any remote control session with a Host (including screen transfers, mouse movements and keystrokes) and play back those recordings.

To record a particular remote control session with a Host please refer to section 4.14.6.

## 4.11.1 Session Recording Listing Window

The right window pane presents recordings located at a particular folder in the directory window pane by the user (similar to windows explorer).

To playback a recording simply double click on it in the recording listing window pane of the Session Recording tab or right click on a recording and choose Playback from the resulting menu. The right window pane (or recordings window pane) also contains a column header which allows the user to arrange the different recordings by either date recorded, duration, Guest ID, Host ID, description. To arrange recordings by a particular

category simply click on the corresponding tab. You may also choose different views of Hosts by selecting the corresponding icon in the Toolbar. (Large icons, small icons, details, etc.).

Once you have recorded a session it will be saved in the corresponding directory on your drive as an *.DWR file. Besides using the Session Recording utility within NetOp to playback a recording you may also click on it's corresponding DWR file (which is associated with the NetOp Guest Program). This will then start the NetOp Guest program and automatically playback the specified recording. You may also transfer DWR files between Guest PCs.

To use a Session Recording directory at another location (e.g. shared on a server).

Specify this in the NETOP.INI file (Section 12.3 'The NETOP.INI File'), in the entry `Recordpath=` in the `[Guest]` section. The NETOP.INI file should be in your Windows directory.

*Note: DWR files will playback recordings only if NetOp version 6.x or above is installed.*

## 4.11.2 Recording Playback

When a particular session recording is played back, a new window will display the recording. The window will contain a Session Recording Toolbar (see the following figure) that can be used to navigate through the particular recording. As in the Guest Control Panel Toolbar the Session Recording Toolbar can be moved resized or otherwise manipulated.

The Session Recording Toolbar contains the following controls (left to right).

### Stop

Stop the current playback session and exit the particular session recording window.

### Pause

Pause the particular recording. To continue the playback session press the *Play* or *Pause* button again.

### Play

Click this button to playback the specific recording.

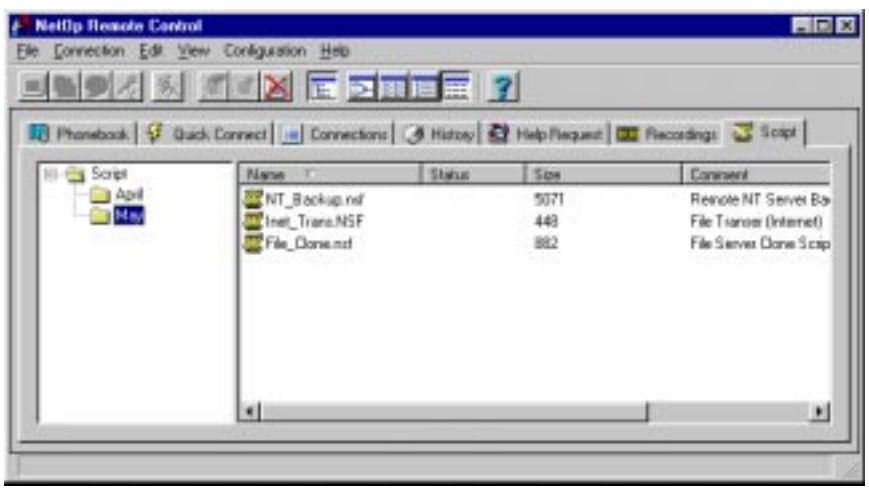
### Full Rewind

Restart the particular recording.

When viewing a recording in full-screen mode (pressing CTRL+Z), the Toolbox will contain a button allowing to return to windowed mode.

## 4.12 The Script Tab

The *Script* Tab is shown in the following figure:




The Script Tab allows for organization and maintenance of NetOp Scripting Files (or *.DWS files) created using the NetOp Scripting Utility (For more information regarding the NetOp Scripting utility please refer to Chapter 7).

The same organizational methods that apply to the Phonebook, History List, and Recording tab apply also to the Script Tab. The right window pane presents a Tree View of folders created by the user containing script files. You may also select different views of files using the corresponding icons in the Toolbar or by using the Menubar. For more information regarding organizational methods within tabs please refer to Section 4.5 ‘Guest Control Panel Tabs’.

From the right window pane or the 'Script Listing' window pane, you may select one of several actions by right clicking on the particular script file.

### Run/Stop

By selecting these options you may choose to either Run a script or Stop a script that is running at the moment. The status of a script can be viewed in the Script Listing window's column header when 'Detailed' view is enabled.

### Edit

Selecting this option will bring up the NetOp Scripting Utility, allowing you to edit actions within the particular script.

### New Script

Selecting this option will bring up the NetOp Scripting Utility allowing you to create a new script. You may also choose to create a new folder as in the Phonebook, History List, and Recordings tab.

By default NetOp places script files in a directory called 'Script', which is a subdirectory to the NetOp program directory. To use a script directory at another location (e.g. shared on a server), specify this directory in the NETOP.INI file (Section 12.3 'The NETOP.INI File'), in the entry `Scriptpath=` in the `[Guest]` section. The NETOP.INI file should be in your Windows directory.

## 4.13 Guest Communication Profiles

A communication profile is simply a collection of information about a communication device.

*Note: Communication Profiles are explained in more detail in chapter 11.*

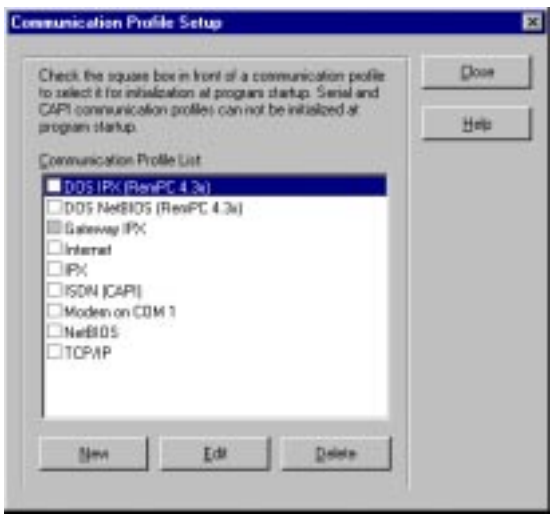
A communication device is a protocol or interface NetOp can use for communication (e.g. NetBIOS or serial).

By collecting all information about a device (or interface) in a communication profile NetOp makes it easy to quickly switch between communication setups.

## 4.13 Guest Communication Profiles

NetOp comes with a number of predefined communication profiles, one for each supported device except TCP/IP(TCP).

To maintain the communication profile database select *Communication profiles* from the *Configuration* menu. This activates the following dialog box:




*Note: You may also edit, delete or create a new communication profile in the communication profile section of the quick connect tab.*

The list shows you the existing records in the database. They are always sorted alphabetically. Each communication profile has a check box that allows any profile except Gateway to be initialized at program startup. See section 4.13.1, ‘Initialize communication’.

### Inserting

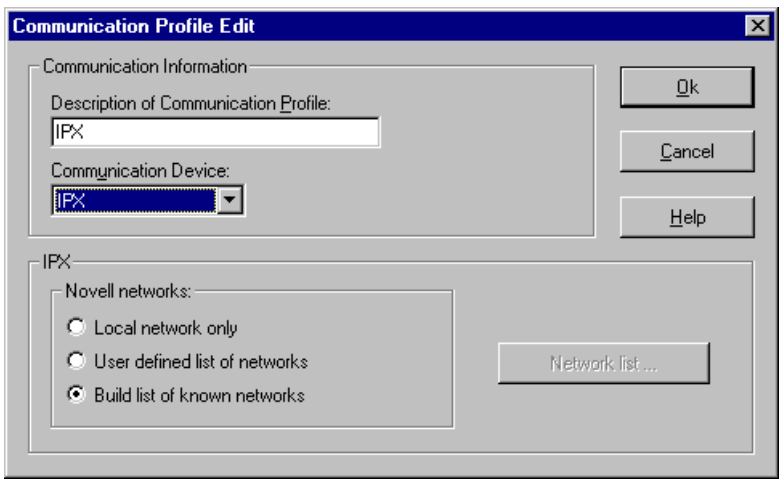
If you activate the *New* button (or press ALT+N), you will add a new record to the database. Its contents will be similar to the selected record’s (except for the name which will be blank).

### Deleting

You can delete records by clicking the *Delete* button (or by pressing ALT+D on your keyboard).

### Editing

If you activate the *Edit* button (or press ALT+E) you will edit the selected record. A new dialog box will appear (see the following figure):




### Description of Communication Profile

This is the name with which you wish to identify the current communication profile.

### Communication Device

Choose the communication device to use for the profile. It can either be NetBIOS for Microsoft/IBM networks or compatible, IPX for Novell networks or compatible, TCP/IP (UDP) or TCP/IP (TCP) for IP networks, Windows modem, serial or null modem communication, ISDN for communication on an ISDN network with a CAPI compatible adapter, IrDA for infrared communication or a ‘Gateway’ Communication profile for use with an outgoing Gateway (See Chapter 10 - ‘The Gateway’).

The following devices are dial up devices which only allow a point-to-point connection: Serial, Windows modem, ISDN, Infrared and TCP/IP (TCP). The following devices are networking devices which allow browsing: TCP/IP (UDP), IPX and NetBIOS. Consult your system administrator if you are in doubt about which device you should use for communication.

### Device specific

In the lower part of the dialog box you will find parameters which vary with the communication device you have chosen. Please refer to Chapter 11 - 'Communication Profiles' for a description of the various device specific settings.

## 4.13.1 Initialize communication

Before a communication profile can be used to reach another PC it has to be initialized. NetOp's default way of handling this is to initialize a given profile whenever it is needed and then de-initialize it when done.

It is also possible to have networking communication profiles initialized when the Guest launches. Communication profiles initialized this way remain so until the Guest program is terminated.

Initializing communication at startup serves several purposes:

When *browsing* (scanning a network for Host PCs), NetOp can look for PCs on any initialized network, this allows for simultaneous scanning for Hosts on multiple devices.

Calling and browsing is faster on a communication profile which is initialized at startup. This saves the time it takes to initialize the device for every call/browse.

When using the *help service* (see section 4.10, 'Help Service') facility the NetOp Guest will accept Help Requests only via communication profiles which are initialized at startup.

You can choose which profiles to initialize from the *Communication Profile Setup* dialog box.

To include a communication profile in the group of profiles that are initialized at startup, check the box next to the communication profile in the list.

Note that it is not possible for a *communication device* to be initialized multiple times simultaneously. As a result of this you will get a warning if you try to select the same kind of communication device more than once. Please note that if you have more than one IP address in your computer you can specify the addresses in the communication profiles and thus initialize several TCP/IP configuration profiles at the same time, or have several NetBIOS communication profiles initializing several adapters at the same time.

Changes in the *Initialize communication* setup take effect from the next time the Guest is started.

## 4.14 Connection Properties

A number of options are set from the *Connection Properties*.

At first when a Host is called, NetOp uses the settings specified by the user from:

**The Phonebook:** The Connection Properties are specified by right clicking on any Phonebook entry and choosing Connection Properties from the resulting menu. Or by clicking on the corresponding button in the Toolbar.

**The Quick Connect Tab:** The Connection Properties are specified by clicking the Connection Properties button. These settings will apply to both manually entered Hosts and Hosts in the browse list.

**The History List:** The Connection Properties are specified by right clicking on any history entry and choosing *Connection Properties* from the resulting menu.

**The Help Request Tab:** The Connection Properties are specified by right clicking on any Help Request Entry and choosing Connection Properties from the resulting menu.

During a remote control session, the Connections Options can be changed by right clicking on the title bar of the corresponding Remote Control Window then selecting *Connection Properties*. This can also be done from the system menu in the title bar. In the Phonebook the connection properties apply to the properties of the particular Host at the last hangup.

## 4.14.1 Startup

The following figure represents the *Startup* connection properties tab:


### Host Window Startup Size

Use this option to define the mode of a Host Window when it is first connected to. You may choose to view the Host in full screen mode, windowed, minimized or maximized.

### Actions

**Lock Host keyboard and mouse**

When this option is selected NetOp will lock the Host keyboard and mouse immediately upon connection to it. Users at the Host will not be able to activate the Host mouse and/or keyboard locally.

**Blank Host Display**

When this option is selected NetOp will blank the Host screen immediately upon connection to it.

## 4.14.2 Display

The following figure represents the *Display* connection options tab:


### Host window fit

**Fit window to Host screen**
When this option is selected, the window displaying the Host window will have the same size (number of pixels) as the Host screen. The window can be resized, however, it cannot be larger than the Host screen. If the window is resized to be smaller than the Host screen, scroll bars will appear allowing you to see the entire Host screen.

**Fit Host screen to window**
When this option is chosen the entire Host screen will be displayed in the window. The Host screen will occupy the entire window. NetOp might need to shrink or stretch the Host screen bitmap depending on the height and width of the window and Host screen.

**Do not fit**
When this option is chosen the Host window will not change its size according to the Host screen. Neither will the Host screen be stretched to fit the Host window. If the Host window is larger than the Host screen, the surplus area will be painted black. If the window is smaller than the Host screen the scroll bars will be added to the window.

### Limit number of Host display colors

This lets you specify how many colors should be transferred from Host to Guest. Choose a higher number of colors for higher realism, a lower number for better speed. This setting only has effect if the *Host screen transfer* is set to *Transfer Host screen as bitmap.*

### DOS Box Font

This setting is used to change the font NetOp uses when the Guest displays a full-screen command prompt from this Host. You can check *System default* to let NetOp use the normal system font, or you can press *Select font* to choose another typeface and/or font size.

NetOp uses monospaced (fixed) OEM fonts. If you are not satisfied with the available fonts you might want to obtain additional 3rd party fonts.

## 4.14.3 Keyboard and Mouse

The following figure represents the *Keyboard and Mouse* connection options tab:

### Remote / Local Keyboard

Use this option to choose whether special key combinations are transferred to the Host or executed locally on the Guest. The combinations are ALT+KEY combinations and CTRL+ESC/ALT+TAB/ALT+ESC/WINDOWS KEY.

### No Keyboard Control

Choose whether the Guest should be able to remote control the Host keyboard. Use this option e.g. when remotely monitoring mission critical servers, when you do not want to run the risk of accidentally sending fatal keyboard combinations to the Host.

### Remote/Local mouse

In remote mouse mode, the Host's mouse will always follow the Guest mouse. Use this method if the Guest user is instructing the Host user on how to accomplish a task which involves the mouse. The remote mouse method is also required if you want the Guest mouse to follow the shape of the Host mouse. The Local mouse option is used to save bandwidth, and increase performance. When the guest mouse pointer (the local mouse) is moved, this action will not be transmitted to the host. As soon as a mouse button is activated, the Host's mouse position will be updated to the local mouse position and the click will be executed. This method yields high performance, since mouse activity generates a minimum of communication traffic.

### No mouse control

Mouse actions are not transferred from the Guest to the Host.

### Display Host mouse movements

By selecting this option a user at the Guest PC will be able to view all mouse movements as they appear on the Host (This includes mouse movements initiated by a user at the Host PC).

## 4.14.4 Compression

The following figure represents the *Compression* connection options tab:


### Compression level

The level of compression decides how much processing NetOp uses for reducing the amount of data to be transmitted between the Guest and the Host. The slower the communication device and the faster the PCs, the higher compression one should generally use. Normally you should select *Automatic*. On slow WAN links you should manually select *high*.

### Host screen transfer

The NetOp Remote Control Host has two different routines for reading the screen of the Host PC. Choose between the routines in the *Host screen transfer* section.

To change the mode when connected you *must* disconnect and reconnect after changing the mode.

**Transfer Host screen as commands**
This mode is usually faster but demands well behaved applications and drivers. The Host must be a Windows 3.1x, Windows 95/98/2000 or Windows NT 3.51/4.0 PC for this mode to work. If the Host is a Windows NT 3.1/3.5 or OS/2 PC, the Host screen will be transferred as bitmap – even if *Transfer Host screen as commands* is selected.

**Transfer Host screen as bitmap**
This mode has a higher level of compatibility but is typically slower. Use this mode if you have problems updating the screen (entire screen or part of screen is black/does not update).

### Cache

Use this setting to designate the size (in Kbs) which is used to store cached bitmaps in. Using *Cache* will normally increase performance but requires the specified amount of memory. The default cache is set to *Automatic*.

## 4.14.5 Desktop

The following figure represents the *Desktop* connection options tab:

### Optimize screen transfer

This section determines when the options in the *Optimization parameters* (see below) are to be used.

Select *Always* for the optimization parameters to be used on every connection to a Host machine.

If *Only when high compression* is selected, the optimization parameters will only take effect when *High compression* has been selected in the *Compression* dialog. This is normally used to optimize the speed across a slow line.

If you wish to disable the optimization parameters from being used, select *Never*.

### Optimization parameters

This section is used to define which settings should be optimized on the Hosts desktop.

Choose between Full optimization and Custom optimization. The available options are described below.

**Disable wallpaper**
Select this option to disable the Host's wallpaper setting. This will not change the pattern settings, as they are usually small and do not cause a problem.

**Disable screen saver**
Select this option to disable any screen savers set on the Host machine. This does not remove any passwords that have been assigned to screen savers.

**Disable animation gimmicks**
Select this option to disable the animation that takes place when minimizing or restoring applications and folders. This option is only applicable when controlling Windows 95/98, NT 4.0 and Windows 2000 Hosts.

On Windows 98 and Windows 2000 Hosts this option will also disable menu animation, combo box animation, list box smooth scrolling, and gradient title-bars.

**Disable full window drag**
Select this option to disable full window drag. This option is only applicable when controlling Windows 95 Plus!, Windows 98, Windows 2000 and NT 3.51/4.0 Hosts.

**Disable Active Desktop**

Select this option to disable the Active Desktop feature upon connection to Windows 95/98 Hosts and Windows 2000 / NT 4.0 Hosts where applies. Upon disconnection the desktop will return to it's original state.

Any of the desktop settings can be changed while remote controlling the Host. NetOp will return the Host's desktop settings to their original state when hanging up the connection.

## 4.14.6 Record

The following figure represents the *Record* connections options tab:


### Record remote control session

Enable this option to record a remote control session with a particular Host or Hosts. The Session Recordings can then be viewed using the Session Recording tab (please refer to section 4.11 'Session Recording').

## 4.15 Session Types

You can establish 4 different types of sessions with a Host:

1. Remote Control
2. File Transfer
3. Chat
4. Audio Chat

The different session types can be started independently of each other, and in all combinations.

For example - A support engineer upon receiving a Help Request can start a Chat session with the person sitting in front of the Host PC, he can then either start a Remote Control or File Transfer session depending upon the nature of the problem.

## 4.16 Remote Control

The following figure represents a Guest involved in multiple remote control sessions with different Hosts:

When connected to a Host PC, the Host screen will be shown in a new window created by the Guest (as shown in the above figure). The Guest's keyboard and mouse can be used to remote control the Host's keyboard and mouse.

The new window containing the Host's screen can be zoomed to full screen, resized or otherwise manipulated.

The following is a list of options offered during remote control.

## 4.16.1 Remote Control Toolbar

The following figure represents the Remote Control Toolbar:

The Remote Control Toolbar offers shortcuts to the most common commands used during a remote control session. It also offers the ability to start different session types with the particular Host being remote controlled.

By default the Toolbar will be located under the Remote Control Screen's title bar, but it can be moved and resized freely (as in the Guest Control Panel Toolbar).

The commands offered in the Toolbar are as follows (from left to right):

**Remote Control**

**File Transfer**

**Chat**

**Audio Chat**

**Hangup**

**Connection Properties**

**Full-Screen**

**Send Ctrl+Esc**

**Send Ctrl + Alt + Del**

**Restart Host**

**Send Clipboard**

**Receive clipboard**

**Marker mode**

**Blank Display**

**Lock Keyboard and Mouse**

*Note: To use the Toolbar it must be enabled in the Remote Control Section of the Program Options.*

## 4.16.2 Full Screen Toolbox

When remote controlling a Host in full-screen mode a Toolbox similar to the Remote Control Toolbar will be displayed. This Toolbox contains shortcuts to the most common remote control commands. It also offers the ability to start different sessions with the particular Host.

*Note: To use the Toolbox it must be enabled in the Remote Control Section of the Program Options.*

## 4.16.3 Send Keystrokes

Some key combinations can not be intercepted on the Guest and must therefore be sent manually using the *Send Keystrokes* commands. ALT+TAB and CTRL+ESC can also be sent using Hotkeys.

Click on the Host Remote Control Window's title bar or system menu then choose *Send keystrokes* from the resulting menu.

When *Send keystrokes* is selected, a sub-menu will appear showing the available options.

### Send Ctrl+Esc

This command activates the task list on operating systems such as Windows 3.x and OS/2. Using this command when controlling a Windows 95/98/2000 or NT 4.0 Host will activate the Start button.

### Send Ctrl+Alt+Del

Sending this command to a Host can have various effects. For example, sending this command when controlling an NT Host will bring up the task manager, but sending the same command to an OS/2 Host will reboot the Host machine with no warning. This keystroke will not be transferred to Windows 95/98/2000 Hosts.

Do not use this command to reboot the Host PC, instead use the *Restart* option in the *Connection* menu.

### Send Alt+Tab

Choosing this option will send the Alt+Tab keystrokes to the Host which switches between the active windows on the Host's desktop in a clockwise order.

### Send Alt+Shift+Tab

Choosing this option will send the Alt+Shift+Tab keystrokes to the Host which switches between the active windows on the Host's desktop in an anti-clockwise order.

### Send Print screen

Choosing this option will send the print screen command to the Host. This option prints a copy of the whole screen on the Host PC and copies it to the clipboard.

## 4.16.4 Clipboard

### Send to Host

This option will send the contents of the Guest's Clipboard to the Host Clipboard where it can then be used as if it the contents were placed there locally.

### Retrieve from Host

This option will retrieve the contents of the Host's Clipboard to the Guest Clipboard where it can then be used as if it the contents were placed there locally.

*Note: This utility is intended mostly in conjunction with text and graphics being copied to the clipboard, files however can not be copied through the clipboard. If you wish to transfer files you may use the NetOp File Manager or Scripting Utility.*

### 4.16.5 Full Screen

Instead of viewing the Host screen in a window, it is possible to zoom to a full screen view. In full screen view, the Host window takes up the entire Guest screen. This gives the Guest the most realistic view of the Host.

The Host screen can be zoomed by right clicking on the Host Window title bar (or system menu) then choosing *Full screen* from the resulting menu or by pressing the zoom Hotkey (default value CTRL+Z).

Switch back from zoom mode by pressing the zoom Hotkey (default value CTRL+Z) or if the Toolbox is enabled you can click the full screen button or use the Toolbar.

### 4.16.6 Blank Display

It is possible for the Guest user to blank ("turn off") the Host PC's screen.

Right click on the Remote Control Window's title bar or system menu then choose *Blank Display* from the resulting menu, or select this options by pressing the corresponding button in the Remote Control Window Toolbar.

Please note that the Host program must have been configured to allow display blanking, otherwise the menu item will be disabled on the Guest. Refer to section 5.6, 'Security' for a description on how to configure Guest rights on the Host.

The blank display feature requires the Host PC's video adapter to be 100% VGA compatible. This feature is not available when controlling NT 3.1 Hosts.

Use this feature if you wish the person sitting at the Host PC not to see the activity taking place during a remote control session.

### 4.16.7 Lock Host Keyboard and Mouse

NetOp allows the Guest user to lock the keyboard and mouse on the Host PC.

Right click on the Host Window's title bar or taskbar then choose *Lock Keyboard and Mouse* from the resulting menu or choose the corresponding icon from the Remote Control Window's Toolbar.

Use this feature to prevent a user from interfering while working on a Host, e.g. when reconfiguring a server.

The Host keyboard and mouse are unlocked by Right clicking on the Host Window's title bar or system menu, then choosing *Lock Keyboard and Mouse* from the resulting menu, or by pressing the corresponding Toolbar button again.

The lock status is indicated on the menu. When locked, a check mark will be displayed next to the menu item, and the Toolbar button will be pressed.

Please note that the Host program must have been configured to allow lock of keyboard and mouse, otherwise the menu item will be disabled on the Guest. Refer to section 5.6, 'Security' for a description on how to configure Guest rights on the Host.

### 4.16.8 Restart Host

NetOp includes a feature which lets the Guest restart the Host PC. Right click on the Host Remote Control Window's title bar or Taskbar then choose *Restart* from the resulting menu, or select the corresponding button from the Remote Control Window's Toolbar.

A confirmation dialog box will be displayed to ensure that the Host PC is not booted by mistake.

Please note that the Host program must have been configured to allow Restart from the Guest, otherwise the menu item will be disabled on the Guest. Refer to section 5.6, 'Security' for a description on how to configure Guest rights on the Host.

### 4.16.9 Refresh

This option is used to redraw the Host's screen while remote controlling.

This may be necessary if problems occur when the Host screen is being updated on the Guest. If the Host's screen does not appear correctly, right click on the Host Window's title bar or system menu then choose *Refresh* from the resulting menu.

## 4.17 File Transfer

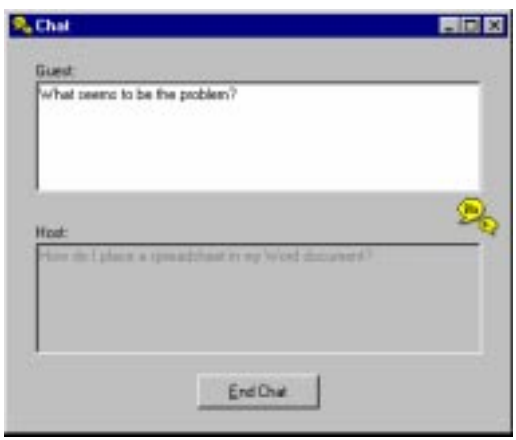
For more information regarding NetOp's File Manager utility please refer to Chapter 6 'File Manager'.

## 4.18 Chat with Host

The chat function brings up a window on the Host and Guest which allows the users to communicate.

Press the *chat* button located in the Toolbar to initiate a chat with a selected Host (see the following figure):

You may also choose *Chat* from the *Connections* menu, or right click on any Host from either the Phonebook, Connections, Quick Connect, History List, or Help Request menu and choose *Chat* from the resulting menu. This brings up the dialog box shown in the following figure:




A similar dialog will be displayed on the Host. Everything typed on the Host and Guest will be communicated between the users and displayed in the dialog boxes.

Please note that chat has to be enabled in the Host security settings (see section 5.6, ‘Security’), otherwise the chat button and the chat menu item will be disabled.

Chat can also be initiated by a Host, which is being remote controlled. Tthis will also bring up the chat window on both Host and Guest.

## 4.19 Audio Chat

NetOp includes an Audio Chat utility which enables a user at the Guest to communicate with the user at the Host side by using their respective PC's sound systems.

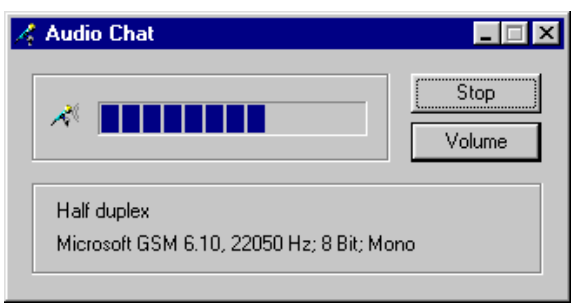
*Note: To use the NetOp Audio Chat feature both Guest and Host must have a sound card which has been properly set up, speakers and an input device (microphone).*

To start Audio Chat press the Audio Chat button on the Toolbar (see the following figure):

You may also choose *Audio Chat* from the *Connections* menu, or right click on any Host from either the Phonebook, Connections, Quick Connect, History List, or Help Request menu and choose Audio Chat from the resulting menu.

During an Audio Chat session, all audio picked by the Guest input device (or microphone) will be heard through the Host's output device (speakers) and vice-versa, allowing users to talk to each other or otherwise transfer audio data picked up by the respective audio input devices

During an Audio Chat the following dialog will appear:




Use the Audio Chat indicator at the top of the dialog to monitor current Audio Chat activity.

It is also possible to adjust sound levels by pressing the Volume button, this will bring up your system's volume control setup (for more information please refer to your operating system and audio device documentation).

The text box located at the bottom informs the user whether full or half duplex is currently being used and what type of audio compression codec applies to the current Audio Chat session.

To stop an Audio Chat session simply click on the *Stop* button located at the top right-hand corner of the dialog.

For more information regarding Audio Chat options please refer to section 4.4.5.

## 4.20 Remote Printing

The NetOp Remote Print facility allows a Guest to redirect a print job to a Host and vice-versa. This option is available for Windows 95/98, Windows NT4 and Windows 2000.

To utilize this facility you must first add a NetOp printer in the Remote Printing Program Options (see section 4.4.7).

Once you have added a NetOp Printer on the Guest, you are ready to send any print jobs to the Host PC. First you must establish a connection to one or several Hosts. This can be either a Remote Control session, File Transfer, Chat, or Audio Chat.

Once a connection has been established, a user at the Guest PC can print from any application running the Host PC by choosing one of the NetOp Remote Control Printers which have been added in the Remote Control Program Options. Depending on the settings you have chosen, the print job will be either sent directly to the Host's default printer or a dialog box will be displayed, listing all printers available on the Host. You can then choose, which printer the print job should be redirected to.

*Note: If you are printing from a NetOp Guest connected to more than one host, you are always prompted with a list of hosts to choose between. You can not redirect one print job to several Hosts simultaneously.*

## DOS Printing

To redirect a print job from a DOS application on the Guest PC to a Host printer you must do the following:

**Windows NT 4 and Windows 2000**

Share the NetOp printer as for example “myprinter”. Then, from the command line in a DOS box type the command below, where “mypc” is the name of your computer and “myprinter” is the name you shared the printer with. The reason for sharing the printer is only to enable the “net use” command to detect it, not to share it with others. If you do not share the printer, “net use” rejects to operate on the printer.

**net use lpt1: \\mypc\myprinter /persistent:yes**

**Windows 98/95**

Utilize the NRPWATCH.EXE program located in the NetOp directory. Open a DOS command prompt, change directory to the NetOp install directory and type NRPWATCH for an explanation on its usage. NRPWATCH requires that your third party application can print to a file instead of directly to a port.

Basicaly, NRPWATCH listens for files being saved in a directory of your choice. When a file is saved to this location, it detects it, prints it to a printer of your choice and deletes it. If the printer you choose is a NetOp printer, and if a NetOp connection is open, NRPWATCH will print your file on a remote printer.

If you wish a permanent setup, generate a DOS command line which does what you want following the NRPWATCH syntax, and add it to your Windows startup section.

# 4.21 Security

## 4.21.1 Logout

This option will only be available if the Guest is using an Access Server for authentication. It will enable the Guest to logout from the Access Server and login as the same or as a different user. When this option is selected you will be asked to confirm your action and the dialog in the following figure will be displayed:


To login as the same or a different user to the Access Server, enter the new Guest ID in the *Guest ID* field and enter the password for the user (if any) in the *Password* field. Press the *OK* button to continue.

If the *Cancel* button is pressed at this stage, you will be exited from the Guest program.

## 4.21.2 Change Login Password

The change login password option is used if you wish to change your password for logging into an Access Server. This option will only be available if the Guest is using an Access Server for authentication.

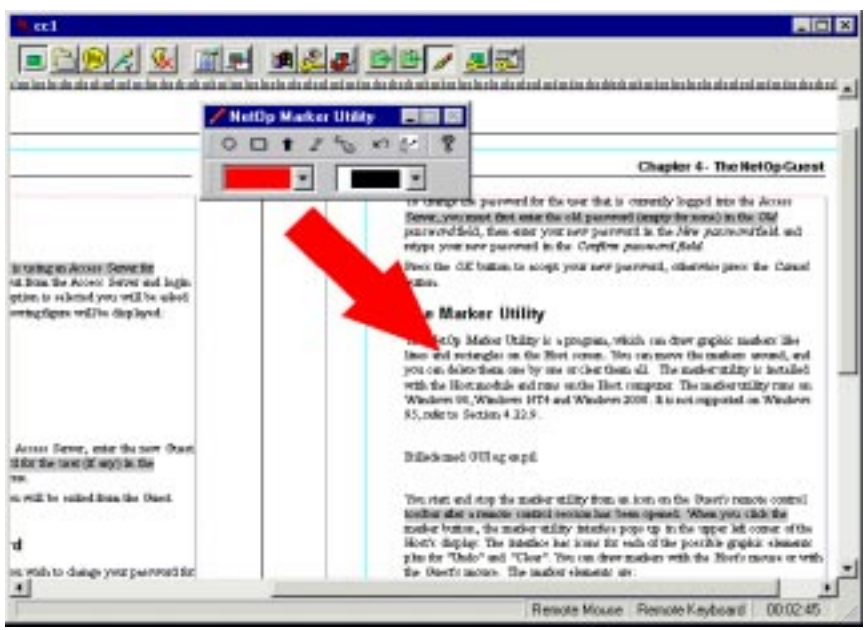
When this option is selected the dialog in the following figure will be displayed:

To change the password for the user that is currently logged into the Access Server, you must first enter the old password (empty for none) in the *Old password* field, then enter your new password in the *New password* field and retype your new password in the *Confirm password field*.

Press the *OK* button to accept your new password, otherwise press the *Cancel* button.

## 4.22 The Marker Utility

The NetOp Marker Utility is a program, which can draw graphic markers like lines and rectangles on the Host screen. You can move the markers around, and you can delete them one by one or clear them all. The marker utility is installed with the Host module and runs on the Host computer. The marker utility runs on Windows 98, Windows NT4 and Windows 2000. It is not supported on Windows 95, refer to Section 4.22.9.




You start and stop the marker utility from an icon on the Guest's remote control toolbar after a remote control session has been opened. When you click the marker button, the marker utility interface pops up in the upper left corner of the Host's display. The interface has icons for each of the possible graphic elements

plus for "Undo" and "Clear". You can draw markers with the Host's mouse or with the Guest's mouse. The marker elements are:

Straight lines

Freehand line

Rectangle

Ellipse

Arrow

You start drawing a marker by clicking its icon. The pointer will now change shape. Move the cursor to the start point and follow the instructions below for each single marker. When done drawing a marker, you must click an icon again, if you wish to draw another marker.

### 4.22.1 Drawing straight lines

At the start point, click MB1 (the left mouse button for right handed people). Move the pointer to the next point on your polyline, and click MB1 again. Repeat this as many times as you wish. When you want to end the line, press MB2 (the right mouse button for right handed people).

### 4.22.2 Drawing freehand

At the start point, press MB1 and keep it down. Move the pointer around with the mouse, and a line will be drawn following the pointer. Release the mouse button when you are done.

### 4.22.3 Drawing a rectangle

At the start point press MB1 and keep it down. Drag out the desired rectangle, and release the mouse button when done.

### 4.22.4 Drawing an ellipse

At the start point press MB1 and keep it down. Drag out the desired ellipse, and release the mouse button when done.

### 4.22.5 Drawing an arrow

At the start point press MB1 and keep it down. Drag out the desired arrow, and release the mouse button when done.

### 4.22.6 Color and Width

Below the toolbar, you will find two comboboxes, one for color and one for width. The selected color and width will apply to the next graphic element you create. The color and width of the elements you have already drawn, can be changed by right clicking each element, then selecting the new properties in the menus which appear. The size and shape of elements can't be changed, neither can you rotate them.

### 4.22.7 Deleting elements

You can delete an element by selecting the "Undo" command from the menu which pops up, when you right-click it. If you choose "Clear all" instead of Undo, all elements are erased. Undo and Clear all are also buttons in the toolbar. Here the Undo button will delete the selected element. When you draw an element, it becomes the selected one. If you later click on an element with MB1 or MB2, that element becomes the selected element. When an element is deleted, the element last drawn becomes the selected element.

### 4.22.8 Minimising the User Interface

When you minimize the NetOp Marker Utility, it places an icon in your icon tray, showing the kind of graphic element last drawn. If you click with MB1 on this icon, the same happens, as if you had clicked the corresponding icon in the toolbar. If you click with MB2, you have the option of restoring the original interface or drawing any specific graphic element.

### 4.22.9 The Marker Utility and Windows 95

The Marker Utility calls the Microsoft Windows API functions. On a classic Windows 95, even simple correct calls to a needed function eventually crash Windows' GDI.EXE and bring your machine to a halt. Therefore, the marker utility is disabled on Windows 95.

When installing application programs, especially Internet Explorer, you may have updated most or all of your operating system. On such a PC, the marker utility may work; we have had very mixed test results. If you want to experiment with the marker utility on Windows 95, you can set these lines in the [MARKER] section in your NETOP.INI file (use capitals only):

I_HAVE_UPGRADED_COMCTL32_TO_472=YES

I_ALMOST_TRUST_WINDOWS_REGIONS=YES

I_TRUST_WINDOWS_REGIONS=YES

The first line is needed to start the utility at all. You must make sure that the version of the file COMCTL32.DLL in your Windows system directory is 4.72 or higher. You can get updates from www.microsoft.com.

Next, you can try add the second line. This will tell the marker utility to use only simple function calls. If this works, you may try replace the second line with the third, and the utility will try run as on 98/NT/2000.

## 4.23 Command Line Options

The NetOp Guest can be operated directly from the command line, the complete syntax is:

NGSTW32 [/H:*name*] [/C:*prof.*] [*/P:Phone no*] [/R:] [/F:] [/V:] [/A:] [/B::file] [/S::file]

By using the command line options you can call a Host directly from the command line. If you wish to call by phonebookfile instead of computername, use

NGSTW32 /E:filename.dwc /R: (default path is phbook folder)

If one or more communication profiles are set to initialize at startup (see section 4.13.1, ‘Initialize communication’), you can leave out the /C: parameter. In this case NetOp will try to find the Host on any of the initialized communication profiles.

Examples:

To remote control a Host with the computer name *john* using the communication profile IPX, use the following command line:

NGSTW32 /H:john /C:IPX

To remote control a Host with the computer name *peter* via any initialized communication profile use the following command line:

NGSTW32 /H:peter

When connecting directly to a Host via dial-up (Modem or ISDN), the dial parameter should be used along with the number to dial. Use the /C: parameter to specify whether you are using Modem or ISDN. The Host name parameter is not used unless you are connecting directly via a Gateway. Use the following command line option with the relevant communication profile and phone number:

NGSTW32 /C:”Modem,Com1” /P:12345678

You can start a File Manager session by typing

NGSTW32 /E:filename.dwc /F:

Or a chat session by typing

NGSTW32 /E:filename.dwc /V:

Or an audio chat session by typing

NGSTW32 /E:filename.dwc /A:

Or start a script by

NGSTW32 /S:filename.dws (default parth is script folder)

Or edit a phonebook entry’s properties

NGSTW32 /E:filename.dwc

Or play back a session recording file

NGSTW32 /B:filename.dwr (default path is recordings folder)

# Chapter 5
# The NetOp Host

# 5.1 Summary

This chapter describes how to use the NetOp Host software. This is the NetOp module that enables a PC to be remote controlled.

Areas covered in the chapter include: How to start the Host, how to set up the Host, security configuration, and operation during remote control sessions.

For a description of how to install the Host please refer to chapter 2, ‘Installation’.

# 5.2 Introduction

## 5.2.1 Starting the Host

To start the NetOp Host do the following:

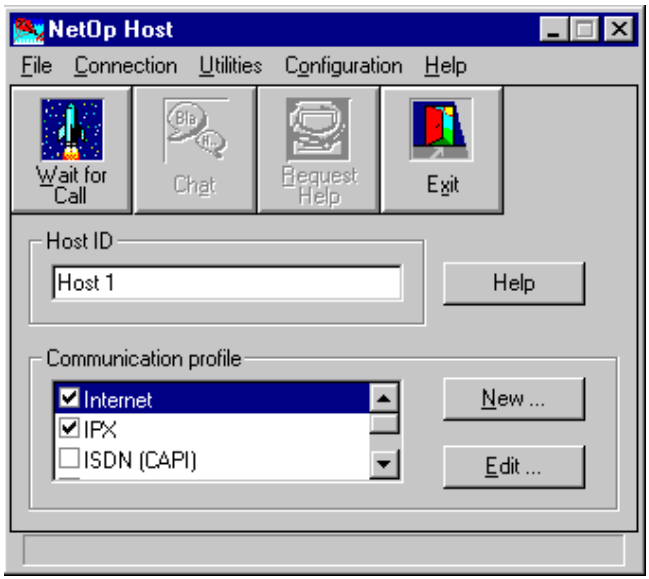
1. Open the program folder in which you installed NetOp.

2. Double-click the Host icon.

This will launch the program NHOSTW.EXE on Windows 3.x PCs or NHSTW32.EXE on Windows 95/98 Windows NT 4.0 / 3.51 or Windows 2000 PCs.

## 5.2.2 The Host Screen

An example of a running NetOp Host program is displayed in the following figure. This window is called the main Host dialog.




### Title bar

The title bar of the Host window contains a status message which dynamically changes. This status is also displayed with the icon when the Host is minimized. This feature lets the Host user know when a remote control session is active.

### Menubar

The Host program contains a Menubar where all NetOp commands are available.

### Toolbar

In the Toolbar (which is placed below the Menubar) shortcut buttons for the most common commands are available.

### Status line

The status line at the bottom of the NetOp Host window contains menu hints which show a brief description of the menu entry currently selected.

### Host ID

In this field the name of the Host is entered and displayed. This is the name that Guests will use to identify the Host.

### Communication profile

This is where the communication profile(s) are selected. The communication profile specifies a communication device and parameters related to that device.

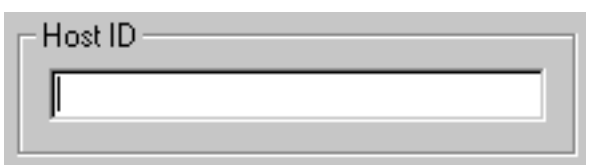
## 5.3 Configuration

### 5.3.1 Host ID

The Host ID is the name used by Guests to identify the Host. The default situation is that this field is automatically filled with theWindows computer name, so you will see a field showing the computer name, but it is greyed out.

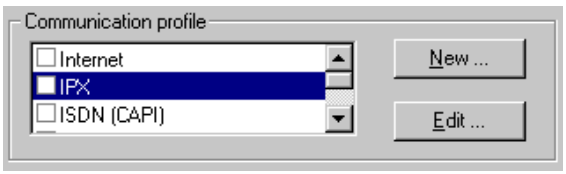
If you wish to specify your own string here, select *Enter name or leave name field blank* in the *Host Name* tab page of the *Program Option*s dialog. The field will now be enabled and you can type in a string, which is limited to 32 characters.

If an enabled Host ID field is left empty, the Host can still be called by IP address or DNS name when using TCP/IP, and by MAC address when using IPX or NetBIOS.



## 5.3.2 Communication Profile

This field defines the communication profiles that should be used to communicate with NetOp Guests (See Chapter 11, for a description of communication profiles).




Use the checkboxes to select one or more communication profiles. The Host will wait for calls on the profiles selected, when the *Wait for Call* button is pressed.

For example: A Host can Wait for call on both a modem profile and a TCP/IP profile allowing it to be accessed by Guests on it's LAN or users at remote locations contacting the Host via a modem.

*Note: A Host can not be controlled by more than one Guest at the same time.*

When you have entered the necessary information click the *Wait for call* button in the Toolbar (see the following figure) or choose W*ait for call* from the *Connection* menu.


To re-configure the Host after initialization activate the *Stop Host* button in the Toolbar (see the following figure) or select *Stop Host* in the *Connection* menu. Note that these options are only available when the Host is waiting for a call. After this you can change configuration settings which will be active the next time you select *Wait for call*.

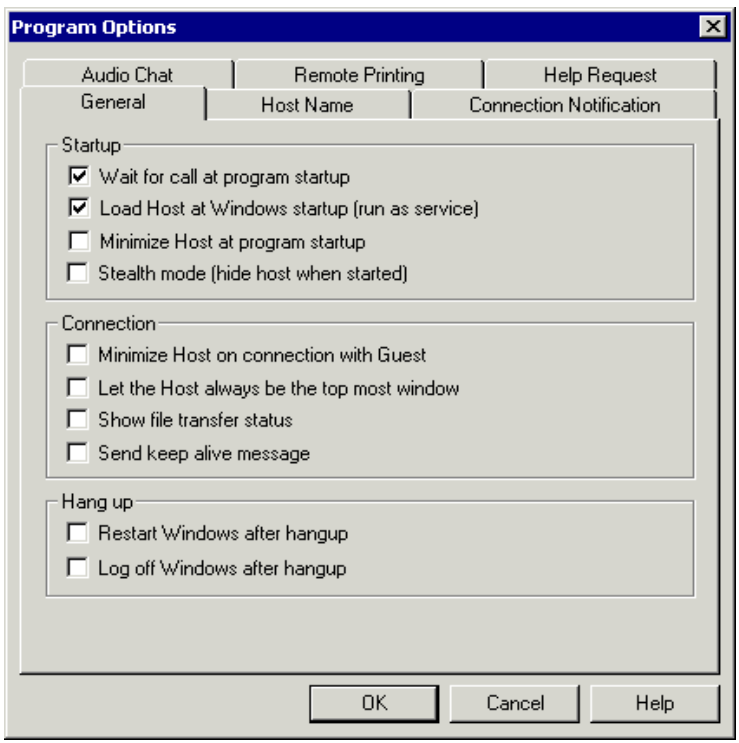
You can instruct the Host to automatically initialize at startup, see the following section 'Program options' for more details.

# 5.4 Program options

Select *Program options* from the *Configuration* menu to configure various Host options. This dialog is set in tabbed format containing six sections, *General, Host name*, *Connection Notification, Audio Chat, Remote Printing* and *Help Request*.

## 5.4.1 General

The following dialog box shows the *General* options tab:




### Wait for call at program startup

If this option is enabled, the Host will not wait for the user to enter configuration information when started but rather initialize with the configuration, which was used the last time the Host was run.

### Load Host at Windows startup

When this option is enabled the Host will automatically load when Windows starts. This option is normally used in conjunction with *Wait for call at program startup* and *Minimize Host at program startup*.

This option intelligently handles differences between Windows/Windows for Workgroups 3.1x, Windows 95/98, Windows NT and Windows 2000:

**Windows/Windows for Workgroups:** The Host is loaded via the RUN= line in the WIN.INI file.

**Windows 95/98:** The Host is loaded via the registry.

**Windows NT/2000:** A special 32-bit NetOp Host service is added.

This option will enable you to remote control the login screen of Windows 98/95 and NT/2000 PCs.

### Minimize Host at program startup

Enable this option to run the Host minimized. This setting is useful when the Host is loaded automatically.

### Stealth mode (hide Host when started)

This option allows the Host user to hide the Host program from view. The Host program remains invisible until a special program called “ShowHost” is run.

The ‘SHOWHOST.EXE’ program is found in the NetOp directory and can be renamed or copied to another location such as a diskette. This option takes effect when you restart the Host program.

### Minimize program on connection with Guest

When this option is enabled the Host will minimize whenever a Guest connects to it.

### Let the Host always be the top most window

When this option is enabled and the Host is being controlled, the Host window will always be on top (both as a window, and when minimized to an icon on Windows 3.x and NT 3.x). This makes it easier to know when a remote control session is active.

### Show file transfer status

This option allows the Host user to monitor a file transfer when initiated by the Guest.

### Send Keep Alive message

NetOp uses a non-polling communication technique. In a sense this means that if there is nothing to be sent between Guest and Host (e.g. keystrokes from Guest to Host or screen changes from Host to Guest) nothing will be sent. By checking this option you will be sure that a connection timeout will occur if there is a bad or unstable connection between the Guest and Host. This option should be unchecked if you want to take advantage of the CAPI short-hold-mode feature or if communicating through an ISDN router that should be shut down if there is no activity to save cost.

### Restart Windows after hangup

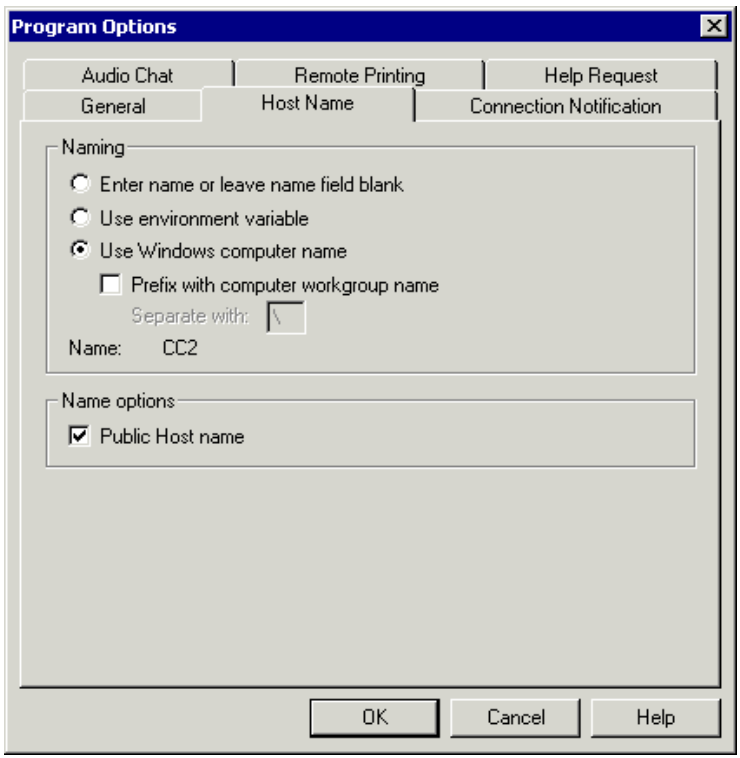
This option shuts down and restarts Windows after hangup. The shutdown is “unconditional”, which means that open programs will be closed even if they contain unsaved information or documents.

### Log off Windows after hangup

On Windows 2000/NT/95/98, you also have the possibility to log off Windows after hangup. If you have checked this option, NetOp will log you out of the computer when the connection is ended. If you also have checked *Wait for call at program startup* and *Load Host at Windows startup* another Guest can connect to the machine but gets the ‘Press Ctrl + Alt + Delete to log on’ prompt on Windows NT/2000 or the Windows 95/98 login dialogs.

## 5.4.2 Host Name

The following dialog box shows the *Host Name* options tab:




### Enter name or leave name field blank

Enable this option if you wish to enter your own name in the Host ID field or if you wish to leave the Host ID field empty.

If you leave the Host ID field empty, NetOp will use the machines MAC address if IPX or NetBIOS is enabled. If TCP/IP is used then NetOp will use the machine's IP address as the Host ID.

If a NetOp Gateway is being used and IPX, NetBIOS and TCP/IP are being used, NetOp will use the IP address as a way of identifying the Host on a browse list.

### Use environment variable

Enable this option if you wish to use the value of an environment variable as the Host name. When this option is selected, the name of an environment variable should be entered in the text field. Environment variables can be set in different manners depending on your operating system. Windows NT and 2000 allow you to define them from the Control Panel or from a DOS prompt, while 3.x/95/98 forces you to edit the AUTOEXEC.BAT file like for example this:

```
SET HOSTNAME=PETER
```

where HOSTNAME is the name of the environment variable, and PETER is the value assigned to it. If you now enter HOSTNAME in the text field, the Host's Host ID will be PETER.

A common trick is to use the environment variable USERNAME, which is automatically assigned the value of the name of the person who logged in. An environment variable may also be set in Netware Login Scripts (for more information see Section 12.2.1)

### Use Windows computer name

Enable this option if you wish to use your Windows computer name as a Host ID. This feature is useful as it identifies the Host with unique predefined names.

When this option is selected you have the opportunity of prefixing the computer name with the Workgroup name. There is also an option to choose the character that separates the computer and workgroup name. Enter this in the available field.

The Workgroup name option is not available when using Windows NT 3.x.

### Public Host name

The public Host name option decides whether Guests browsing for Hosts are permitted to find this Host when browsing.

## 5.4.3 Connection Notification

The following dialog box shows the *Connection Notifications* options tab:

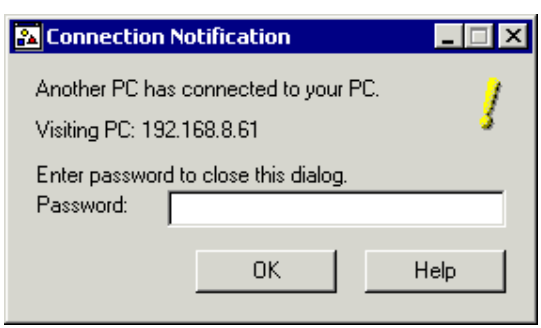

The Connection Notification settings provide various means for notifying the Host user about a connection. The Connection Notification settings are divided into three groups depending on the state of the connection.

**Upon connection**

The following options are available:

Play sound: If checked, the Host program will play a short tune.

Display notification message: If checked, the following dialog will be shown:



This dialog tells you that you are connected to192.168.8.61.

Password: If checked, the above dialog will be protected by a password that prevents the guest from removing the notification.

**During connection**

You have the following options:

Play sound: If checked, the Host program will play a short tune.

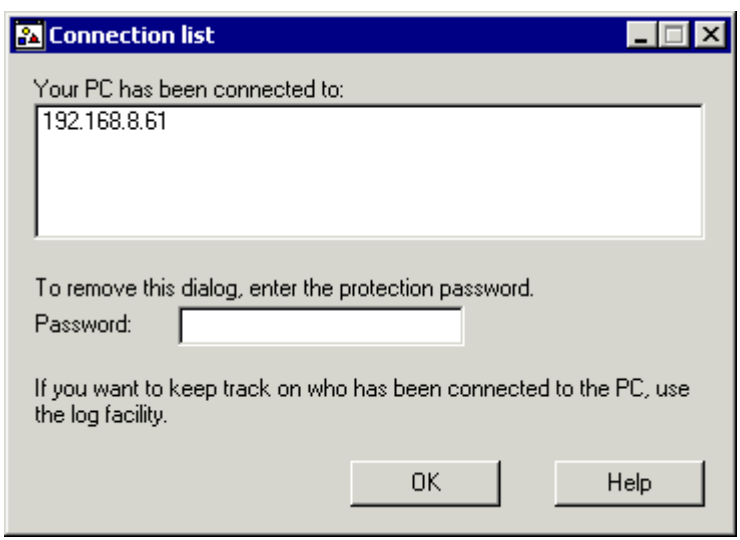
Interval: This tune will be repeated with the interval specified.

Display Guest name (if available) in the title bar: The Guest name will be shown in square brackets in the title bar as shown in the following picture.


**After connection**.

You have the following options:

Display notification message: If checked, the following dialog will be shown:



This dialog shows  that the Host has been connected to 192.168.8.61. If you close the dialog, the connection history will be lost. If you want a connection history you should use the NetOp log facility.

Password: If checked, the above dialog will be protected by a password that prevents the guest from removing the notification on subsequent connections.

The guest names displayed in the various dialogs is selected with the following priority:

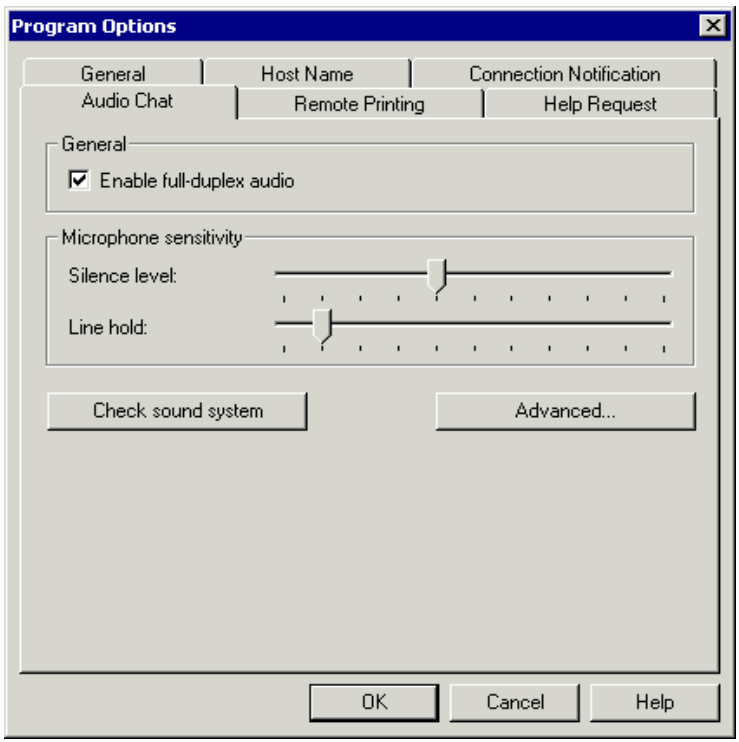
1 The login name from the NetOp authentication or from Windows Security Management authentication depending on the Guest Access Method.

2 The Guest ID.

3 Guest MAC or IP address depending on the protocol used.

## 5.4.4 Audio Chat

The following dialog box shows the *Audio Chat* options tab:




Use the *Audio* options to configure Audio Chat settings. For more info regarding Audio Chat see section 4.19.

### Enable Full Duplex

Select this option to enable full duplex sound for use with the NetOp Audio Chat feature.

Using Full-duplex enables a user at the Guest to talk to and hear a user at the Host PC at the same time. If this option is enabled NetOp will detect whether full-duplex is available and then use it.

*Note: Please consult your audio hardware documentation to verify that the particular sound device being used supports the full-duplex sound option.*

### Silence Level

The silence level thumb adjusts the Audio Chat silence level which refers to the audio level threshold that must be reached before a particular sound is picked up and used by the NetOp Audio Chat feature.

If full-duplex is not available or not used, NetOp must arbitrate the ownership of the microphone because the Guest and Host can not talk at the same time (similar to a walkie-talkie) i.e. The Guest must stop speaking before the Host can speak and vice-versa. For NetOp to release the ownership of the microphone it must be able to detect silence, which can not be completely attained because of background noise. Experiment with the thumb, by placing it in a position where nothing is sent when you are not talking, and everything is sent when you are talking.

If full duplex is used the silence thumb can be set in a low position so the microphone is turned on all the time. If you are communicating over a slow line (e.g. modem) you might want to experiment with the thumb to limit the bandwidth.

### Line Hold

Use this option to configure the amount of audio data, which is sent as “one-unit” across a communication link. For example, if a user is engaged in a normal vocal Audio Chat, the line hold will probably be set to medium or low, allowing for both Guest and Host modules to interact with each other without long delay times. The line hold should be set to high, if a user wishes to transfer a continuous piece of audio data over the link, as this requires a continuous stream of information for smooth play.

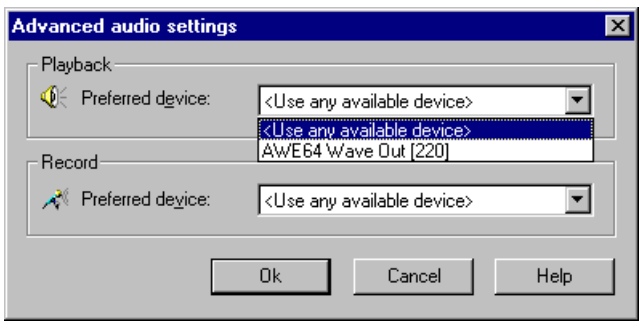
### Check Sound System

Use this option to check the current sound system installed on your PC for use with the NetOp Audio Chat feature.

*Note: Before initiating NetOp Audio Chat please make sure that you have configured all sound components and device drivers. For more info please consult your audio device hardware documentation as to available drivers and features of your particular audio device.*

### Advanced

The advanced tab allows you to configure both audio input and output devices. By default NetOp will use the most suitable devices available, in case a PC has more than one sound device installed you may choose one from the advanced menu as shown in the following figure:

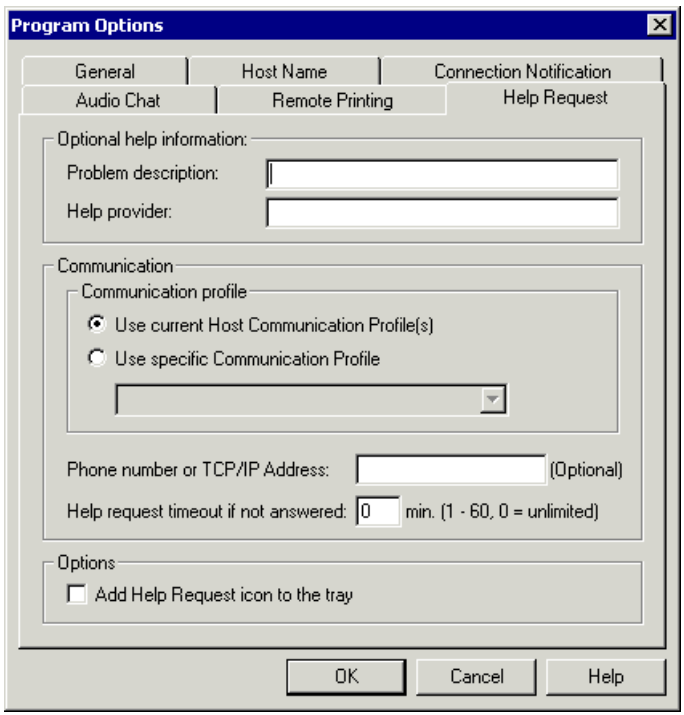



## 5.4.5 Remote Printing

Remote printing is described in Chapter 4 “The NetOp Guest”, Section 4.4.8

## 5.4.6 Help Request

The following dialog box shows the *Help Request* section:




These options are applied to use when a user requests help from a registered NetOp Help Provider.

### Problem Description

Use this dialog to enter a particular problem description. This description will be sent to the Help Provider chosen by the Host every time the *Request Help* button is activated from the main Host dialog.

*Note: By leaving this field blank you will be prompted to enter a description of the problem you are experiencing every time the Request Help button is activated.*

### Help Provider

Use this field to enter a name of a NetOp Help Provider. NetOp will attempt to reach the particular Help Provider every time the Request Help Button is activated.

*Note: By leaving this particular field blank the user will be presented with a list of available Help Providers, when the Request Help Button is activated.*

### Communication Profile

By using this option it is possible to define a specific communication profile that will be used for Help Requests exclusively. For example if a Host waits for call using the IPX communications profile, the particular Host may reach a NetOp Help Provider by using TCP/IP instead.

In the communication profile section of the Help Request tab you can choose to either *Use current Host communication Profile(s)* or *Use a specific Communication Profile* from the drop down list. When a user activates the Help Request button the specific "Help Request Communication Profile" will be activated.

### Phone Number or IP address

Use this field to specify a phone number or an IP address when using either a dial-up communication profile or an outgoing Gateway communication profile.

### Help request Timeout

By entering a number from 0 to 60 you may specify the length of time (in minutes) in which a Help Request should remain active after it has been forwarded to the Help Provider. By entering '0' the Help Request will remain active until serviced by the Help Provider or cancelled by the Host user.

### Add Help Request icon to the tray

Selecting this option will add a Help Request icon to the Host PC's system tray. By double clicking this icon the Host will search for available Help Providers (Performing the same function as the Request Help button does in the main Host dialog).

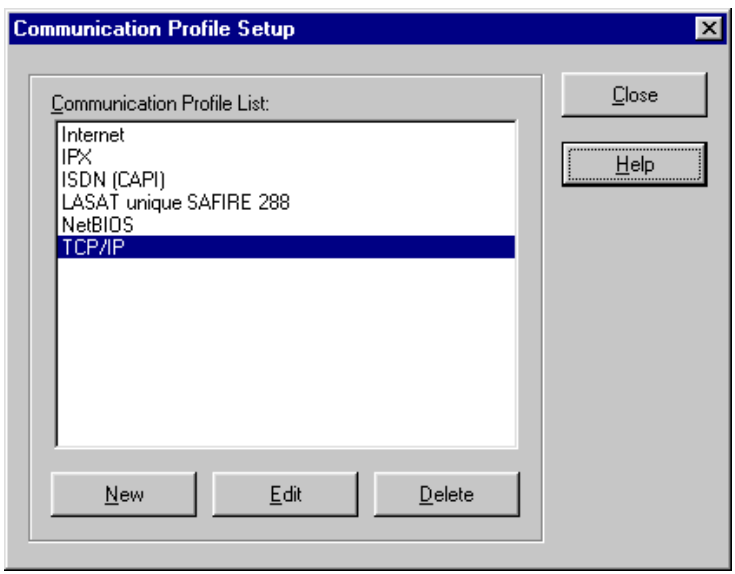
*Note: Hosts running in "Stealth Mode" will be able to request help using the system tray icon, while the main Host dialog remains completely hidden.*

## 5.5 Communication Profiles

A communication profile is simply a collection of information about a particular communication device (a protocol or interface NetOp can use for communication (e.g. NetBIOS or serial)).

By collecting all needed information about a device in a communication profile NetOp makes it easy to quickly switch between communication setups.

NetOp comes with a number of predefined communication profiles, one for each supported device expect TCP/IP (TCP). To maintain the communication profile database select *Communication profiles* from the *Configuration* menu. This activates the following dialog box:



The list shows you the existing profiles in the database which are always sorted alphabetically.

### Searching

You can search for a record by pressing a key. For example pressing A will move you to the first profile starting with the letter 'A' (or 'a').

### Inserting

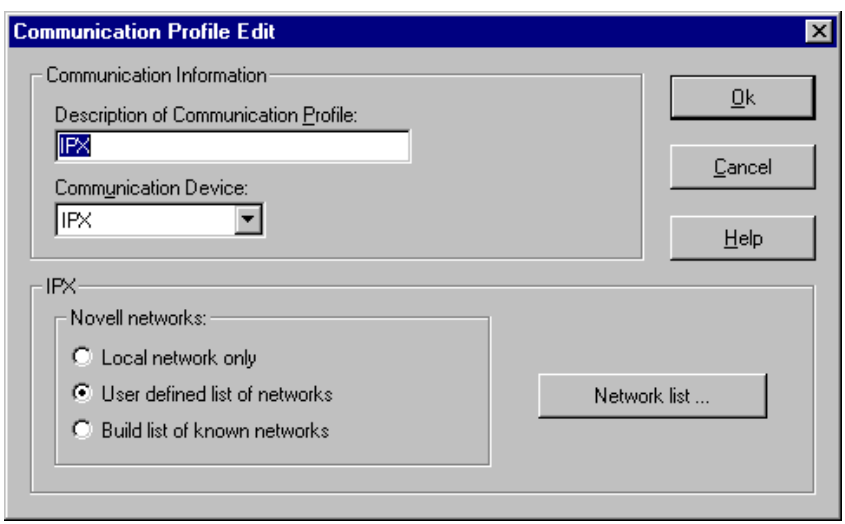
If you activate the New button (or press ALT+N), you will add a new record to the database, its contents will be similar to the selected profile's (except for the name which will be blank).

### Deleting

You delete profiles by clicking the *Delete* button (or by pressing ALT+D on your keyboard).

### Editing

If you activate the *Edit* button (or press ALT+E) you will edit the selected profile. A new dialog box will appear:



The following is a general description of the communication profile ‘Edit’ dialog box. For more info regarding communication profiles please refer to chapter 11.

### Description of Communication Profile

This is the name with which you wish to identify the current communication profile.

### Communication Device

Choose the communication device to use for the profile. NetOp supports a wide range of devices. Please refer to Chapter 11 ‘Communication Profiles’.

### Device specific

In the lower part of the dialog box you will find parameters which vary with the communication device you have chosen. For a description of the various device specific settings please refer to Chapter 11 ‘Communication Profiles’.

## 5.6 Guest Access Security

The NetOp Host includes a number of security features. Use these to prevent unauthorized access to the Host PC and to limit the number of actions a Guest PC can perform.

The security settings can be accessed by selecting *Guest Access Security* from the *Configuration* menu. A tabbed dialog then appears. On the first tab page, *Guest Access Privileges* are displayed. The *Guest Access Privileges* define what type of authentication is going to be used (the Guest Access Method) and what the Guest is allowed to do on the Host (the privileges).

Use this Guest Access Method drop down list to choose between the following authentication methods:

- Grant all Guests default access privileges
- Grant each guest individual access priviledges using NetOp authentication
- Grant each guest individual access priviledges using Windows Security Management
- Use NetOp Access Server on Guest side
- Use NetOp Access Server on Host side

The different authentication methods will be described in the following paragraphs.

In the *Guest Password Policy* tab page, the action to take when invalid logins are detected is defined.

In the *MAC/IP Address List Setup* it is possible to limit access to the Host to Guests with MAC or IP addresses in the list. The *Guest Password Policy* and *MAC/IP Address List Setup* are also described in the following paragraphs.

## 5.7 Grant All Guests Default Access Privileges

The following figure shows the *Guest Access Privileges* dialog box when the access method is set to *Grant all Guests Default Access Privileges*:

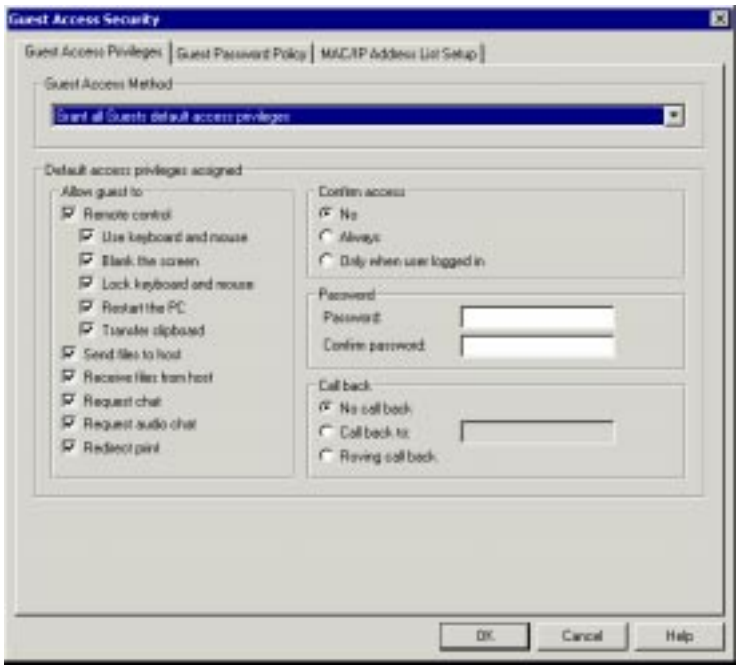
This is the simplest way to configure security. When using this method, you only specify one set of security settings, which is used no matter which Guest connects to this Host.

A Guest user will not have to identify himself with a name when connecting to the Host but might have to enter a password, if one is defined by the Host.

The settings available in this security mode are described in the following paragraphs.

## 5.7.1 Default Access Privileges Assigned

This section of the security dialog contains the settings, which define what a Guest is allowed to do on the Host. The options available are:




### Remote Control

Specifies whether the Guest is allowed to remote control the Host. If this option is disabled the Use Keyboard and Mouse, Blank the screen, Lock Keyboard and Mouse, and Restart the PC options will automatically be disabled.

### Use keyboard and mouse

If this option is disabled the Guest will not be able to remote control the Host's keyboard and mouse, but only view the screen. It is sometimes referred to as view only mode. It also controls whether the Guest is allowed to enter marker mode or not. For this option to be enabled, you must also enable the *Remote Control* option.

### Blank the screen

Specifies whether the Guest is allowed to blank the Host's screen. For this option to be enabled you must also enable 'Remote Control'.

### Lock keyboard and mouse

Specifies whether the Guest is allowed to lock the Host's keyboard and mouse. For this option to be enabled you must also enable 'Remote Control'.

### Restart the PC

Specifies whether the Guest is allowed to boot the Host PC. For this option to be enabled you must also enable 'Remote Control'.

### Transfer clipboard

Specifies whether the Guest is allowed to transfer the contents of the clipboard back and forth.

### Send files to Host

Specifies whether the Guest is allowed to transfer files from the Guest to the Host.

### Receive files from Host

Specifies whether the Guest is allowed to transfer files from the Host to the Guest.

### Request chat

Specifies whether the Guest is allowed to start a text chat.

### Request audio chat

Specifies whether the Guest is allowed to start an audio chat.

### Redirect print

Specifies whether the Guest is allowed to redirect print jobs

### 5.7.2 Confirm Access

If this option is enabled, the Host will be presented with a dialog box every time a Guest attempts to make a connection. From this dialog the Host user can accept or deny the remote control attempt.

Enabling confirm access ensures that the host is not accessed while unattended. There are two modes of Confirm access that can be configured:

Always use confirm access

Only use Confirm access when a user is logged in.

### 5.7.3 Password

The Host can be protected by a password which a Guest must enter correctly in order to control the Host. A password is defined if the password field is not blank. Remember to confirm the password in the confirm password field.

### 5.7.4 Callback

This setting is only used if the Host is called via a dial-up connection.

Set the Callback level in the *Callback* section of the security dialog.

If Callback is enabled, the Host will answer incoming calls from a Guest and then hangup and call the Guest back.

The Callback facility serves two purposes:

1. Security: By specifying a Callback number it can be ensured that the Host is only controlled from specific telephone numbers.

2. Phone charges: Callback can be used to reverse phone charges from Guest to Host.

There are three different settings for Callback:

1. No *Callback*: No Callback will be performed.

2. *Callback to*: A Callback is attempted to the specified number.

3. *Roving Callback*: The Guest is prompted for the number to Callback to.

For modem and ISDN communication profiles, the amount of callback delay can be specified in the communication profile configuration. Here you can enter the number of seconds to wait before the Host initiates the Callback session. A count down timer will appear in the Host's title bar when Callback begins.

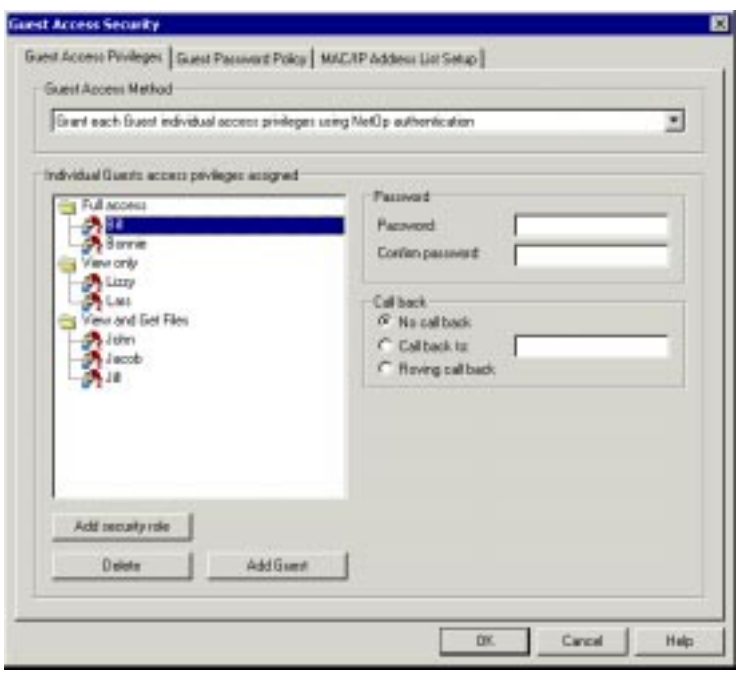
## 5.8 Grant Each Guest Individual Access Privileges Using NetOp Authentication

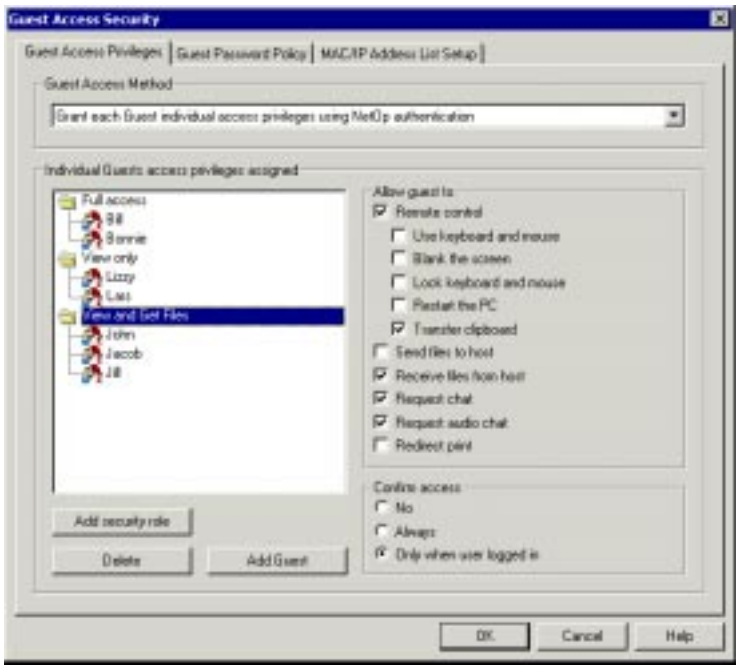
This is a more advanced way of configuring security on the Host. Using individual Guest access privileges, you specify separate settings for every Guest. For instance you can allow some Guests to remote control keyboard and mouse and limit other Guests to only view your screen. In order to do that a Guest user has to identify himself with a name and a password (if any) when connecting to the Host.

Select *Grant each Guest individual Access Privileges using NetOp authentication* in the *Guest Access Method* drop down list to use this method of authentication. If this option is selected you will see a tree structure in the *Individual Guest access privileges* section representing a directory listing of guests who can call this host.

The folder icons represent security roles. It specifies access privileges for a group of Guests, which belong to the same security role folder. Guest are represented as Guest icons contained in the folders

The right pane of the dialog will change depending on whether a Guest is selected or a security role is selected. The figure below shows the right pane when a guest is selected. The next figure shows the right pane when a security role is selected.






The Host comes with two predefined security roles, but security roles can be added and deleted as you wish. In this example we have added a new role, where we can put people who may not only view the screen, but also pick up files from the Host.

Select the *Add security role* to add a new security role. Select the *Add Guest* button to add a Guest definition to the active security role folder. Changes to a security role or to a Guest are made by editing the right side pane of the dialog. To rename a Security role or a Guest right click in the list box and select rename in the resulting menu. You can move Guest elements in the hierarchy by using drag and drop with the mouse. If you doubleclick a security role icon,  you will expand or collapse the role. If you delete a security role folder, all Guests belonging to this folder are deleted as well.

### 5.8.1 Settings for Security Roles

A security role defines a set of access privileges such as:

- Allow guests belonging to this role to remote control this PC.
- Always to present a confirm access message when the Guest connects

The various security role access privileges are described in Section 5.7.1 and 5.7.2

### 5.8.2 Settings for Guests

Each Guest icon represents a Guest with a name, a password (if any) and callback information. These settings are individual to the Guests. For more information regarding the settings offered please refer to sections 5.7.3 and 5.7.4.

## 5.9 Grant Each Guest Individual Access Privileges Using Windows Security Management

This is a security access method similar to *Individual Access Privileges using NetOp Authentication*. But this method is integrated with the Windows security management and leaves most of the administration of guests and passwords to Windows.

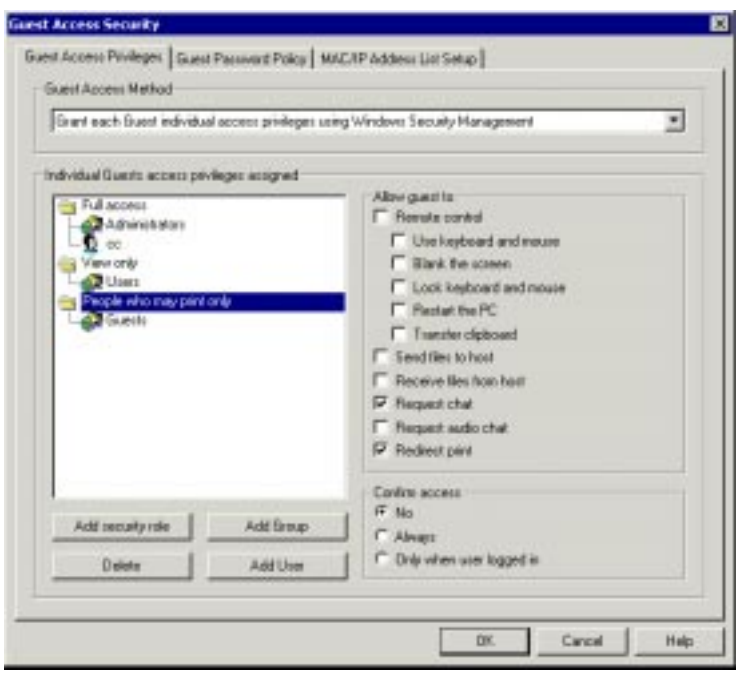
When using Windows security management, the NetOp Guests are identified by their Windows user accounts in a Windows NT/2000 domain or local accounts on the Host computer. Only Windows NT/2000 Hosts can use locally defined accounts.

In order to connect to a Host, the Guest user has to enter his Windows login name (the user name) and the corresponding password. When using Windows security management with NetOp, Guests connecting to a Host are referred to as users, meaning users in the Windows security management terminology. Windows can arrange users into groups of users. NetOp handles users and groups in the same way.

Select *Grant each Guest Individual Access Privileges using Windows Security Management* in the *Guest Access Method* drop down list to use this method. If this option is selected, you will see a tree structure in the *Individual Guest access privileges* section representing a directory listing of users and groups who can call this host.

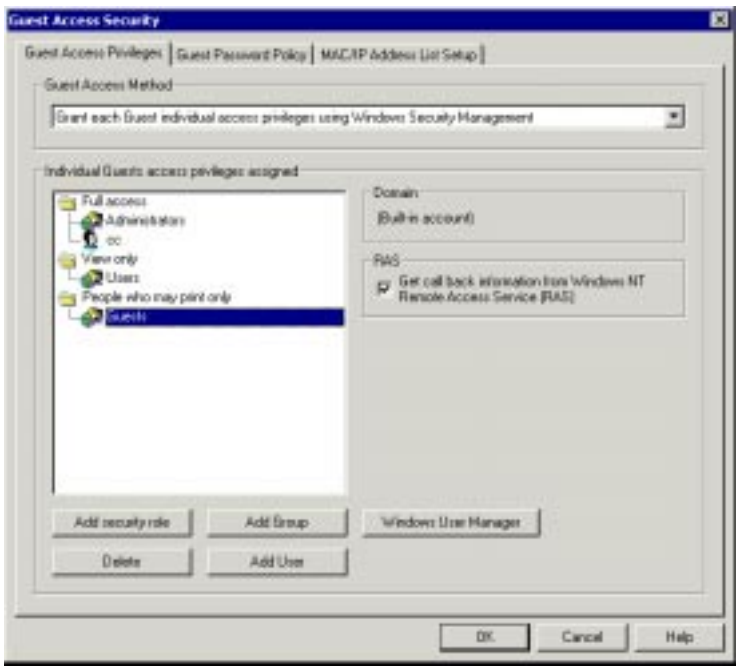
The folder icons represent security roles, specifying access settings for a number of users or a number of groups belonging to the security role folder. Users are represented with the left icon below, and groups with the right icon

The right pane of the dialog will change depending on whether a user/group is selected or a security role is selected. The first figure below shows the right pane when a security role is selected.



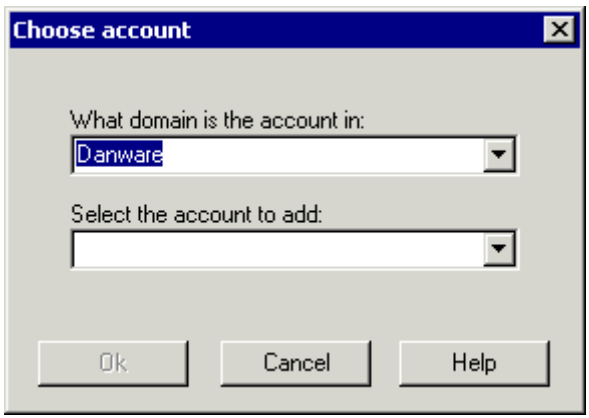
## 5.9 Grant Each Guest Individual Access Privileges, Windows authentication

The next figure below shows the right pane when a user or a group is selected. The Host comes with two predefined security roles, but security roles can be added and deleted as you wish. Deleting a Security role folder will also delete all user and group references belonging to this folder, from the listing. Deleting user or group references from the list does not delete the accounts from Windows itself.




Select the *Add security role* to add a new Security role. Select the *Add User* button to add a user reference to the active security role folder and activate the *Add Group* button to add a Group reference to the active security role folder.

When selecting the *Add User* button or the *Add Group* button the following dialog appears:




First, select the domain the account (user or group) is in. On Windows NT and Windows 2000, a list of available domains is presented. On Windows 95 and 98, a domain name must be entered manually. When the domain name is chosen, a list of available accounts will appear in the second combo box. Depending on whether a user or a group is being added, the list will contain users or groups. *S*elect the account that should be added in the lower combo box, and click *Ok*.

Changes to a security role, a user or a group are made by editing the right side pane of the dialog. To rename a security role, right click in the list box and select rename in the resulting menu.

You can move user and group elements in the hierarchy by using drag and drop with the mouse. By double clicking on a security role icon, you will expand and collapse it (Show/hide Guests).

If you have administrator privileges on Windows NT or Windows 2000, click the *Windows User Manager* button to add or delete users or groups.

## 5.9.1 Settings for Security Roles

A security role defines a set of access privileges such as:

Allow guests belonging to this role to remote control this PC.

Always to present a Confirm access message to the Host user

The various Security role access privileges are described in Section 5.7.1 and 5.7.2

A user can be a member of several security roles either directly (via user name) or implicitly through the membership of a group. This means, that a user can belong both to a security role where Remote Control is enabled and to another security role where Remote Control is disabled at the same time. The following describes how the different settings are combined.

All settings in the *Allow guest to* group are or'ed together. Hence, if the user belongs to both a Security role where Remote Control is enabled and to another security role where Remote Control is disabled, the user is allowed to remote control the Host. On the other hand the Confirm access settings are and'ed together. Consequently, if the user belongs to a security role where Confirm access is enabled and another security role where Confirm access is disabled, the user is allowed to connect to the Host without Confirm access.

## 5.9.2 Settings for Users and Groups

It is not needed to define passwords in this authentication mode, because NetOp will use the password validation available in the Windows security management.

Callback settings can be applied to a user or group. Because a user can appear several times in the list (either directly or indirectly), special rules apply to how callback information is extracted. The callback information is taken from the first occurrence of the user. If the user is not found, because the access to the Host is available through the membership of a group, the callback information is taken from the first occurrence of a group, which the user is a member of.

If access to the Host is controlled through membership of groups, and individual callback information is needed, add a security role at the top of the list without any privileges, and enable Confirm Access. Add users to this security role, and specify the necessary callback information.

On Windows NT 4 and Windows 2000, NetOp can collect the callback information from Windows Remote Access Services (RAS). If *Get callback information from Windows NT Remote Access Services (RAS)* is checked, NetOp will collect callback information from RAS, and the callback section in the dialog will be hidden. Please note that callback information can be specified in RAS without granting RAS access for the user. The RAS settings are also referred to as *Dialin* information in Windows.

### 5.9.3 Tips for Central Administration of NetOp Access

The Windows groups feature gives you the possibility to deal with groups of users, rather than having to deal with the privileges for each user. If for examle a new employee starts in the sales department, you only need to add him or her to the *Sales* group. The new employee will automatically be assigned access to the same Host PCs as the rest of the employees in the sales department, but with his/her own password. This works fine, as long as all members of a certain Windows user group are supposed to have the same NetOp access privileges.

If the user access privileges to Host PCs doesn't fit into your current pattern of groups, you can create a number of new Windows groups (as many as needed) on the Windows server specifically used to administer the NetOp security. The groups could for example be called:

NetOp Host Administrator

NetOp Host Supporter

NetOp Host Backup

NetOp Host Guest

On the Host PCs, you should create a security role for each group, and name them after the Windows Groups (but the name really doesn't matter). For each group assign the access privileges that should be used for users belonging to this group. For example, the *NetOp Host Administrator* should be allowed to do anything while *NetOp Host Backup* users only should be allowed to make file transfer.

If a new supporter joins, he/she is just added to the *NetOp Host Supporter* group. If a supporter needs to have administrator privileges rather than support privileges, he/she is just moved from the *NetOp Host Supporter* group to the *NetOp Host Administrator* group.

Instead of using an organizational method for assigning privileges, you could also create Windows groups more specifically reflecting the set of access privileges in NetOp like for example:

NetOp Host View Only

NetOp Host Keyboard and Mouse Control

NetOp Host File Transfer

If a user is a member of the *NetOp Host ViewOnly* group, he/she will only be able to view the Host screen. If the user should be able to control the keyboard and the mouse as well, he/she should also be a member of the *NetOp Host Keyboard and Mouse Control* group.

## 5.9.4 Tips for Deploying Identically Configured Hosts

All settings in the *Individual Guest access privileges assigned* section are stored in the file SECUR_NT.NDB in the NetOp folder.

To configure multiple Hosts to use the same settings for security roles and memberships use the following four steps:

1. Make sure that all Hosts involved are the same version and build number of NetOp. The operating systems do not need to be identical.

2. On a prototype Host configure the desired Security roles and memberships, then click *OK*.

3. Copy the resulting secur_nt.ndb to the other Hosts.

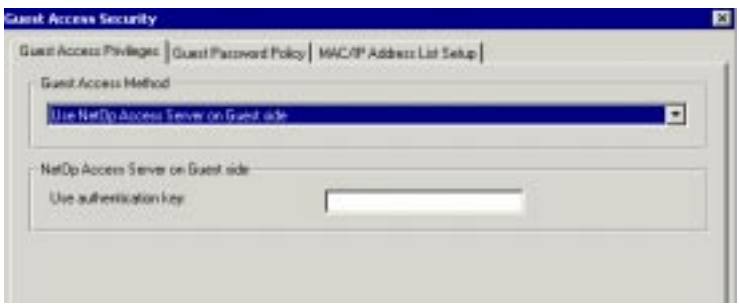
4. Remember to configure the Hosts to use Windows security management and other required settings.

Steps 1, 3 and 4 are most easily accomplished using the NetOp Deployment Utility, see Section 12.2.

## 5.10 Use NetOp Access Server on Guest Side

The NetOp product family includes a module for central security management of Guest access to Hosts – the NetOp Access Server. The NetOp Access Server is a special Host module that can be used to manage Host security and Guest privileges. For a comprehensive description of the NetOp Access Server please refer to Chapter 9.

Select *Use NetOp Access Server on Guest side* in the *Guest Access Method* drop down list to use this method of authentication. Select this Guest access method if you want the Guest to be authenticated by an Access Server before trying to take control of this Host.




The Guest will have to locate an Access Server on its own network, be authenticated and retrieve the access privileges it has when controlling this Host.

The option *Use authentication key* string is used to assure the validity of the Access Server and that the Guest is authenticated by an Access Server that the Host trusts.

## 5.11 Use NetOp Access Server on Host Side

Select *Use NetOp Access Server on Host side* in the *Guest Access Method* drop down list to use this method of authentication. Select this access method if you want the Host to authenticate the Guest on an Access Server when the Guest tries to take control of this Host.

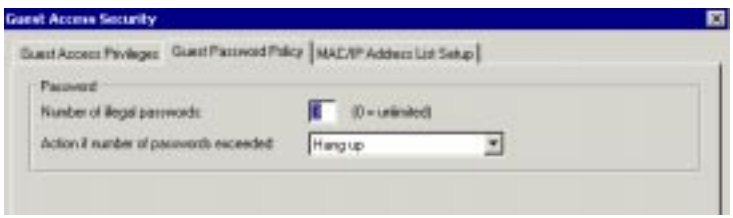
With this option, the Host will have to locate the Access Server, on its own network rather than on the Guest's network. The Host will authenticate the Guest on the Access Server and retrieve the access privileges the Guest has when controlling this Host.


The option *Use authentication key* string is used to assure the validity of the Access Server. The second option *Use Access Server with MAC/IP address* is used to ensure that the Access Server is situated on a certain MAC/IP address. This option could also be used in a situation where the Host is unable to find the Access Server (e.g. if the Access Server is located on a different TCP/IP segment).

The first time the Host needs an Access Server to authenticate a Guest it will locate one with a matching authentication key. All subsequent authentication calls will go to this Access Server until it's no longer available. The Host will now try to locate a new Access Server with the same authentication key. This allows a fault tolerant configuration, but requires that the option *Use Access Server with MAC/IP address* is blank.

## 5.12 Guest Password Policy

In the previous Sections, we learned different ways that a Host can be protected by a password which a Guest must enter correctly in order to control the Host. It is possible to specify how many times the Guest is allowed to try enter a correct password, before the Host will take action to protect itself. It is also possible to specify which action it is to take.




### Number of illegal passwords

After the specified number of invalid passwords entered by a Guest, the Host will take action.

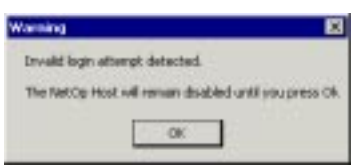
### Action if number of passwords exceeded

Should a Guest enter more than the allowed number of invalid passwords, you can specify that the Host should

Hang up the connection to the guest,

Boot the computer, which also implies a hangup

Disable itself while displaying the messagebox shown below



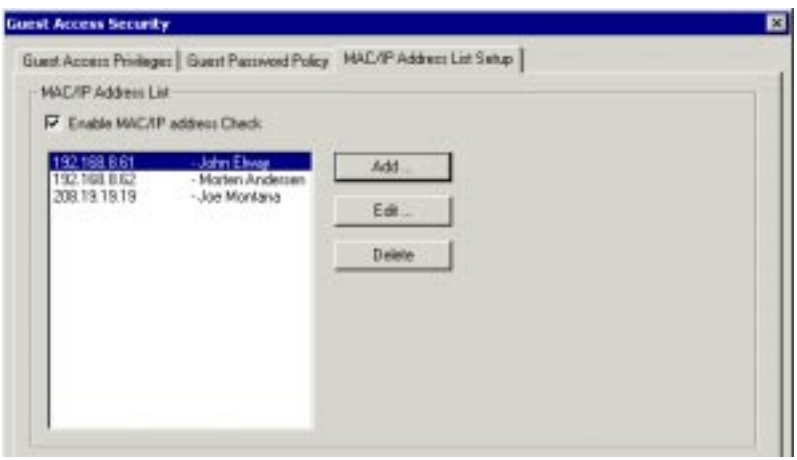
## 5.13 MAC/IP Address List

Select the *MAC/IP Address List Setup* tab in the *Guest Access Security* dialog to define, edit or delete a MAC/IP Address as shown in the following dialog:

Check the *Enable MAC/IP Address Check* check box to enable this option and add the MAC or IP you wish. When this feature is enabled, only Guests from the listed addresses will be allowed to contact the Host. To disable this option, uncheck the check box.

The Guest MAC addresses are entered using a special syntax: 0x*nnnnnnnnnnnn* , where *nnnnnnnnnnnn* is the 12-digit hexadecimal burn-in address on the network adapter being used. For example 0x08005AABD3EF.

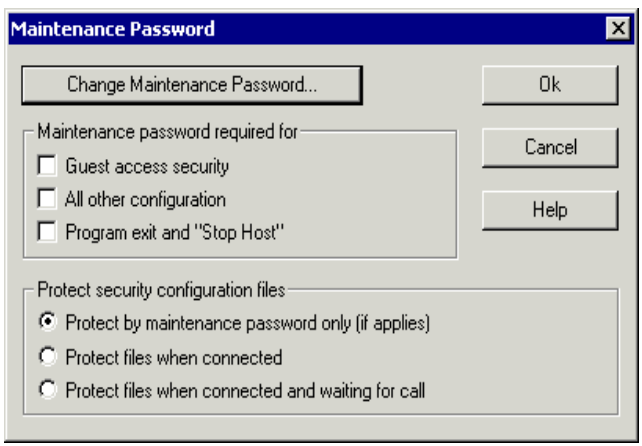
The Guest IP addresses must be entered in dot-decimal notation like ‘208.0.0.1’.



## 5.14 Maintenance Password

The Host's settings can be protected by a maintenance password. This option can be configured so a password has to be entered to access various parts of the Host's configuration setup. This ensures the Host user against unauthorized changes to configuration settings (e.g. by a Guest).

Select *Maintenance Password* from the *Configuration* menu and the following dialog will be displayed:




To define (or change) the maintenance password press the *Change Maintenance Password* button. In the resulting dialog enter your old password (empty for no previous password) in the *Old password* field, enter your new password in the *New password* field and finally re-enter your new password in the *Confirm password* field.

If you wish to assign the maintenance password to other parts of the program, simply enable the check boxes next to each option. These options are described below:

### Guest Access Security

Enable this option if you want the user to enter the maintenance password when selecting *Guest Access Security* from the *Configuration* menu.

### Gateway Access Privileges

Enable this option if you want the user to enter the maintenance password when selecting *Gateway Access Privileges* from the *Configuration* menu. This option is only available if you are using the NetOp Remote Control Gateway module.

### All other configuration

Enable this option if you want the user to enter the maintenance password to access the configuration settings on the Host (other than Guest access security) such as log setup, program options, the modem database, etc.

### Program exit and Stop Host

Enable this option if you want to keep the Host running without user intervention. If this option is enabled the user will have to enter the maintenance password to stop the Host (if it is running) and to exit the program.

### Protect Security Configuration Files

The following three options allow a user to select a particular method in which the Host configuration files should be protected. These files store security and other configuration settings. The three options offered are as follows:

### Protect by maintenance password only (if applies)

By selecting this option, Host configuration files will be protected only by the maintenance password.

### Protect files when connected

By selecting this option, all Host configuration files will be protected while a connection is established with a Guest. This will prevent users from deleting, overwriting, or otherwise tampering with the files. You may use this option in conjunction with maintenance password protection.

### Protect files when connected and waiting for call

By selecting this option, all Host configuration files will be protected while a connection is established with a Guest, and while the Host is waiting for call. This will prevent users from deleting, overwriting, or otherwise tampering with the files. You may use this option in conjunction with maintenance password protection.

## 5.15 On-line Choices

This section describes the choices which are only available on the Host during a remote control session.

### 5.15.1 Chat

The chat function brings up a window on the Host and Guest which allows the users to communicate.

To start a chat session with the Guest, choose *Chat* from the *Utilities* menu or activate the *Chat* button in the Toolbar (see the following figure):


Similar dialogs will be displayed on the Host and Guest. Everything typed on the Host and Guest will be communicated between the users and displayed in the dialog boxes.

Please note that chat has to be enabled in the Host security settings, otherwise the chat button and the chat menu item will be disabled.

### 5.15.2 Hangup

The Host can choose to disconnect the Guest at any time during a remote control session. Select the *Hangup* button in the Toolbar (see the following figure), or select *Hangup* from the Connection menu.

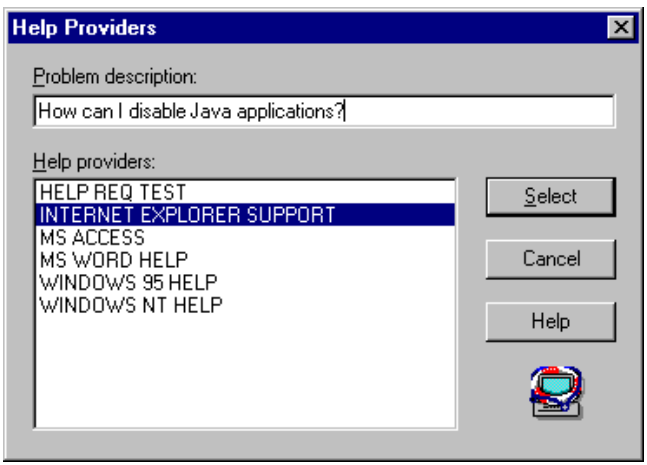
Please note that the hangup button and menu items are only available when a remote control session is active.

## 5.15.3 Call for Help

The Host user can activate the *Request Help* button in the Toolbar (see the following figure), or select *Request help* in the *Utilities* menu to initiate a *Help request* to any registered help provider (see chapter 4 for details regarding 'Help Service').

You can only request help if you have initialized communication by activating the *Wait for call* button. If more then one communication protocol is initialized, NetOp will prompt the user to select the protocol that should be used to search for a Help Provider.

When the call for help function is activated the Host browses the network for help providers. If any help providers are found, the following dialog box appears:


Enter a description and choose a help service. The help services appearing in the list are the ones registered by the Guests providing help on the network. Press *Select*, the request is now registered.

Whenever a call for help is made the request appears on the screen of the help providing Guest(s). When a Guest handles the request a remote control session is automatically started between the help providing Guest and the help requesting Host.

A Host can only have one pending help request. To cancel a pending request, select the *Cancel Help* button in the Toolbar (see the following figure), or select *Cancel help* from the *Utilities* menu.


It is also possible to have the Host direct a predefined Help Request description to a specific NetOp Help Provider (as detailed in section 5.4.3, 'Help Request').

When a Help Request is made after it has been predefined in the Host options section, the NetOp program will forward only the specified problem description to the predefined Help Provider.

## 5.15.4 Remote Printing

The NetOp Remote Print facility allows a Host to send a print job to a Guest where it will be printed locally and vice-versa. This option is available for Windows 95/98, Windows NT4 and Windows 2000.

Remote printing is switched on or off in the Host's *Guest Access Security* dialog. Defining a remote printer works the same on Host and Guest. Please refer to Sections 4.4.7 and 4.20.

## 5.16 Command Line Options

The NetOp Host can be configured directly from the command line. The complete syntax is:

NHSTW32 [/R:*name*] [/C:*communication profile*] [/W:[+,-]]

**/R:name** will cause the Host to have 'name' as Host ID

**/C:profile** will cause the Host to activate the communication profile 'profile'

**/W**: will force the Host to Wait for Call at startup, no matter what its settings are

**/W**:+ is the same as /W:, but stores the *Wait for Call* setting

**/W**:- forces the Host to NOT listen at startup, and stores the setting

Examples:

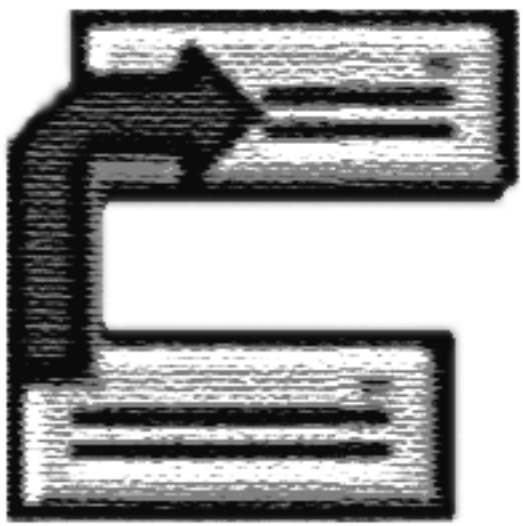
To start an active Host with the name *john* using the communication profile TCP/IP, use the following command line:

NHSTW32 /R:john /C:"TCP/IP" /W:

To start the Host with the same communication profile as the last time it was run but with the name *peter,* use the following command line:

NHSTW32 /R:peter /W:

# Chapter 6
# NetOp File Manager



## 6.1 Summary

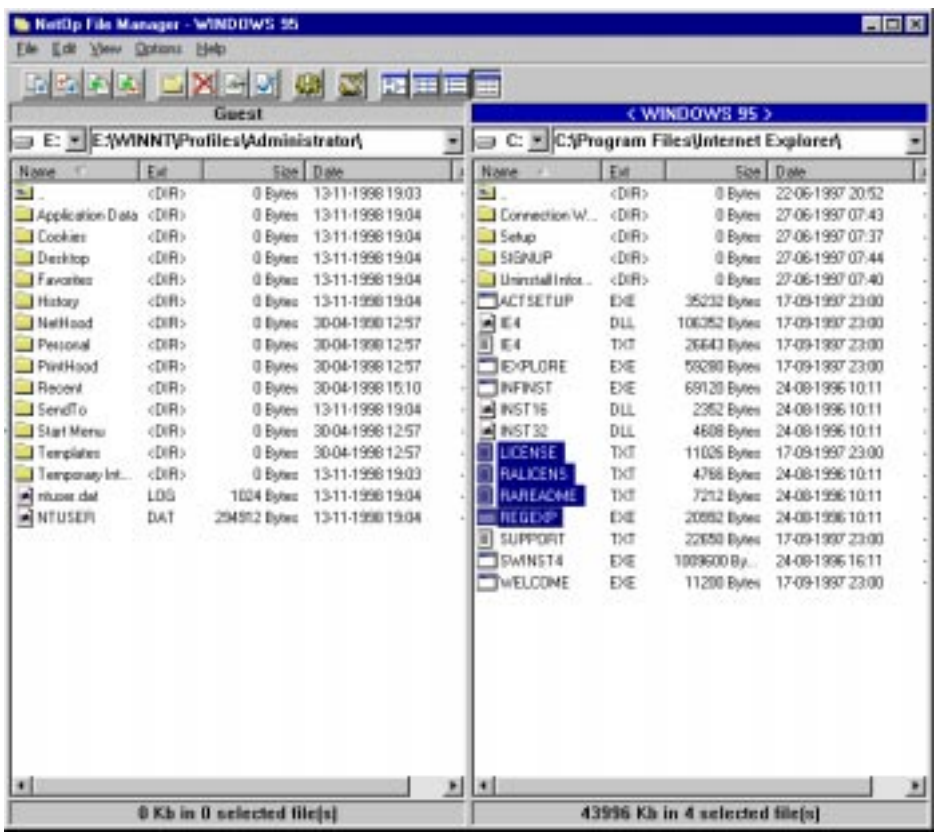
This chapter describes how to use the NetOp File Manager. This is a built-in advanced feature of the NetOp Guest module which allows you to transfer files between Guests and Hosts.

The NetOp File Manager also includes support for long file names on Windows 95/98 and Windows NT/2000.

Areas covered in the chapter include: How to start NetOp File Manager, how to transfer files between Guests and Hosts, File Manager Configuration Options.

## 6.2 Introduction

To activate the NetOp File Manager press the file transfer button in the NetOp Guest, or Remote Control Toolbar, or choose *File transfer* from the *Connection* menu. This brings up the main NetOp File Manager dialog box as shown in the following figure:



## 6.3 User Interface Overview

The main NetOp File Manager dialog is made up of the following: Two windows listing files and directories from both Guest and Host, a Menubar, a Toolbar, and a drive selection list/prompt.

### 6.3.1 The Guest and Host windows

When the NetOp File Manager program is started, a list of all files and directories from both Guest and Host will be displayed inside two fixed windows within the main File Manager user interface. The Guest window will always be placed in the left-hand side of the main File Manager interface while the Host files and directories will be listed on the right. You may use these windows to initiate file transfer functions as explained in later sections. The title of the current active window will be shown in blue.

### 6.3.2 The Menubar


This is where all NetOp File Manager commands and options are available.

### 6.3.3 The Toolbar

In the Toolbar (placed below the Menubar) shortcut buttons for the most common commands and options are available.

### The Drive Selection List/Prompt


A drive selection list and prompt is located above both Guest and Host windows. Use this function to navigate between available drives and directories.

## 6.4 The Guest and Host Window Panes

When started, NetOp File Manager presents the user with a view of all available drives, files, and directories on the Guest and Host. At any time while using File Manager either the Guest or Host Window will be active. The title of the active window (placed under the button menu) will be shown in blue (as shown in the figure below):


You may choose which window will be active by either selecting a directory or file within it or by pressing the TAB key.

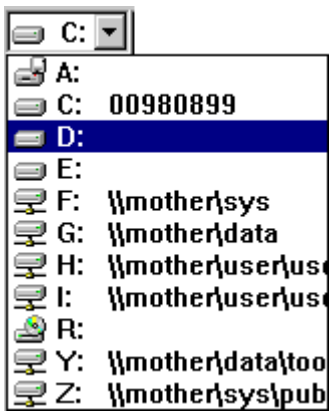
### 6.4.1 General Navigation

You may navigate between files and directories on both Guest and Host by double-clicking on folder icons (as you would using the Windows Explorer program), The current directory in which you are would be shown in the window's corresponding Drive Selection Prompt, while the current drive you are browsing will be shown in the Drive Selection List (both placed directly under the window title).

To navigate to a higher-level or parent directory press the "up arrow" folder located at the top of the window's folder listings:

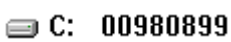
## 6.4.2 Drive Selection List

The Drive Selection List located under the window title allows you to navigate between drives on both Guests and Hosts. By clicking on the drive selection down arrow the user will be presented with a list of available drives on the particular Guests or Hosts. (As shown in the following figure):




To navigate to a particular drive just click on it's icon from the drop-down list. File manager will use the following icons to represent various types of drives:

**Standard Hard Drive:**




Will be shown by the above icon followed by the drive letter and label.

**Network Drive**


Will be shown by the above icon followed by drive letter and network path.

### Floppy Drive


Will be shown by the above icon followed by drive letter.

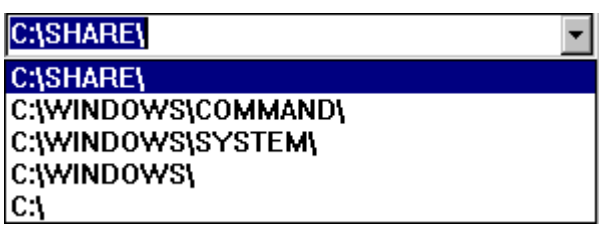
### CD- ROM Drive


Will be shown by the above icon followed by drive letter.

## 6.4.3 Path Field and History List


Use the path field (located above both Guest and Host Window Panes) to quickly navigate between directories and drives. By typing in a path in the field and pressing ENTER , the NetOp File Manager will automatically navigate to that particular directory in the corresponding fixed window pane.

To use the history list click on the down-arrow to the right of the path field. NetOp File Manager will then show the last 30 directories viewed, modified or otherwise navigated through on the corresponding Guest or Host (see the following figure):



To navigate to a particular directory from the list simply click on it. NetOp File Manager will then display the directory in the corresponding window.

### Drag and Drop Copy Functionality

NetOp File Manager contains an advanced drag and drop copying utility which enables you to easily and quickly transfer files between Guests and Hosts.

To transfer a file or directory from one module to the other simply hold the left mouse button over the item then move the object to the desired destination drive or directory. While moving the object a small '+' will be shown next to the mouse pointer showing an item being copied (See the following figure):

*Note: You can not transfer files within one module (i.e. within the Guest). You can only transfer files between modules (or between window panes).*

When placing the item over a directory (i.e. transferring a file or directory into another directory), the target directory will be highlighted.

To place the item in the specified directory simply let go of the mouse button, and the copy dialog will then appear.

*For a description of the Copy dialog box and file copy options please refer to Section 6.5.1.*

## 6.4.4 Attributes and properties

NetOp File Manager provides a column header placed at the top of the file and directory listing which allows for sorting of files and directories by name, extension ,size, date, and attribute. To sort the items by any selected category simply click on the corresponding tab.

*Note: You will not be able to view the attributes of files on Windows 3.x PCs.*

### Attributes

The attributes of files and directories are represented as follows

**r** - Read-only file

**h** - Hidden

**s** - System file

**a** - Archive

## 6.5 Menubar Commands and Options

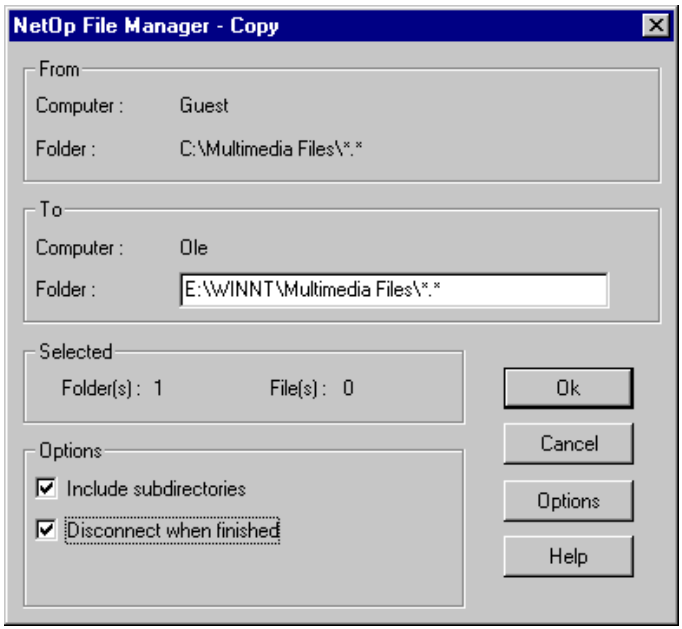
The Menubar contains the following menus: File, Edit, View, Options, Help. By clicking on one of the menu items the menu will appear.

### 6.5.1 File

The file menu contains the following options:

#### Copy File(s)

This command will allow you to copy selected files and directories from Guest to Host and vice-versa. The source directory, and target directory will be decided by the selection made in the Guest or Host fixed window panes.




### Source Directory (From)

Specifies the module name and directory from which the files are to be copied.

### Target Directory (To)

Specifies the target module name (Host or Guest name), and directory.

### Selected

Displays the amount of files and directories.

*Note: NetOp File Manager will not display the amount of files within selected directories.*

### Include Subfolders

Choose this option to copy all subfolders included within folders selected for copy.

### Disconnect when finished

By selecting this option NetOp File Manager will disconnect from the particular Host after the transfer operation is completed.

### Options

For a description of the options dialog refer to section 6.5.4.

### Progress Indicator

Fore information regarding progress indication and transfer history please refer to section 6.6 - File Transfer Monitor.

### Move Files(s)

Selecting this option will move the selected files or folders from one module to the other, while removing the selected files from the source folder. When selecting this option a dialog box identical to the copy-dialog box will appear (with the same options applying).

### Sync File(s)

Selecting this option will synchronize files between selected folders. When selecting this option a dialog box identical to the copy-dialog box will appear (with the same options applying).

### Clone File(s)

When selecting this option NetOp will clone the selected folder on the corresponding module. NetOp File Manager will delete files in the target folder that do not exist in the source folder, by doing so creating a perfect “clone” of the source folder. When selecting this option a dialog box identical to the copy-dialog box will appear (with the same options applying).

### New Folder

Choose this option to create a new folder in the active window pane. NetOp File Manager will prompt the user for the new directory name.

### Delete

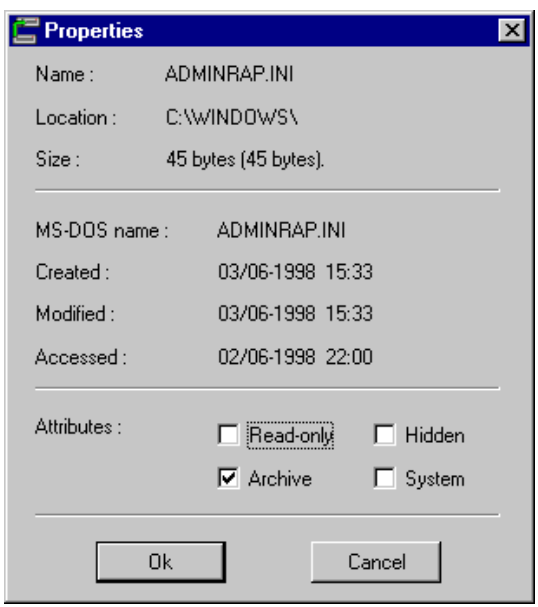
Select this option to delete selected files or folders in the corresponding window pane. File Manager will then bring up a confirmation box. Click OK to delete the selected files or folders.

### Rename

Select this option to rename a selected file or folder in the corresponding window pane. NetOp File Manager will prompt the user for the new name.

### Properties

By selecting a file and then selecting this *option*, the following dialog box will be displayed:



The above dialog box will present you with some information and options regarding the file you have selected.

The name, path, and size of the file are placed at the top of this dialog.

You can also view timestamps related to the file - when it was created, last accessed, and modified.

You will also be able to view and change key file attributes - whether the file is hidden, a system file, read-only, or an archive. For more information regarding file attributes please refer to your operating system documentation.

#### Close

This option will close the NetOp File Manager and return back to the main NetOp program.

### 6.5.2 Edit

The *Edit* menu consists of the following options:

#### Select All

This option will select (highlight) all files and Subdirectories at the current open directory in the active window pane.

#### Select by / Deselect by

Choosing these options you will be able to select and deselect files by using the standard wildcard format.

#### Invert / Clear Selection

Use these options to either clear or invert your current selection of files.

## 6.5.3 View

The view menu allows for different views and arrangements of files and folders as in Windows Explorer.

You may view files and folders using: Large icons, small icons, a list, or with file details shown.

You may also arrange icons by name, type size, date, or choose the auto arrange option.

## 6.5.4 Options

When choosing options the following dialog will appear:

*Note: You may also view this dialog from the* Copy Dialog *by pressing* Options.

## 6.5.5 Transfer Options:

### Transfer only if file exists

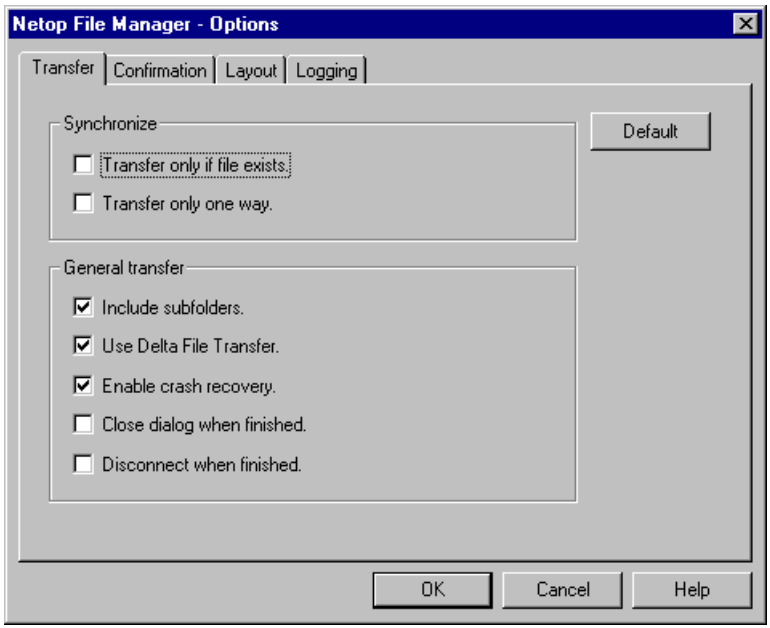
When choosing this options NetOp File Manager will only synchronize files existing on the target module.

### Transfer only one way

When synchronizing files NetOp File Manager will only transfer files from source to target.

### Include Subfolders

All subdirectories within the selected directory will be transferred.




### Enable Delta File Transfer

Delta file transfer is an advanced mechanism designed to enhance the performance of certain file transfer operations. This is done by comparing files with duplicate names and sending only the data that is dissimilar in the source file.

Delta File Transfer becomes especially useful when connecting over modems or slow network links, where file transfer operations can take a large amount of both bandwidth and time.

### Enable Crash Recovery

By selecting this option you will be able to continue a file transfer that might have been interrupted at an earlier stage.

### Close Dialog when finished

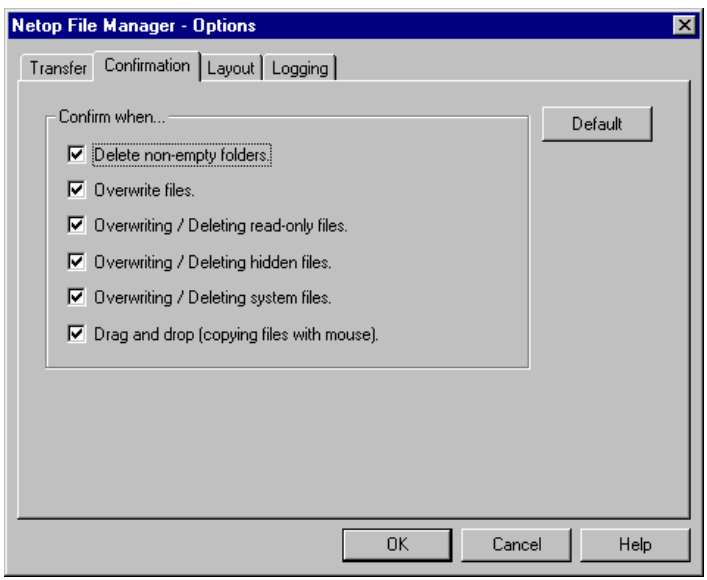
NetOp File Manager will automatically close the copy dialog when all files have been transferred.

### Disconnect when finished

Select this option to disconnect when all files have been transferred.

## 6.5.6 Confirmation

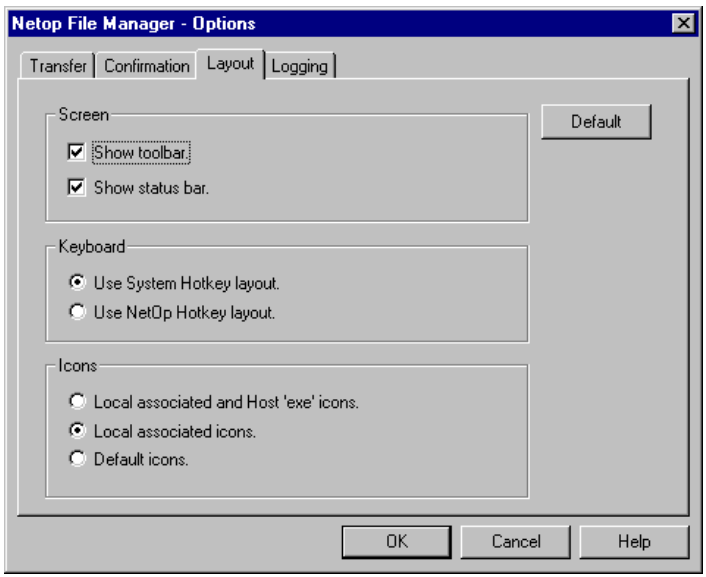
The following represents the *Confirmation* options dialog box:




Use this dialog to specify actions that should be confirmed by NetOp File Manager.

## 6.5.7 Layout

The following represents the *Layout* options dialog box.




### Show Toolbar/Status Bar

This option allows you to hide both Tool and Status Bars from the NetOp File Manager user interface.

### Use System Hotkey Layout.

By choosing this option you can perform various operations within NetOp File Manager by using your system's hotkeys (i.e. using ALT-F4 to close a dialog).

### Use NetOp Hotkey Layout

By choosing this option you will be able to use a set of predefined NetOp Hotkeys. For a list of NetOp hotkeys please refer to table 12-3 in chapter 12 appendix.

### Local associated and Host 'EXE' icons

By choosing this option all file icons will be shown using the local associations except .EXE files which will be shown using the Host association.

### Local associated icons

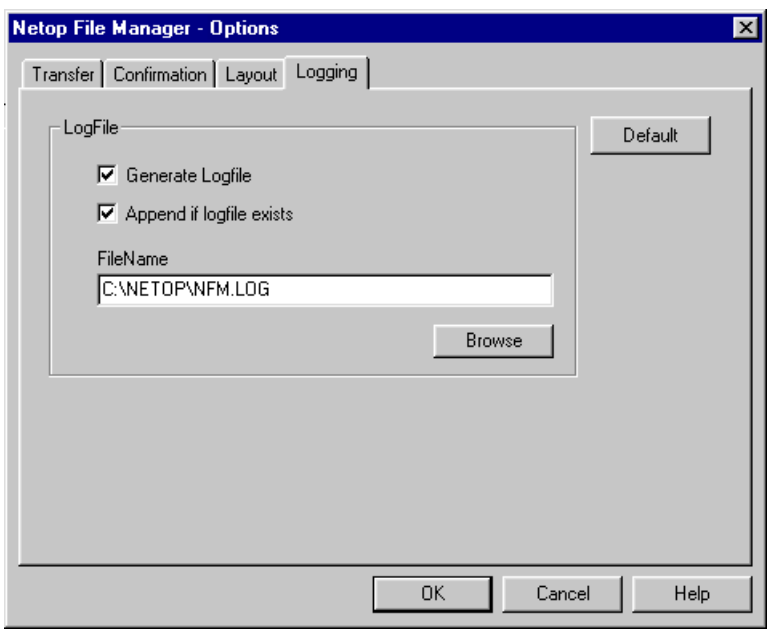
By choosing this option all file icons will be shown using the local associations.

### Default icons

By choosing this option all file icons will be shown using the default NetOp File Manager associations.

## 6.5.8 Logging

The following represents the *Logging* options dialog box:




### Generate Log File

Select this option to have the NetOp File Manager generate a log file of transfer activities. For information regarding the syntax of the Log File please refer to section 12.4.2.

### Append if Log File exists

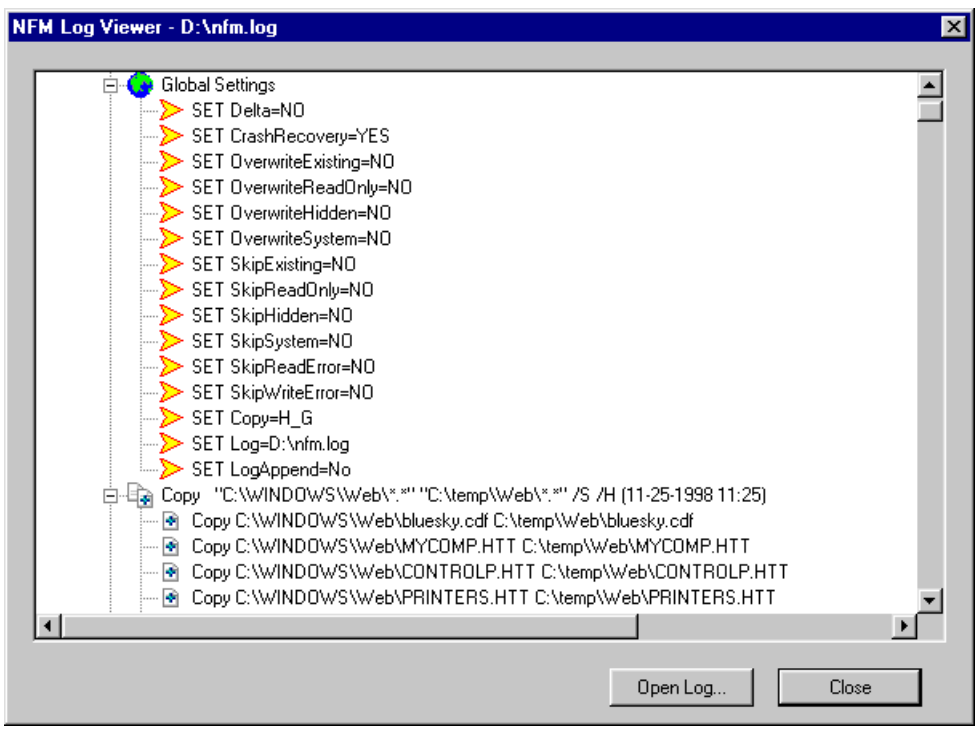
Select this option to add entries to a log file without deleting the previous entries. This will create one continuous log file containing all file transfer activities.

*Note: If this option is not selected all previous records will be deleted from the log File.*

Use the *Browse* button to specify the location and name of the log file.

## 6.5.9 View Log File

The NetOp File Manager Log Viewer is shown in the following figure:



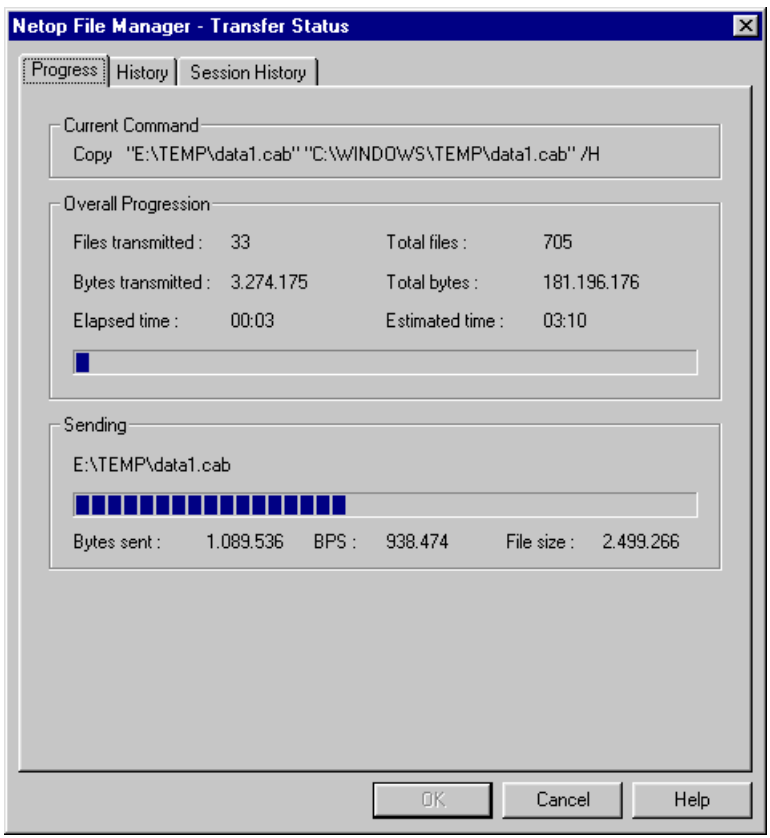
The NetOp File Manager Log Viewer allows a user to view log files generated by either the NetOp File Manager or the NetOp Scripting Utility using an easy to read tree view interface. Once you have selected to View Log File, you will be prompted to point to the particular log file you would like to view.

The NetOp File Manager Log Viewer presents the user with the global settings for a particular session, the Host name being called, and detailed file transfer operations and/or any errors that might have occurred. (For more information regarding global settings please refer to Section 7.4).

For information regarding the syntax of the Log File please refer to section 12.4.2.

## 6.6 File Transfer Monitor

During file transfer operations the following dialog will appear:



## 6.6.1 File Transfer Progress Indicator

The progress indicator supplies the user with the following information:

### Current Command

Displays the current command being executed. This could be Copy, Clone, Synchronize, Move, or in case the progress indicator is viewed from the Scripting Utility, Wait, Run, and Call, and the Scripts global settings.

### Files Transmitted

Displays the amount of files transmitted so far.

### Total Files

Displays the total number of files to be transmitted during the operation.

### Bytes Transmitted

Displays the number of bytes transmitted so far.

### Total Bytes

Displays the total number of bytes to be transmitted.

### Elapsed Time

Displays the amount of time elapsed since the beginning of the operation.

### Estimated Time

Displays the remaining time for the operation to complete.

A progress tab indicates the total transfer progress for the entire transfer operation.

### Received/Sent

This section of the dialog depending on the operation being performed will show the location of the file that is currently being sent or received.

A progress tab indicates the transfer progress for the particular file.

### Bytes Sent

Displays the number of bytes that have been sent of the file currently being transferred.

### BPS

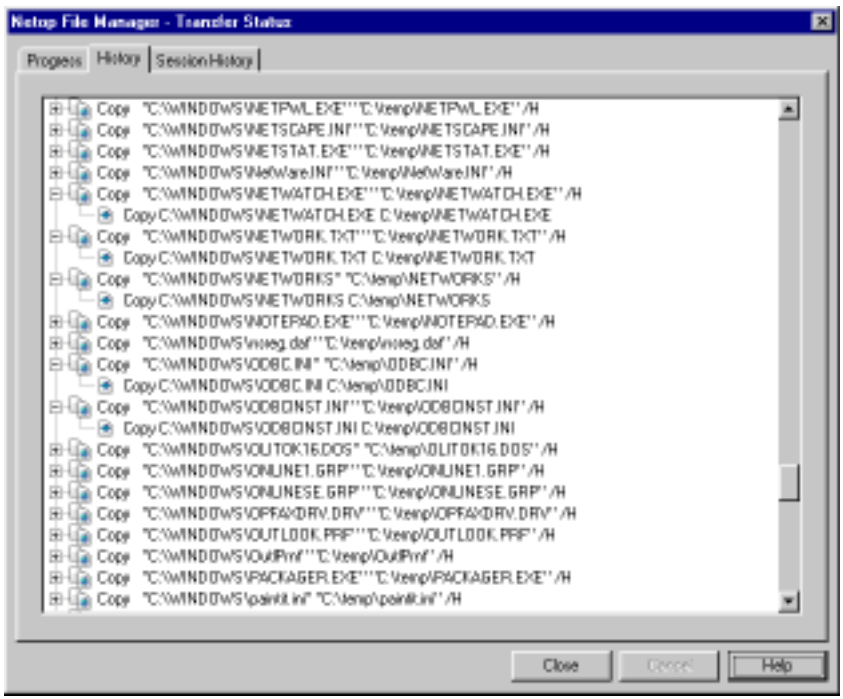
Displays the rate of transfer (Bytes Per Second).

### File Size

Displays the total size of the file currently being transferred.

## 6.6.2 History

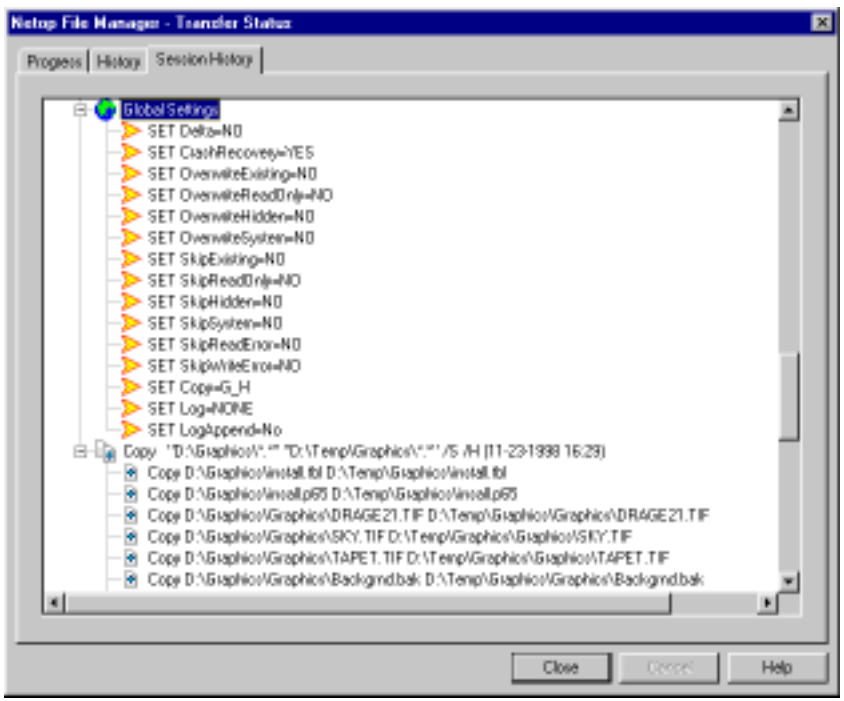
The File Transfer *History* Tab is shown in the following figure:




The History Tab provides the user with an hierarchical representation of actions taken in the latest file transfer operation. By expanding the tree it is possible to view the type of action being performed (Clone, Copy, Synchronize, etc.), the file transferred and/or directory transferred, and error messages if any. (For more information regarding transfer errors please refer to Table 12-4.4). The History list contains information regarding the latest transfer operation only, for information regarding an entire session please refer to the Session History tab or the log file.

## 6.6.3 Session History

The File Transfer *Session History* Tab is shown in the following figure:




The Session History tab provides the user with information regarding an entire session including many file transfer operations with a particular Host. The Session History tab is similar to the Scripting Utility (Please refer to chapter 7), in that it presents the user with the global settings for a particular session, the Host name being called, and detailed file transfer operations and/or any errors that might have occurred. (For more information regarding global settings please refer to Section 7.4).

Before any file transfer operation the user will be presented with the Global Settings applying to that operation only. As in the History Tab, The Session History Tab provides the user with an hierarchical representation of actions taken. By expanding the tree it is possible to view the type of action being performed (Clone, Copy, Synchronize, etc.), the file transferred and/or directory(s).

# Chapter 7
# The Scripting Utility

## 7.1 Summary

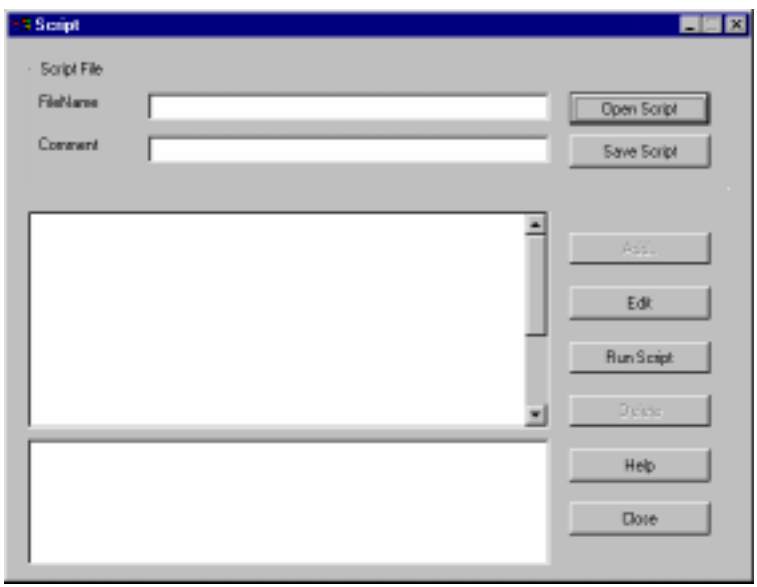
NetOp File Manager includes a scripting utility which is designed to automate file transfer operations between a Guest and Host and execute programs remotely. By creating a script you can transfer, synchronize and perform other file transfer operations using File Manager at specified times without user intervention.

The NetOp script file (or *.DWS file) contains a list of instructions that can be created by using the NetOp Scripting Utility or by editing the file manually.

## 7.2 Starting the Scripting Utility

The NetOp Scripting Utility is started from the NetOp File Manager by selecting *Script* from the *Options* menu or by clicking on the Script icon (shown in the following figure), or by utilizing the Script Tab (Refer to Section 4.12).

The following dialog will then appear:



## 7.3 Creating a new Script

To create a new script click on the *Open Script* button. In the resulting menu enter a name for the new script in the *File Name.* After clicking *Open,* a dialog will appear asking you to confirm the creation of a new script. The *file name* field will present you with the location and file name of the script you are creating.

*You may also create or open a script by simply typing it's full path and name in the file name field and pressing ENTER or leaving the Path empty and clicking on the* Open Script *Button.*

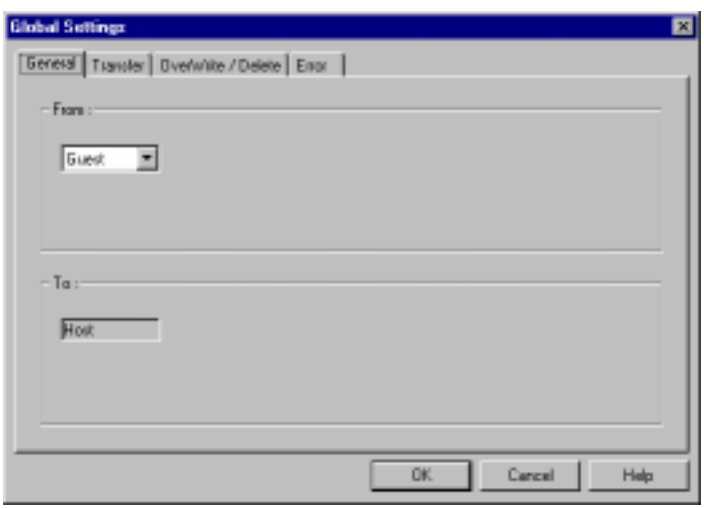
After you have selected yes a dialog box will appear prompting you to enter your script's Global Settings (See next section for details).

## 7.4 Global Settings

The Script's global settings are set from a multi-tabbed dialog containing options regarding the script being created. The global settings will apply to every action added to the script unless otherwise specified by the user.

### 7.4.1 General

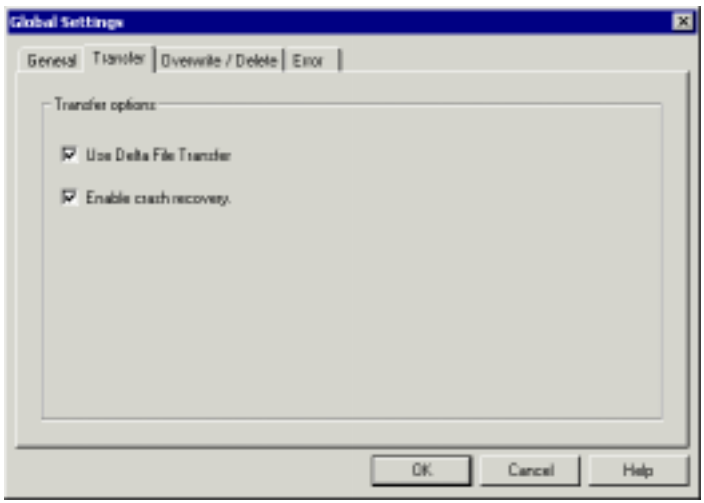
The *General* global settings tab is shown in the following figure:




Use the drop down list to select whether files should be transferred from Host to Guest or vice-versa.

## 7.4.2 Transfer

The *Transfer* Global Settings tab is shown in the following figure.




### Use Delta File Transfer

Delta file transfer is an advanced mechanism by which target files are searched for content identical to the source file content, so as to minimize the number of bytes transferred. Doing so may enhance performance, especially on slower lines.

### Enable Crash Recovery

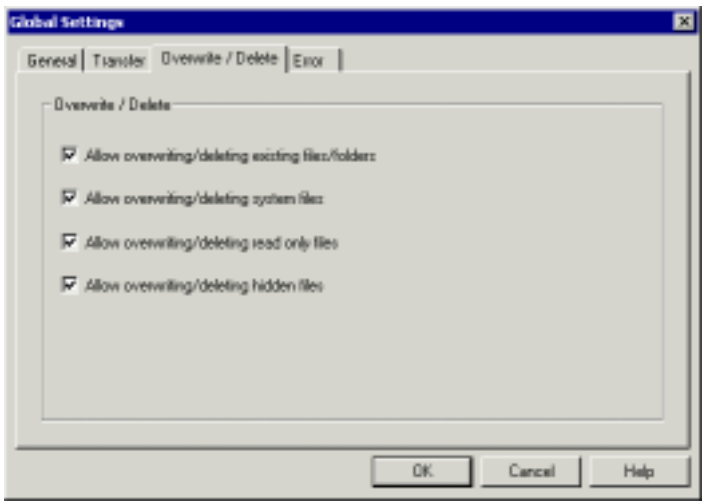
By selecting this option and switching delta file transfer on, you will be able to continue a file transfer that might have been interrupted at an earlier stage.

## 7.4.3

This Section is intensionally left blank.

## 7.4.4 Overwrite / Delete

The *Overwrite/Delete* Global Settings tab is shown in the following figure:




In this tab you may set whether or not the script is allowed to overwrite or delete different types of files. If you uncheck for example hidden files, all copy actions which try to overwrite or delete a target file marked with the hidden attribute, will be skipped. As the script runs in batch, there is prompt for confirmation. The types are

Existing files and folders

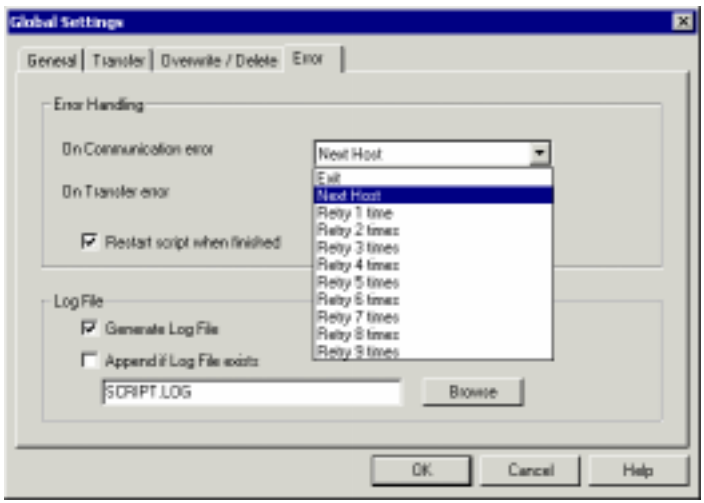
System files

Read-only files

Hidden files.

## 7.4.5 Error

The *Error* Global Settings tab is shown in the following figure:




### On communication error

Using the drop down list you may specify how communication errors should be handled by the NetOp scripting utility . This applies to errors such as a lost communications link, or any other type of lost communication between Guest and Host.

You may choose from the following options.

**Exit**

Selecting this option will end the current script when there is a transmission error.

**Next Host**

By selecting this option your script will skip all instructions until the next Call command. It will continue running the script from that point on. If no further Calls are specified, the current script will end.

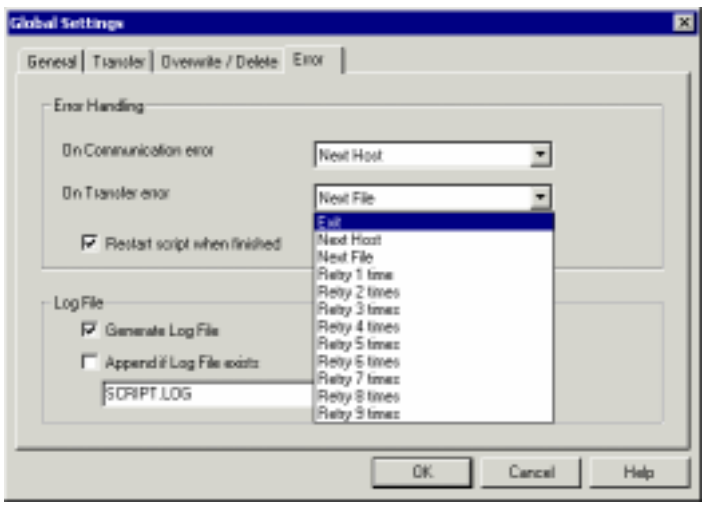
**Retry X times**

You may use this field to specify the number of times (from 1 to 9) that the NetOp scripting utility should try and reestablish communication with the particular Host. If communication can not be established the current script will end.

### On transfer error

Using the drop down list you may specify how file transfer errors should be handled by the NetOp scripting utility. This applies to files that can not be opened or can not be transferred (etc.).

You may choose from the following options.




**Exit**

Selecting this option will end the current script.

**Next Host**

By selecting this option the NetOp scripting utility will skip to the next Host specified in the script, and continue running the script from that point on. If no other Host is specified the current script will end.

**Next file**

By selecting this option the NetOp Scripting Utility will skip to the next file specified in the script or the next file in the current specified directory. If no more files are specified in the script it will then be terminated.

**Retry X times**

You may use this field to specify the number of times (from 1 to 9) that the NetOp Scripting Utility should try to transfer the specified file or directory. If the operation can not be completed within the number of tries specified, the current script will end.

### Restart script when finished

By checking this box, the current script will be run again when finished. It will keep running forever, or until you manually press the cancel button in the progress dialog. It may be a good idea to use the wait command at the end of a script, when you switch this option on.

### Generate Log File

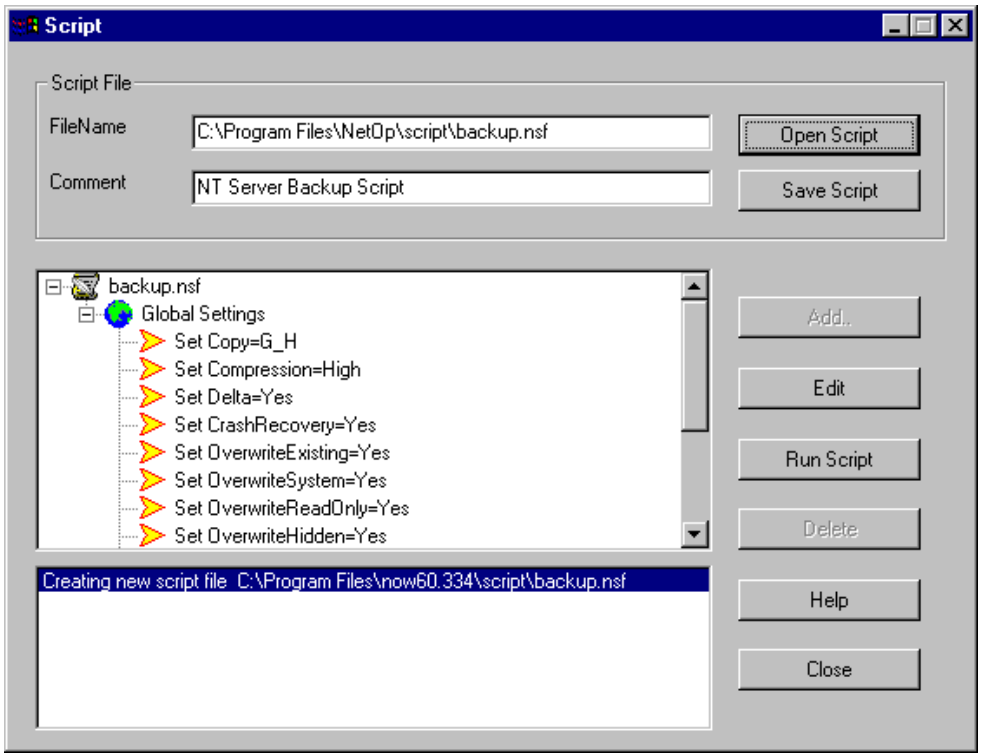
Use this function to generate a Log File for the particular script being created. Use the *Browse* button to specify the location and name of the log file. For detailed information regarding the Log file please refer to section 12.4.2.

### Append if Log File exists

Select this option to add entries to a log file without deleting the previous entries. This will create one continuous log file containing all file transfer activities.

*Note: If this option is not selected all previous records will be deleted from the log File.*

By pressing *OK* in the *Global Settings* dialog, the following dialog will appear:




In the File Name and Comments fields you will be able to view the script name, location, and comments added by the user.

The center display presents a Tree View of the script and global settings created. Click on an element or it's '+' sign to view the next level.

By expanding the Global Settings icon you will be able to view the global settings created for the particular script. (For more information regarding syntax and manual creation of NetOp Script Files please refer to section 12.4).

If the particular script was created or edited manually the text box located at the bottom of the scripting dialog box will present the user with script syntax errors (for more information regarding syntax and manual creation of NetOp Script Files please refer to Table 12.4-3 in chapter 12 ' Appendix').

Any element from the main dialog may be edited by selecting it with the mouse then clicking *Edit* , this will bring up the dialog box referring to the particular element.

## 7.5 Adding Elements

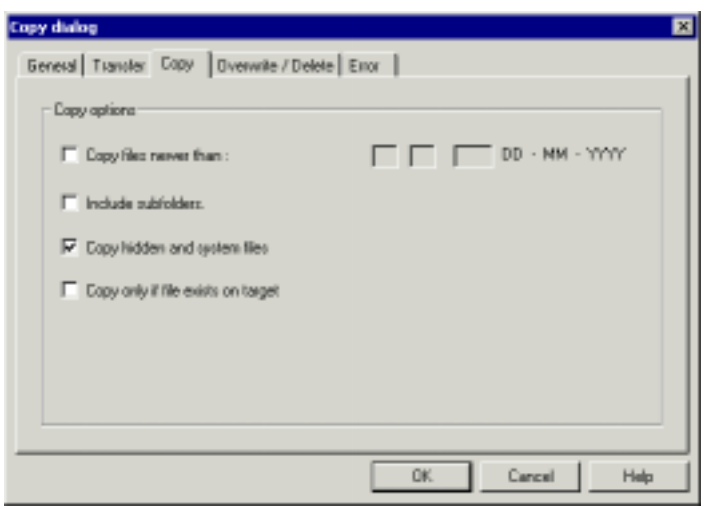
To add an element to the script, click on the Add button. A drop down list will then be displayed. To add the desired element, simply select it from the drop-down list. Refer to Section 7.6 if you don't see the commands you expect to see.

### 7.5.1 Copy

The copy command copies one or more files from Host to Guest or vice-versa. The source file(s) are left unaltered. What happens with the target file(s) is subject to how you set the options described in this Section and to your global settings, if you do not change anything here.

Use the drop down listing in the *General* tab to select whether files should be transferred from Host to Guest or vice-versa. For the local side, you can press the *Browse button* to select the location of the file or folder to be copied and it's target location, or type in a path. For selecting files and folders on the remote side, you must type in the path. Normal Windows rules apply to the file filters you type. You can use a star and question marks, and you can also use environment variables like %WINDIR%.

The *Copy* dialog contains a transfer, overwrite/delete, and error handling tab which match the ones in Gloal Settings, where the default options are specified. It also contains the Copy tab page shown below



### Copy files newer than

If you check this box, you will be able to specify a date. Files with a ”modified” date before this date will not be included in the copy process

### Include subfolders

If you check this box, files in subfolders of your selected folder will be included.

### Copy hidden and system files

If you check this box, files which are marked as hidden or as system files are included in the copy process.

### Copy only if file exists on target

If you check this box, it will be a condition for the copy process, that there is a target file with the correct name already. New files can not be created if this option is on.

## 7.5.2 Move

Moving is identical to copying, except that the source files are deleted. The *Move* dialog is identical to the *Copy* dialog.

## 7.5.3 Synchronize

This command synchronizes the selected directories and files including all subdirectories (if specified) from the source to the destination. Files are matched on their names. If a file with a given name in a given source subfolder does not exist in the target subfolder, the source file is copied to the target folder. If a file with a given name has no matching file in the source folder, it is copied here. If a file with a given name exists in both folders, the file which has the latest “modified” timestanp survives, and overwrites the file with the older timestamp. If the timestamps are identical or do not differ by more than 2 seconds, no action is taken.

Synchronize is independent of direction. That is, it gives the same result if you switch source and target folders. The *Synchronize* dialog is identical to the *Copy* dialog.

## 7.5.4 Clone

Cloning is similar to synchronizing in that the two folders end up having the same content. They are however most different with respect to which files are kept and which files are deleted. When you clone, all files in the target folder and optionally also its subfolders are deleted, and replaced by the ones from the source. The outcome of cloning is critically dependent on which is the source and which is the target.

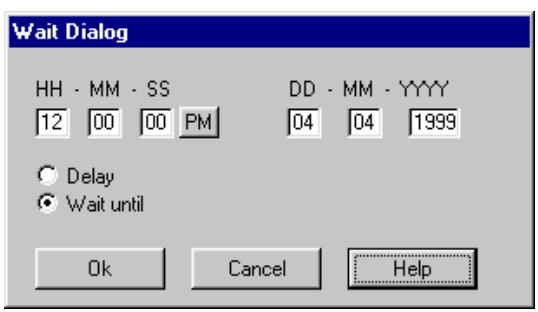
The *Clone* dialog is identical to the *Copy* dialog.

## 7.5.5 Call

When calling a Host using the NetOp Scripting Utility, a Phonebook entry must be specified which then represents the particular Host that should be called. This is done by pointing to the Phonebook entry's *.DWC file. Specify the path and name of the *.DWC file in the field provided, or press the *Browse* button to browse for *.DWC files. The NetOp Scripting Utility will then use the connection information stored in the *.DWC file to call the particular Host. The call will automatically be hung up when you make the next call or when the script ends.

## 7.5.6 Wait

The following figure presents the *Wait* dialog:




### Delay

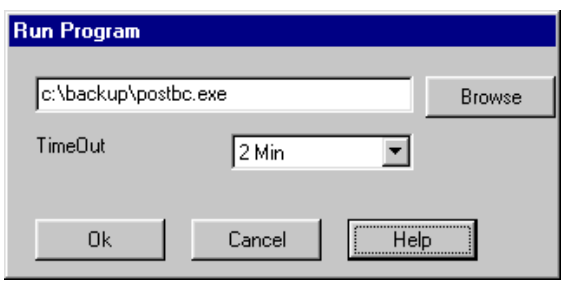
Select this option to add a particular delay time at this point in the script. No other actions contained in the particular script will be executed until the delay time specified is passed.

### Wait until

Use this option to instruct the NetOp Scripting utility to wait until a particular date and time before executing the remaining actions in the script. No other actions contained in the particular script will be executed until the specific date and time have been reached. If the time is in the past, the wait command will return an error and the script will continue.

A very useful special date is 00-00-0000 which will be interpreted as “any day”, so if you for example end your script with such a wait command and if you also check the Restart when finished checkbox, your script will restart at the same time every day. For more detailled control, you must use an external scheduler program. You can start a script from the DOS command line with NGSTW32 /S:scriptname.dws

## 7.5.7 Run Program



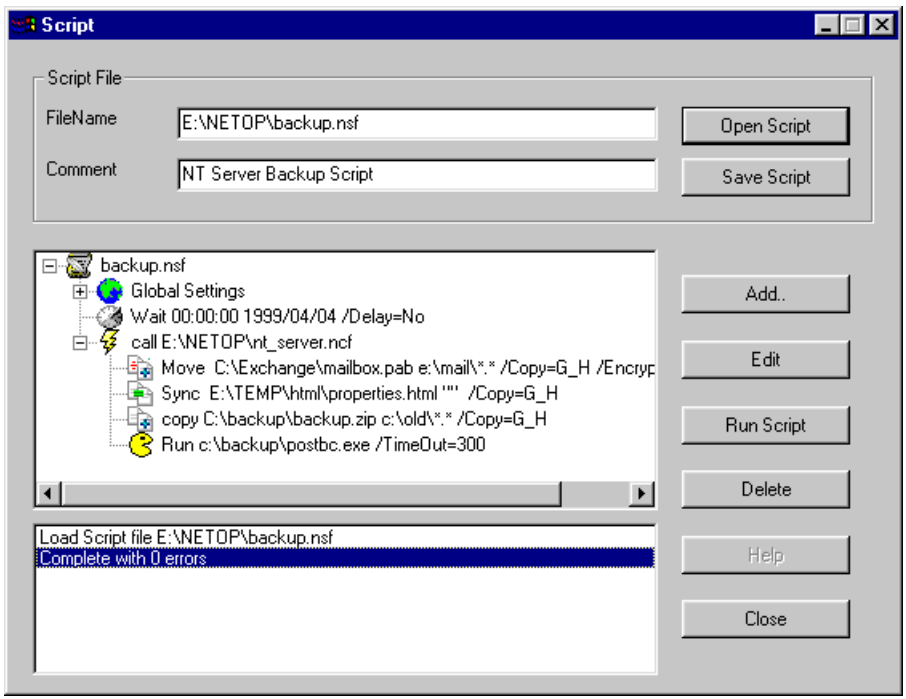

The run command starts an executable program. If you add the run command inside a call, the executable will run on the host. If you add the run command outside calls, so it appears non-indented in the editor, it will run on your local Guest machine. For more info on placing actions please refer to the section 7.6 ‘Placing an action’.

It depends on your operating system, what files are executable. For Windows 95/98/NT/2000, executables are EXE, BAT and COM files. If you want to execute an operating system command like DIR, please note that there is no DIR.EXE executable. You will have to enter the name of the OS shell executable which is CMD.EXE for NT/2000 and COMMAND.EXE for 95/98. Such a line could for example be

RUN “CMD/C DIR C:*.* > C:\TEMP\MY.LOG”

## 7.6 Placing an action

*Transfer* actions (Copy, Move, Sync, Clone) must apply to a *Call* to a particular Host. To add a transfer action, select the particular *Call* command, then click *Add.* You may also click on an action already inside that *Call*. Press *Add,* then choose a new action. It will then be placed below the action you selected.




If you have selected the top most element or the script name, you may only add a *Call*, *Wait* or *a locally executed Run* command.

Actions may be deleted by clicking the particular element, then choosing *Delete*.

*Note: If a particular Call is deleted, all actions associated with that particular call will be deleted as well.*

## 7.7 Deleting a Script

To delete a particular script select it's name from the main Scripting Utility dialog and press delete, a dialog box will appear confirming your action.

## 7.8 Running the script

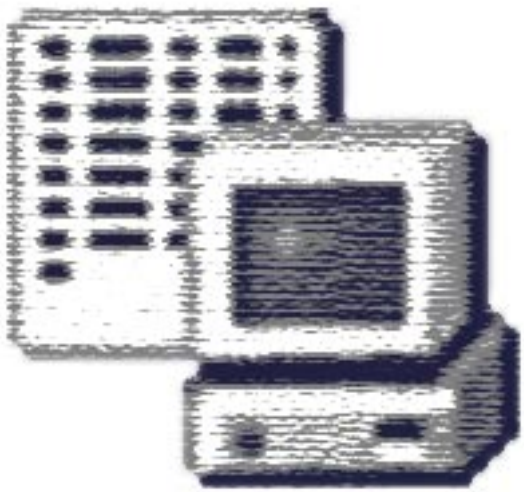
To run the script press the *Run Script* button, the current script will then be started.

## 7.9 The NetOp Script ActiveX Control

NetOp offers an advanced method of using the Scripting Utility and other file transfer operations. This method is intended mostly for programmers and application developers who wish to utilize NetOp's scripting and file transfer capabilities from their own applications.

For more regarding the ActiveX control and its usage please refer to section 12.5.

# Chapter 8
# The Log Setup



## 8.1 Summary

This chapter describes how to use the NetOp Log feature. This feature allows a Guest and/or a Host to log activity during a remote control session.

Activity can be logged locally and/or to the special NetOp Log Server program.

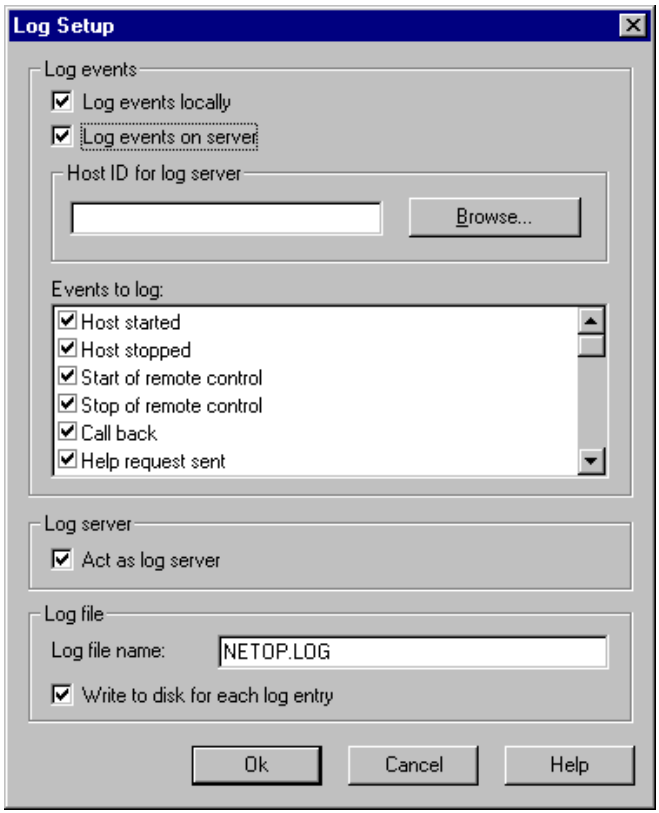
The Log Server program is a special Host module that can act as a logging mechanism for NetOp activity in a particular environment, logging activity from a number of workstations. This feature is particularly useful for monitoring purposes allowing a Network Administrator to track what remote control activity has been going on, who has controlled what PCs and when, what has been done, e.g. file transfers and re-boots.

## 8.2 Starting the Log Setup

The log setup can be started from the Guest and/or the Host machine, as well as from a Log Server and an Access Server.

To start the log feature select the option *Log setup* from the *Configuration* menu.

When you have selected the Log setup, the following dialog will appear:




## 8.2.1 Log Events

There are two options as to how you can log events from your Guest or Host machine. Logging events locally or logging events on a NetOp Log Server.

The option *Log events locally* will create a log file which will be located on your local hard drive. To select this option activate the *Log events locally* check box.

The option *Log events on a NetOp Log Server* will log to a log file located on a NetOp Log Server. To select this option activate the *Log events on a NetOp Log Server* check box.

If you select this option you must specify a name of the special NetOp Log Server Host. If you know the name of the Host, enter the name in the *Host ID for Log Server* field or use the *Browse* button to search for Hosts that are setup as Log Servers.

## 8.2.2 Log Server

The Log Server module is a special version of the NetOp Host module, which can act as a logging mechanism for NetOp activity. For this special module an extra option to *act as Log Server* is available in the *Log Setup* dialog. If this option is enabled then your PC can be used to log events from other NetOp modules.

To activate this option, simply enable the *Act as Log Server* check box in the *Log Server* section of the dialog. If you wish to stop your machine from acting as a Log Server disable the *Act as Log Server* check box.

## 8.2.3 Events to Log

After you have selected where and how to log, it is possible to select which events you wish to log.

You will notice that the default setting is for all events to be logged. This is shown by all of the check boxes being enabled.

To add or remove an event from being logged, select the event and enable or disable the appropriate check box. The changes you make will not take effect until the *OK* button is pressed.

When these events have been logged, they will appear in abbreviated form in the log file. See the following section 'Log File'.

Table 12-2.1 and Table 12-2.2 in Chapter 12 ' Appendix' show how the abbreviated form will appear when logged in the log file.

## 8.2.4 Log File

Once you have configured your log setup you can send all log activity to a file. The default name for this file is NETOP.LOG and will be saved in your NetOp directory.

If you wish to change the log file name you can do so by typing the new file name in the *Log file name* field.

NetOp has the option of immediately flushing each line to disk. This means that if this option is enabled NetOp bypasses the machine's cache memory thereby keeping the log safer from data loss, for example, if your machine suddenly crashed.

To select this option, enable the *Write to disk for each log entry* check box in the log file section of the dialog.

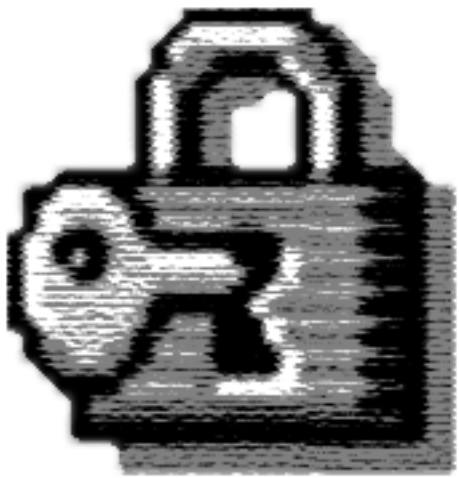
## 8.2.5 Example Log File

The following is an example of a short log file. The file comes from a Host called 'John' that is logging locally. The Guest connects and starts a remote control session with the Host, then starts a file transfer.

Each line starts with the date and time the event was logged. The digit after the Host name (john) is the sequence in which the events were logged. The zeros are error message fields and will change if any errors occur. The next field states the event logged. The first line also shows the MAC Address of the Guest. When a file transfer is initiated, the log file lists all files that were sent or received.

```
19970611,08:44,john,0,00000,00000,START REMO,0x00001700559D
19970611,08:46,john,1,00000,00000,FILERECV,C:\TRANS\NHOST.EXE
19970611,08:46,john,2,00000,00000,FILERECV,C:\TRANS\NHOST.DLL
19970611,08:46,john,3,00000,00000,FILERECV,C:\TRANS\NHOST.CFG
19970611,08:48,john,4,00000,00000,STOP REMO,0x00001700559D
19970611,08:48,john,5,00000,00000,STOP HOST,
```

# Chapter 9
# The Access Server



## 9.1 Summary

This chapter describes how to use the NetOp Remote Control Access Server program. The Access Server is a special NetOp Host module with a database that holds security information about Guest and Hosts, including Log Servers and the Access Server itself. The purpose is to centralize control of security settings and to perform authentication tasks.

The Access Server can only be used in conjunction with NetOp version 5.3 or later modules.

An Access Server configuration program is used to edit the information in the Access Server's central database.

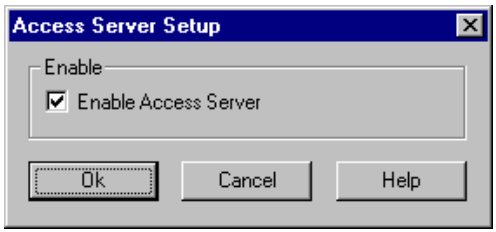
## 9.2 Starting the Access Server

To start the NetOp Access Server double click on the Access Server icon in the NetOp program folder or start the application NACCSW32.EXE located in the NetOp directory or NACCESSW.EXE if the Access Server is installed on Windows 3.x.

The very first time the NetOp Host is run the program will offer to guide you through configuration of your modem. Follow the on-screen instructions.

After this you will be presented with the NetOp Host dialog box. Configure the Access Server Host as you would a normal Host. For details, please refer to chapter 5 'The Host'.

The Access Server Host must be active for Guests to remote control Hosts that require authentication from an Access Server. This is controlled in the Access Server setup dialog. Select *Access Server Setup* from the *Configuration* menu, the following dialog will then appear.




Enable the Access Server by selecting the *Enable Access Server* check box. To stop the Access Server simply disable this check box. Once this option has been disabled existing Guests and Hosts will not be able to use the Access Server for authentication tasks.

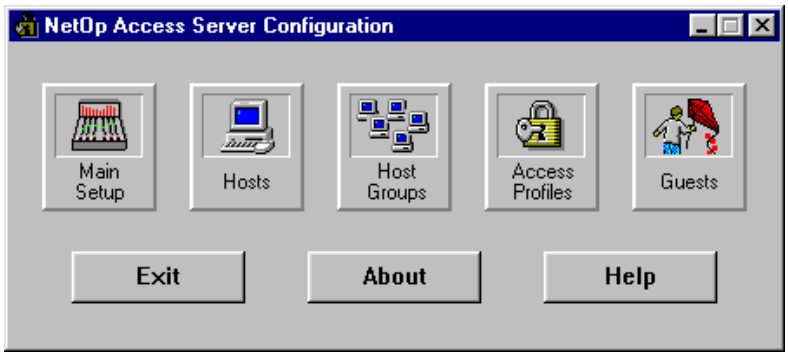
## 9.3 The Configuration Program

### 9.3.1 Starting the Program

To start the configuration program, double click on the configuration program icon in the NetOp program folder or start the NACFGW32.EXE program located in the NetOp directory (NACFGW.EXE on Windows 3.x PCs).

### 9.3.2 Main Menu

When you start the configuration program for the first time and when you logon to the configuration program at any later time, you will be met with the main menu. The following figure shows the main menu dialog:




There are five main choices:

**Main Setup:** Press this button to configure details regarding password rules and the Access Server key.

**Hosts:** Select this option to add, edit or delete Hosts in the Access Server database.

**Host Groups:** Press this button to configure Host groups. Here you can setup, edit and delete security groups, which can contain a number of different Hosts.

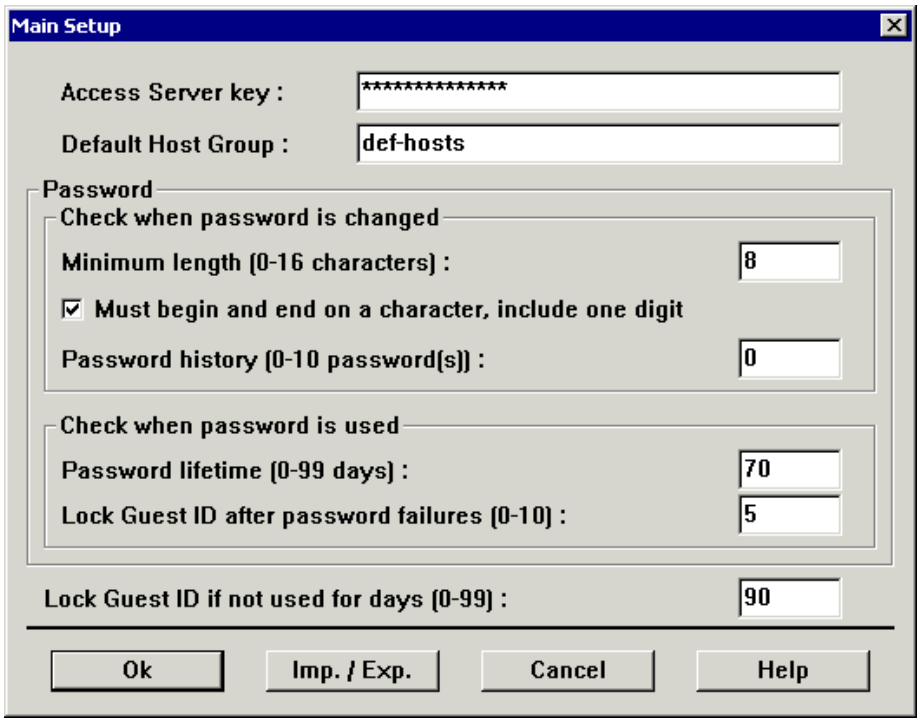
**Access Profiles:** Select this option to define security profiles for Guests and Hosts. These profiles contain details about Guest and Hosts access privileges. You can also assign Host groups to these profiles.

**Guests:** Press this button to configure details about Guests in the Access Server database. Select this option to add, edit or delete Guest security information. Also use this section to assign Administrator privileges to users.

To exit the configuration program at this stage press the *Exit* button.

## 9.3.3 Main setup

When the *Main Setup* button is activated from the main menu, the following dialog will be displayed:




To ensure that Guests are authenticated on an authorized Access Server, the content of the optional Access Server key is compared to the content of the corresponding key on the Host. Enter your own code in this field. Enter this same code on your Host(s). Please see section 5.6 'Security'.

### Default Host Group

In this field you may specify a Host Group set as the Default Host Group. If a particular Host is not set up in the Access Server it will be assigned to the Default Host Group. For more information regarding Host Groups please refer to Section 9.3.5

*Note: This option should not be used when using Guest Side Authentication.*

### Minimum length

Enter a number of alphanumeric characters which should be the minimum length of a password, for example, enter '11' means that the user must have a password containing at least 11 characters.

### Must begin and end on a character, include one digit

Enable this check box if the password should begin and end with a letter and also include at least one digit.

### Password history

Use this option if you wish to force the user to vary their passwords. For example, enter '2' means that the user cannot use their current and previous password when they try to change their current password.

### Password lifetime

Choose how long a password is valid for. Enter a digit between 0-99 days, for example, enter '10' means the password can be used for 10 days only.

### Lock Guest ID after password failures

Choose whether the Access Server should lock the user ID if a password is entered incorrectly. Enter a digit between 1-10, for example, enter '3' means that if the user enters 3 incorrect passwords in any one login attempt, then the Access Server will disable this user from logging on.

### Lock Guest ID if not used for days

This option allows you to disable the user ID if it has not been used for a certain number of days. Enter a digit between 0-99, for example, enter '20' means that if the user has not logged onto the Server for 20 days since his last login, then the user ID will be disabled. Note that this option is not relevant to users with Administrator rights.

### Import/Export

It is possible to import Hosts or Guests to the Access Server configuration program from a comma separated text file. Pressing the *Imp./Exp.* button brings up a dialog where you can enter the path and file name for the file you want to import from. The format is: Host (Or Guest) ID, Comment, Host group E.g.:

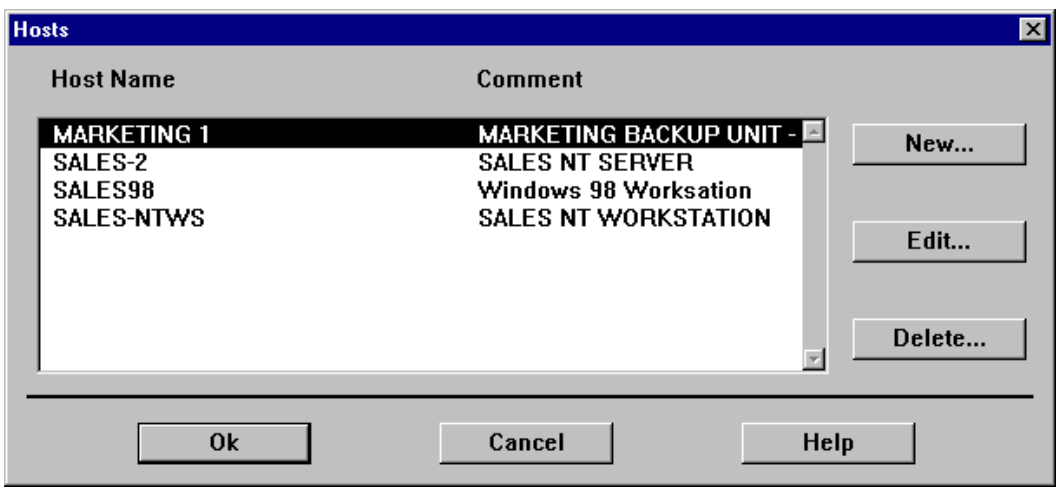
PSmith,Peter's computer,Sales

This will create a Host entry with the ID PSMITH in the group Sales with the comment "Peter's computer". With the radio buttons, you select whether you wish to import or export, when you click Ok.

Press the *OK* button to accept any changes made or otherwise press the *Cancel* button.

## 9.3.4 Hosts

When the *Hosts* button is activated the dialog presented in the following figure will be displayed:



From this dialog it is possible to view all Hosts that are currently defined in the Access Server database.

Also use this dialog to create new Hosts and edit or delete existing Hosts.

To create a new Host press the *New* button and the *New Host* dialog will be displayed.

Enter the Host name in the *Host name field*. If you require any additional information about the Host you can use the *Comment* field. This field is purely for your reference and does not affect how the server program functions. Once you have entered the Host details, press the *OK* button to continue. This Host will now be added to your Host list.

Use *Edit* to change a comment and *Delete* to remove a Host.

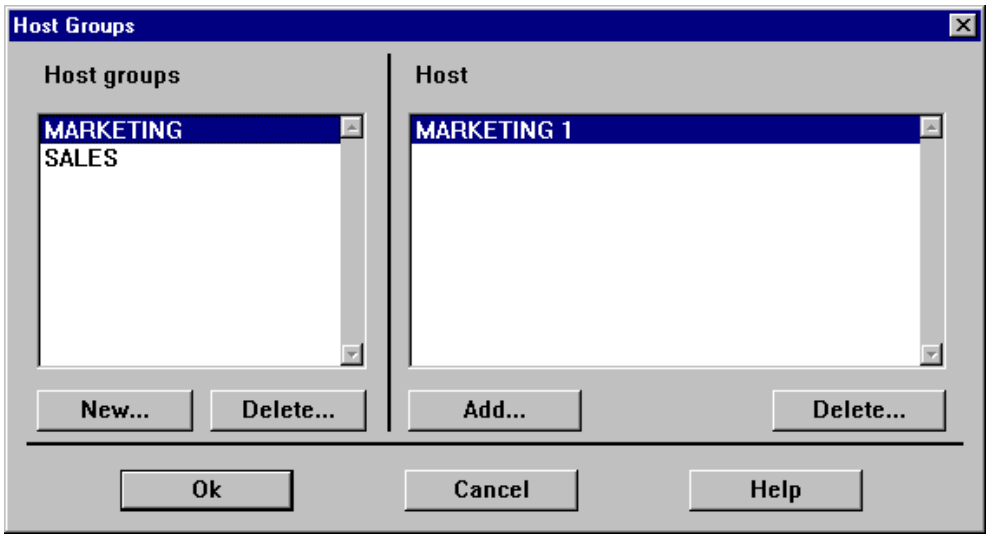
If you wish to change a Host name, you will need to delete the Host and then add a new Host and give it a new name. This can be done by selecting the Host name in the *Hosts* dialog and pressing the *Delete* button. Then return to the steps above if you wish to add a new Host.

To accept your changes and return to the main menu dialog press the *OK* button in the *Hosts* dialog box.

### 9.3.5 Host Groups

To manage the list of Hosts in the Access Server database, it is possible to setup Host groups that contain various Hosts.

When the *Host Groups* button is activated from the main menu the following dialog will be displayed:




The Host Groups dialog contains two sections listing the Host group name and the Hosts attached to that group. To view which Hosts are members of a group, select the group name and the corresponding Hosts will appear in the opposite window. Note that a Host can only be a member of one group.

To create a new group, press the *New* button in the *Host groups* section of the dialog. In the resulting dialog enter a name for the new group in the *Group name* field. Press the *OK* button to accept the new group. When you return to the *Host Groups* dialog, you will notice that the new group has been added to the *Host groups* section.

To add a Host to any group, ensure that the correct group name is selected and then press the *Add* button in the *Host* section of the dialog.

In the *Host Name* field, it is possible to click on the drop-down list to the right of the field, which will display a list of available Hosts. Simply select one of these Hosts and press the *OK* button to add to the group.

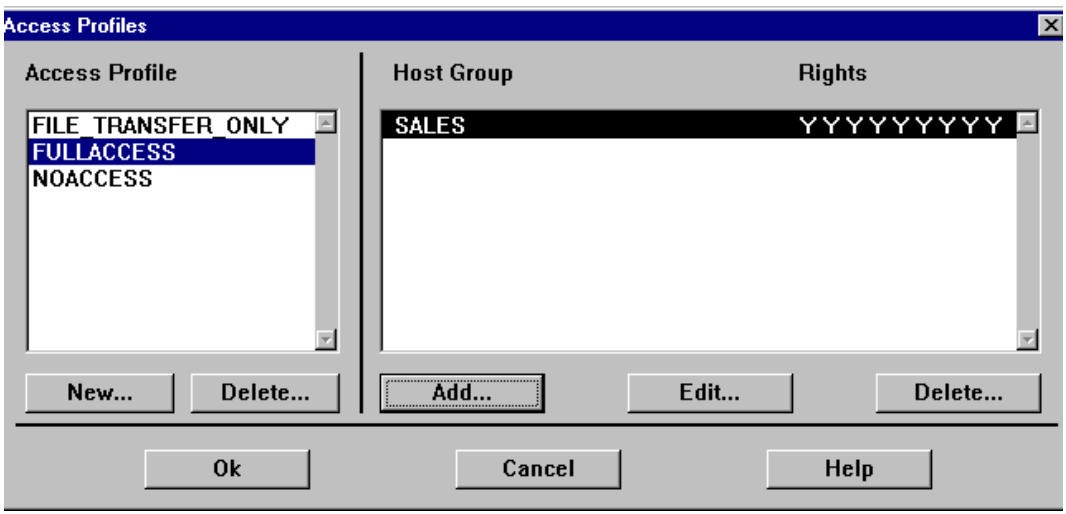
It is not possible to add a new Host from this dialog, however, if you press the *Edit* button this will take you directly to the *Hosts* dialog (see section 9.3.4 'Hosts') where you can add new Hosts to the Access Server database.

If you wish to cancel this operation at any time, press the *Cancel* button.

## 9.3.6 Access Profiles

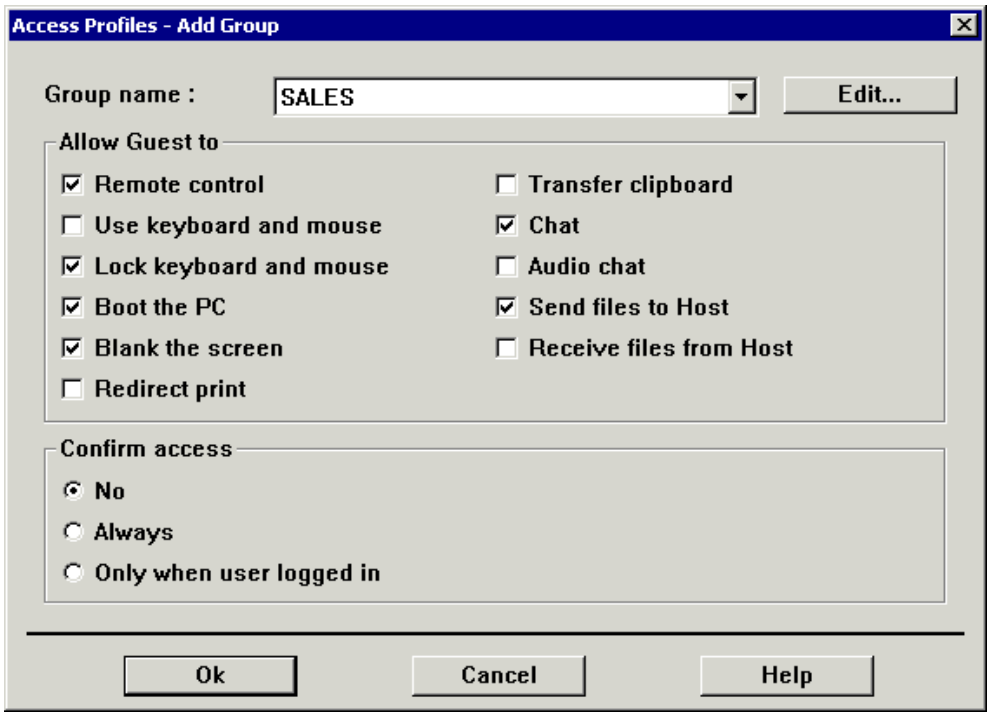
This section describes how to setup Access profiles which contain rights for Guests and Hosts that are managed by the Access Server.

When the *Access Profiles* button is activated from the *Main Menu* dialog, the following dialog will be displayed:




This dialog has two main sections, *Access Profiles* and *Host Groups*. Access Profiles contain access rights that Host groups can be assigned to (individual Guests can also be assigned to an Access Profile which is explained later in section 9.3.7 'Guests'). You can view which Host groups are assigned to what Access Profile by selecting the *Access Profile* name and the corresponding Host groups will appear in the opposite window.

To create a new Access Profile, press the *New* button in the *Access Profile* section of the dialog. The resulting dialog will ask you for a Profile name. Enter a name in the *Profile name* field and press the *OK* button. You will notice, when you return to the *Access Profiles* dialog, that your new Access Profile has been added to the Access Profile list.




To assign a Host group to any access profile, select the appropriate Access Profile and press the *Add* button in the *Host Group* section of the dialog. The following dialog will be displayed:

It is possible to add a group name by selecting the drop-down list to the right of the *Group name* field. This list will contain existing Host groups. Simply select a group name from the list.

It is not possible to enter a new group name from this dialog, however, by pressing the *Edit* button will take you directly to the *Host Groups* dialog where you can add new Host groups (see section 9.3.5 'Host Groups').

Before confirming the new Access Profile there are various option in the *Allow Guest to* section of this dialog which contains information about what actions the Guest can perform on Hosts that are assigned to this profile.

### Remote Control

Specifies whether a Guest is allowed to start a remote control session.

Note: If both Guest and Host are version 6.x or over, disabling this option will also display the use Keyboard and mouse, Blank the screen, Lock keyboard and mouse, and Boot Host options.

### Use Keyboard and mouse

If this option is disabled the Guest will not be able to remote control the Host's keyboard and mouse, but only view the screen. Sometimes referred to as *View only*.

### Lock keyboard and mouse

Specifies whether the Guest is allowed to lock the Host's keyboard and mouse.

### Boot Host

Specifies whether the Guest is allowed to boot the Host PC.

### Blank the screen

Enable this to allow the Guest to blank the screen on the Host.

### Chat

Specifies whether the Guest is allowed to start a chat (see 5.9.1 'Chat' for a description of chat).

### Audio Chat

Specifies whether the Guest is allowed to start an Audio Chat.

### Send files to Host

Specifies whether the Guest is allowed to transfer files from the Guest to the Host.

### Receive files from Host

Specifies whether the Guest is allowed to transfer files from the Host to the Guest.

To select any of these options, simply enable the check boxes to the left of each option.

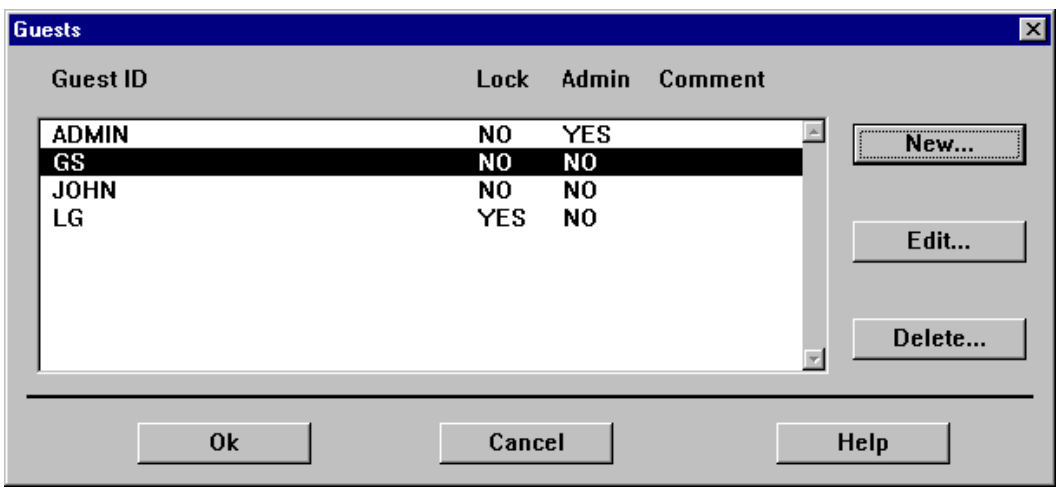
When you are happy with your selection press the *OK* button to add the Host group to the profile. When you return to the *Profiles* dialog you will see that the Host group has been added in the *Host Group* list.

To cancel adding a Host group to an access profile press the *Cancel* button in the *Access Profiles:Add group* dialog.

## 9.3.7 Guests

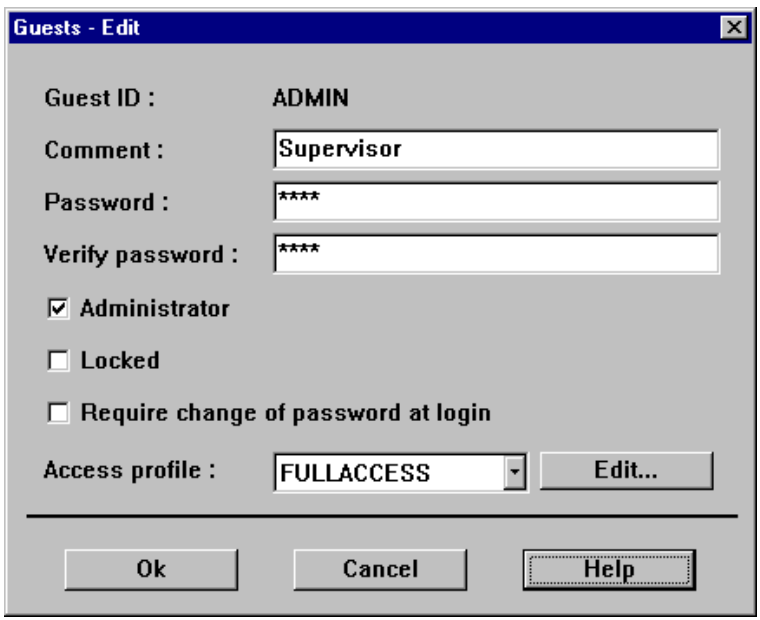
This section contains security and access information for Guests that have been defined in the Access Server database.

When the *Guests* button has been activated the dialog in the following figure will be displayed:



From the dialog box you can create new Guests and edit or delete existing Guests. This is also the section of the configuration program where you can add Administrators for the Access Server.

To add a new Guest press the *New* button, the following dialog will then be displayed:




### Guest ID

Enter the name of the Guest in the *Guest ID* field

### Comment

If you have any additional information about the Guest, enter it in this field. This field is purely for your reference only and does not affect the Access Server program.

### Password

This password is used when a Guest or administrator logs onto the Server. It is an optional feature, however we do recommend a password is given to users at Administrator level. Whenever the password is changed or defined it will also have to be verified.

### Administrator

Enable this check box if you wish the Guest to have administrator privileges. Note that if this option is enabled the user will be able to make changes to the Access Server database using the configuration program.

### Locked

Enable this check box if you wish to lock a Guest from using the Access Server. To unlock a user disable the check box.

### Require change of password at login

Enable this check box if you require the Guest to change their password when they next logon to the Server.

### Access Profile

It is necessary to assign an Access profile to a Guest (see section 9.3.6 'Access Profiles') You can select an existing profile from the drop-down list to the right of the *Access profile* field or create a new or view an existing profile by pressing the *Edit* button.

When you have selected the options for your new Guest press the *OK* button. You will see that the Guest has been added to the Guest list in the *Guests* dialog.

To cancel adding a new Guest press the *Cancel* button in the *Add Guest* dialog.

To edit Guests properties select the Guest name and press the *Edit* button. You will be able to edit any details about the Guest apart from the Guest ID. If you wish to change the Guest ID, you should delete the Guest by selecting the Guest name and pressing the *Delete* button. Then add a new Guest giving it the correct name.

# Chapter 10
# The NetOp Gateway

## 10.1 Summary

This chapter describes how to use the NetOp Remote Control Gateway software. The Gateway is a special version of the Host. It was invented as a converter between the different communication profiles. But as the name indicates, it is most often used as a dial-in point to a network or as a dial-out point from the network.

The Gateway can be configured to be an incoming gateway, which only accepts calls, or to be an outgoing gateway, which helps users on the network share lines out of the house. It is also possible to let it handle both tasks simultaneously. An outgoing Gateway can call in to an incoming Gateway, as well as to a normal Host.

You can dial in using any profile based on one of the dial-in communication devices TCP/IP (TCP), Windows modem, Serial or IrDA. The Gateway can call out using the same profiles. It will route incoming calls on to Hosts on the network using any profile based on any of the network communication devices TCP/IP (UDP), IPX and NetBIOS.

The NetOp Gateway allows you to browse on the network behind it from an outside line, or it lets you connect directly to one of the Hosts on the network. With NetOp 6.5 this extends to browsing on a local network from the Internet, if just 1 of the computers has a public IP address.

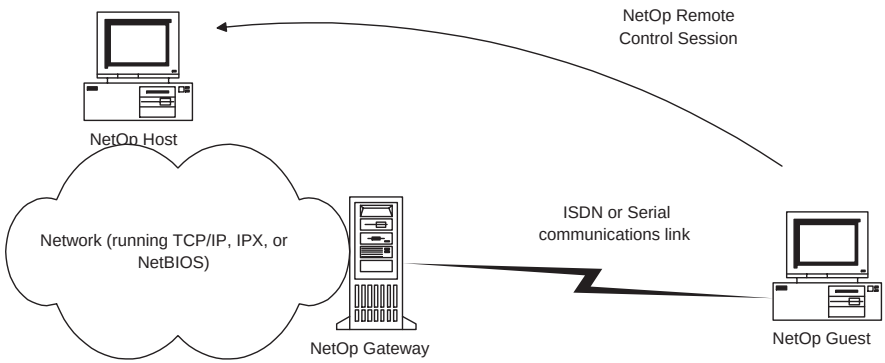
You can remote control the Gateway itself, because it is an extended Host. When you contact an outgoing Gateway, you must use a special communication device type named ‘gateway’.

## 10.2 Introduction

A NetOp Gateway can be any multi-homed computer with two or more of the NetOp supported communication standards installed. As it’s primary function a Gateway acts as a routing mechanism between different environments utilizing different communication standards. It can provide a single dial-in/out point for all NetOp remote control traffic, allowing for example a Guest dialing in using the ISDN (CAPI) standard to remote control all Hosts on an IPX network where the NetOp Remote Control Gateway module is installed .

The following diagrams explains in detail some of the possible implementation of a NetOp Gateway.

*Note: Outgoing Gateway functionality is available ONLY in NetOp Remote Control Version 6.x*



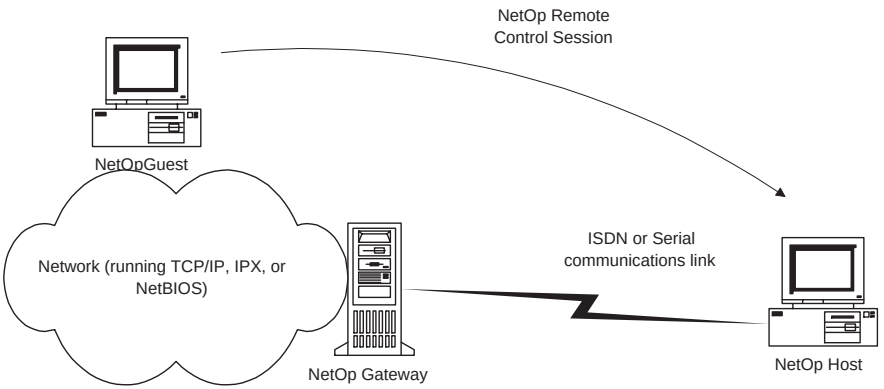

*and up.*

**Diagram 10.1 - Gateway functionality Example 1**

Diagram 10.1 represents a NetOp Guest using a dial-up protocol (ISDN(CAPI) / Serial / TCP/IP (TCP) / IrDA) to dial into a Gateway which then routes the call using a networking protocol (IPX , TCP/IP (UDP) or NetBIOS) to a NetOp Host. Using the Gateway as a protocol converter, the Guest is able to initiate a remote control session with a networked Host, even though it is using a dial-up protocol only.

Please note that is this diagram and in the following diagrams, only modem and ISDN are listed as profiles which can dial in to a gateway. With version 6.5, TCP/IP (TCP) and IrDA have this capability, though it is not listed in the diagrams

**Diagram 10.2 - Gateway Functionality Example 2**




The next example represents some of the outgoing Gateway functionalities. An outgoing NetOp Gateway allows a Guest using networking protocols exclusively to communicate with a Host using a dial-up protocol only. The Gateway acts as a protocol converter, routes the outgoing call from the Guest's Network to the Host as shown in the Diagram 10.2.

**Diagram 10.3 Gateway Functionality Example 3**

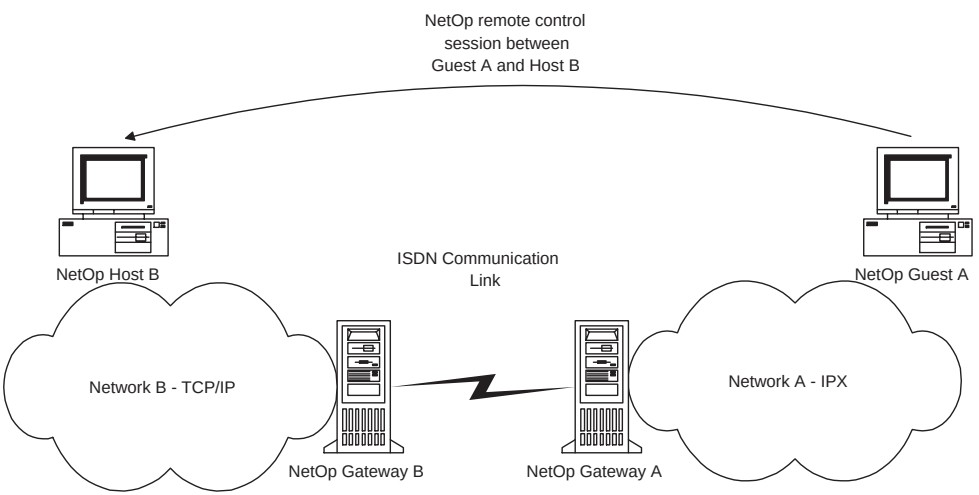
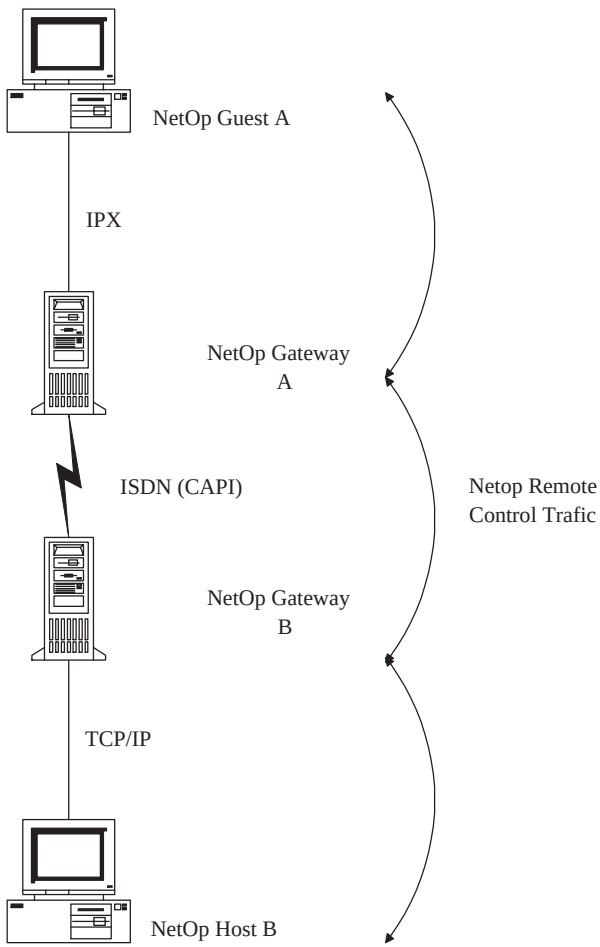


Diagram 10.3 shows a slightly more complex setup, involving two networks. A Guest located at Network A using the IPX communication protocol initiates a remote control session, which is in turn routed by outgoing Gateway A using the ISDN(CAPI) dial-up protocol to incoming Gateway B. Gateway B then routes the call to Host B by using TCP/IP (UDP) initiating the remote control session.

The Gateway routing sequence can also be represented as shown below:

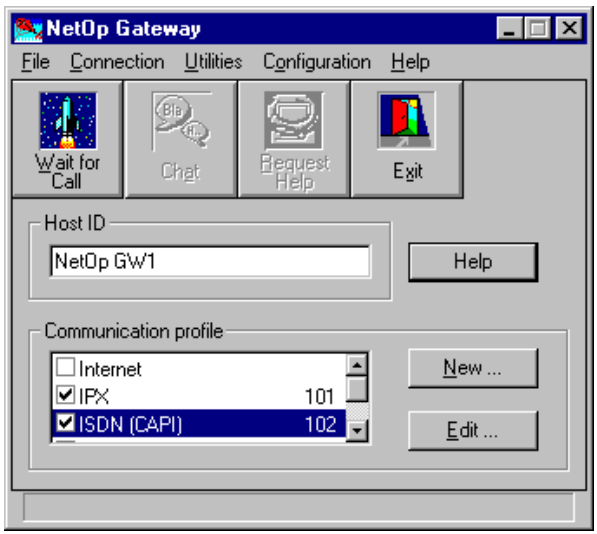


## 10.3 Starting the Gateway

To start the NetOp Gateway, double click on the Gateway icon in the NetOp program folder or start the program NGWW32.EXE (or NGWW.EXE on Windows 3.x PCs).

The first time the Gateway is run the program will offer to guide you through configuration of your modem. Follow the on-screen instructions.

After this you will be presented with the NetOp Gateway dialog box as shown in the following figure:




## 10.4 Configuration

The Gateway interface is very similar to that of the NetOp Host module. The following is a description of the fields in the main Gateway dialog.

### 10.4.1 Host ID

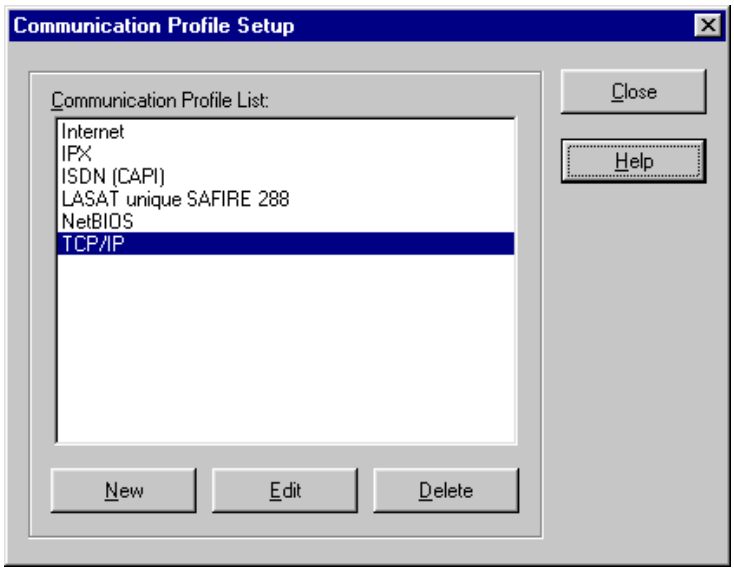

This is the name used by Guests to identify the Gateway.

### 10.4.2 Communication profile


This is where the communication profile is selected. The communication profile specifies a communication device and parameters related to that device. Select each protocol by enabling its checkbox.

## 10.5 Communication profiles

The NetOp Gateway comes with a number of predefined communication profiles, one for each supported device except TCP/IP (TCP). To maintain the communication profile database, select *Communication profiles* from the *Configuration menu*. This activates the dialog box shown in the following figure:




The list shows you the existing records in the database which are always sorted alphabetically.

### Searching

You can search for a record by pressing a key. For example pressing A will move you to the first profile starting with the letter ‘A’ (or ‘a’).

### Inserting

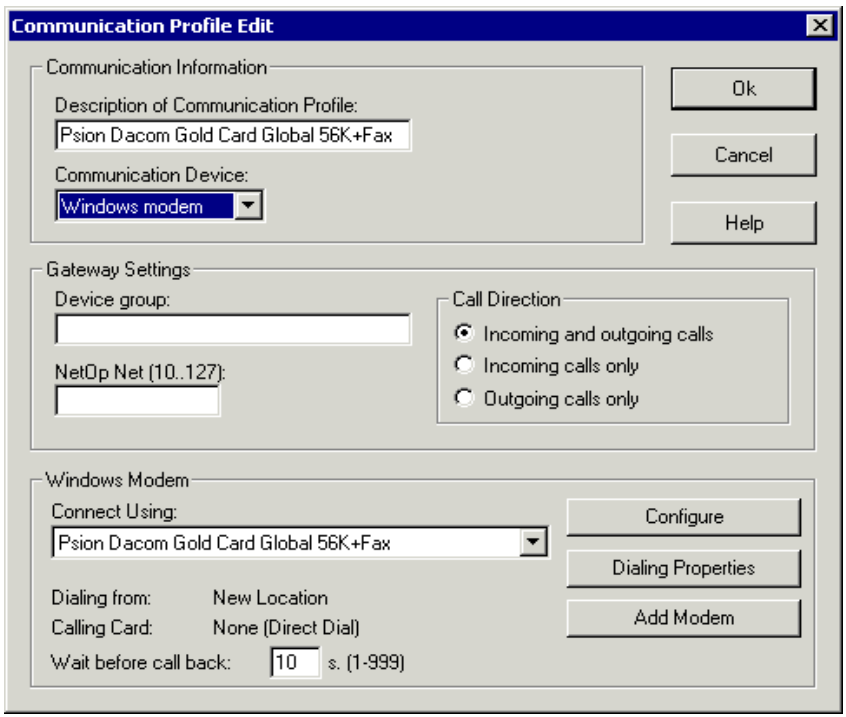
If you activate the *New* button (or press ALT+N), you will add a new record to the database, its contents will be similar to the selected profile’s (except for the name which will be blank).

### Deleting

You can delete records by clicking the *Delete* button (or by pressing ALT+D on your keyboard).

### Editing

If you activate the *Edit* button (or press ALT+E) you will edit the selected record. A new dialog box will appear as in the following figure:




## 10.5.1 Communication information

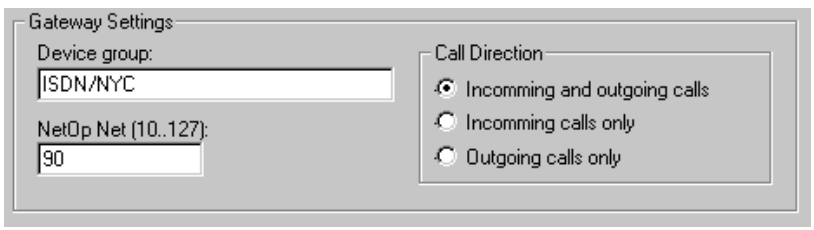
### Description of communication Profile

This is the name with which you wish to identify the current communication profile.

### Communication Device

Choose the communication device to use for the profile. It can either be NetBIOS for Microsoft/IBM networks or compatible, IPX for Novell networks or compatible, TCP/IP for IP networks, Windows Modem/serial for modem or null modem communication or ISDN for communication on the ISDN network with a CAPI compatible adapter. Consult your system administrator if you are in doubt about which device you should use for communication. For more info regarding communication profiles please refer to chapter 11.

## 10.5.2 Gateway Settings




### Device Groups

Lets the user specify the Device Group name that will be used for the particular communication profile chosen. See section 10.6 ‘Gateway Specific Settings’ for more details.

### NetOp Nets

This specifies which NetOp Net should be used with this communication device. See Section 10.6 ‘Gateway Specific Settings’ for more details.

### Call Direction

Specifies weather the Gateway will allow for incoming calls, outgoing calls or both.

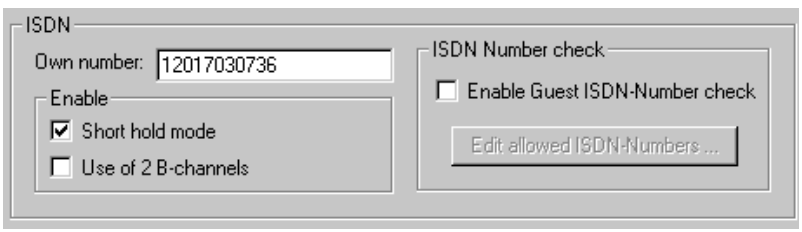
*Incoming and outgoing calls* - When this option is selected the NetOp Gateway will allow for incoming calls from remote locations (using the dial-up profiles), and for outgoing calls originating at the Gateway's own network (using network profiles).

*Outgoing calls only* - Select this option to allow only outgoing calls originating from the Gateway's own network (using network profiles).

*Incoming calls only* - When this option is selected the Gateway will allow for incoming calls from remote locations (using the dial-up profiles) only.

*Note: The Device Group and Call Direction options can only be changed when editing a dial-dp communication profile.*

## 10.5.3 Device Specific Settings




The Device Specific Option will be shown when using one of the dial-up communication devices. Please refer to chapter 11 'Communication Profiles' for more details.

## 10.5.4 Selecting Gateway Communication Profiles

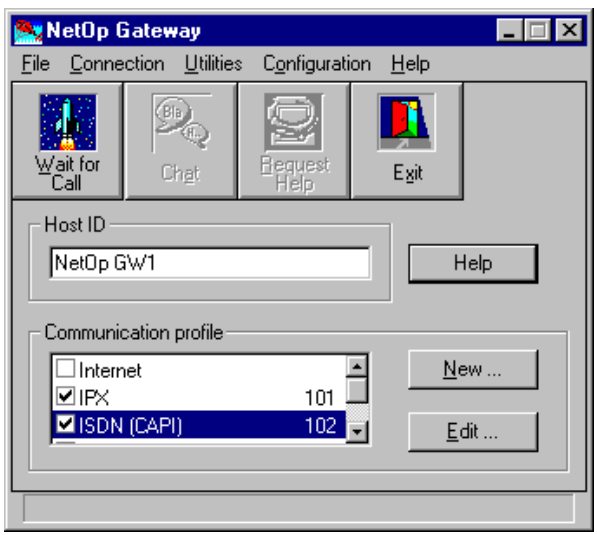
As in the NetOp Host module, it is possible to select more than one communication profile for the NetOp Gateway. For example, a Gateway can be contacted via modem allowing a remote Guest to browse and control Hosts using IPX, NetBIOS and TCP/IP (UDP) without disconnecting. By the same logic a Guest using a networking protocol to call the Gateway can establish a session with a remote Host using a dial-up communication profile through the Gateway. This can be done by selecting the appropriate communication profiles check box in the communication device section of the main Gateway dialog.

It is also possible to setup multiple lines to connect to one Gateway PC. This is particularly useful when more than one Guest wishes to connect to the Gateway or when the Gateway will be accessed by more than one Guest simultaneously to remote control Hosts using a dial-up communication profile. For example, if your machine has two COM ports, it is possible to connect two modems (which are connected to two separate lines) and allow two different Guests to use the Gateway for connecting to their networked PC's.

As in the standard NetOp Host, the communication profiles used by the Gateway are selected at the main Gateway dialog

The following figure shows a NetOp Gateway routing NetOp remote control traffic between the ISDN(CAPI) communication profile and IPX:

The selected communication profiles are marked by a check-mark.



## 10.6 Gateway Specific Settings

When editing a NetOp Gateway communication profile, some extra features are available for editing to help identify particular Gateway functionality. These features are the NetOp Nets, Device Groups, and Call Direction option. The following section focuses on the Gateway Specific Settings and proper configuration and troubleshooting methods that will insure the Gateway works properly.

### 10.6.1 NetOp Nets - Incoming Calls

When you select a communication profile from the communication device section of the main Gateway dialog, a number will appear to the right of the profile. This number is referred to as the NetOp net. This number can be changed by editing the Gateway Settings section of the communication profile.

Normally these fields need not be changed.

It is only necessary to alter the NetOp net numbers in a situation where there are multiple incoming Gateway PCs on a single network. In this situation the following rules apply:

1. The NetOp net number that is attached to the network protocol must be the same on all the incoming Gateways attached to the network. A NetOp net number assigned to a network protocol must be different from every NetOp net number attached to a dial-up protocol.

2. The NetOp net number for the dial-up protocol must be unique on every incoming Gateway and it must be different from the NetOp net number attached to the network protocols.

3. NetOp net numbers must have a value between 10 and 127.

Other than that, the NetOp net numbers can be arbitrarily chosen. NetOp uses net numbers from 100 as default for the first communication profile selected and then continues in sequence for all later profiles.

Example:

A network has three Gateways attached to it. On all three Gateways, the NetOp net number for the *Network protocol (IPX)* is set to 101. The NetOp net number for the *Dial-up protocol (Modem)* is set to 102 on the first Gateway, 103 on the second and 104 on the third.

## 10.6.2 Device Groups - Outgoing Calls

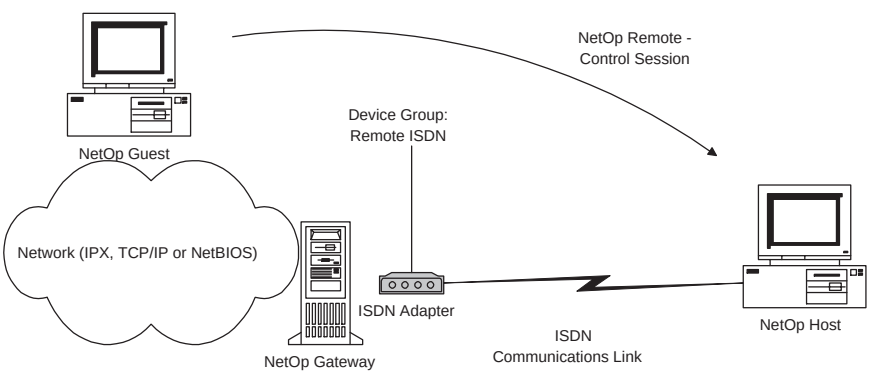
A Device Group associates various dial-up communication profiles on different Gateways. This is done to help group particular Gateways for the purpose of routing outgoing calls.

When a Guest chooses a Gateway communication profile in order to make an outgoing call he is presented with the option of choosing a Device Group or Browsing for Device Groups.

The Device Group identifies the dial-up profile on a Gateway (or multiple Gateways) that is used to reach a particular Host or Hosts at a remote location.

The following diagrams present some examples of Device Group functionality.

**Diagram 10.5 - Device Groups Example 1**



In diagram 10.5 a NetOp Guest is shown initiating an outgoing call through a NetOp Gateway to a remote site. The Guest has specified that for this outgoing call it will be using device group 'Remote ISDN'. At the Gateway the particular Device Group is associated with an ISDN Adapter. The Gateway will then convert the outgoing call from the particular networking protocol to the ISDN(CAPI) interface and route it using the ISDN adapter to the remote location.

**Diagram 10.6 - Device Groups Example 2**

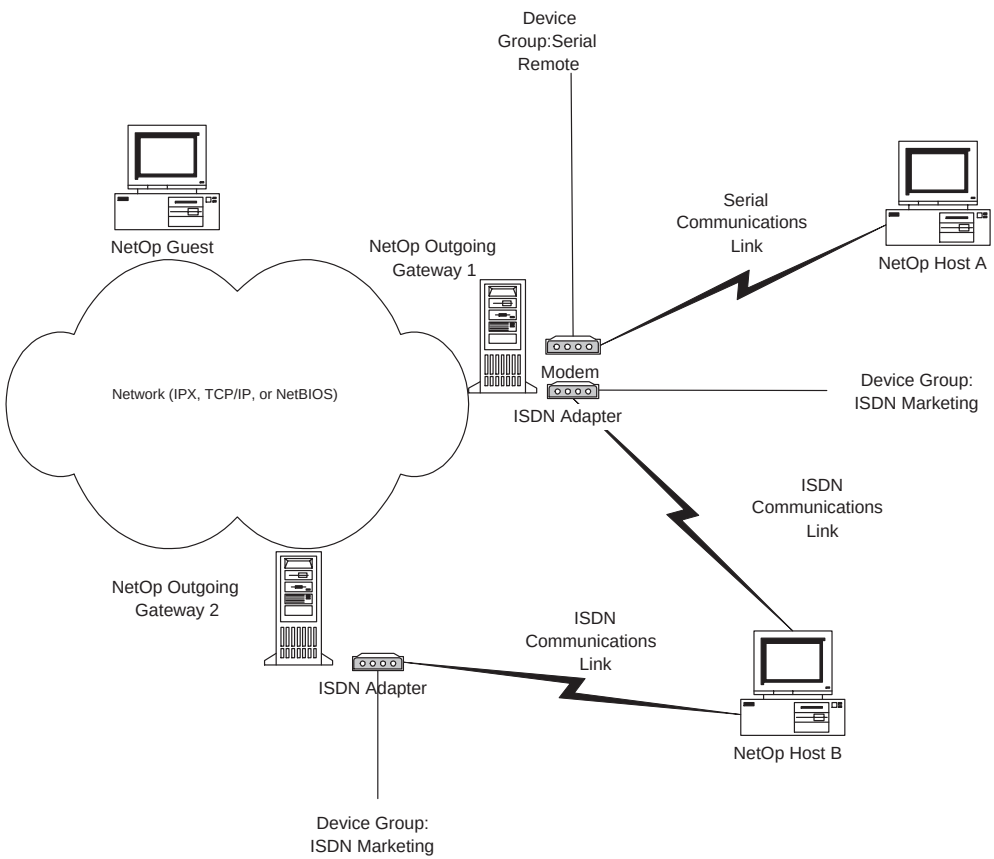


Diagram 10.6 illustrates the following device group associations.

Gateway 1:

Modem - Device Group: Serial Remote

ISDN adapter - Device Group: ISDN Marketing

Gateway 2:

ISDN adapter - Device Group: ISDN Marketing

1. A NetOp Guest attempts to make an outgoing call using the Serial Remote Device Group. Since the Device Group is associated with the modem on Gateway 1, the outgoing call will be routed through the Gateway 1 modem to the remote location.

2. The same NetOp Guest makes another outgoing call using Device Group: ISDN Marketing. Since the particular Device Group is associated with an ISDN adapter on both Gateway 1 and Gateway 2, the call will be routed through the ISDN adapter attached to the first available Gateway (first Gateway to respond).

*Note: When a user at the Guest selects to browse for device groups, a list will appear presenting the Guest with a rundown of available outgoing Gateway to select from. For more info see chapter 4 'The Guest'.*

## 10.7 Security

The NetOp Gateway contains advanced security features to prevent against unauthorized access.

The security configuration of the Gateway is divided into *Gateway security* and *Host security*.

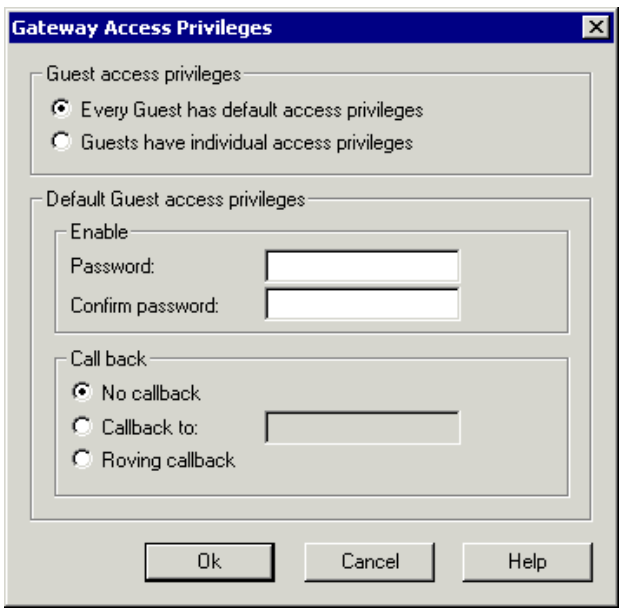
Gateway security must be passed in order to remote control any Host on the network through the Gateway. In addition the individual Host security settings are still active and must be passed as well. Thus Gateway security can be viewed upon as a firewall, which protects the entire network from unauthorized access.

Host security governs security for the Host part of the Gateway, both for external Guests calling through a dial-up profile to remote control the Gateway and for network Guests which want to control the Gateway PC.

## 10.7.1 Gateway Security

The Gateway security is accessed by activating *Gateway Access Privileges* from the *Configuration* menu.

Once Gateway access privileges has been selected, the following dialog will be displayed:




## 10.7.2 Two Levels of Security

You can choose between two different ways of configuring security for the Gateway, default or individual access privileges.

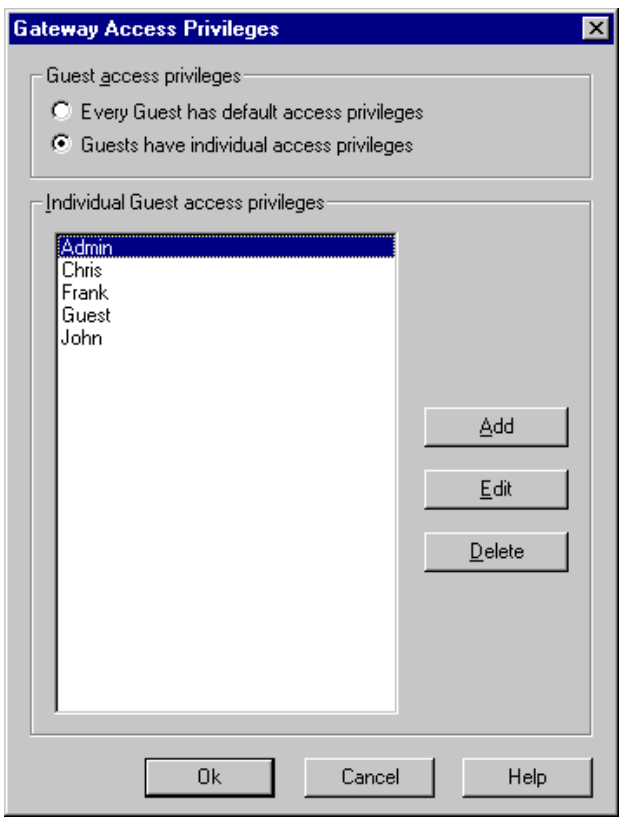
## 10.7.3 Default Access Privileges

This is the simplest way to configure the security. When using default access privileges you only specify one set of security settings which are used for every Guest connecting to the Gateway.

A Guest user will not have to identify himself with a name when connecting to the Gateway but might have to enter a password if one has been defined.

Select *Every Guest has default access privileges* in the *Guest access privileges* section to use this mode of security configuration. If this option is selected you specify the options directly in the *Default Guest access privileges* section of the dialog box.

## 10.7.4 Individual Access Privileges



This is a more advanced way of configuring the security on the Gateway. Using individual Guest access privileges, you specify separate settings for every Guest. For instance you can allow some Guests to be able to call back to a fixed number and prevent other Guests using the Callback feature.

A Guest user has to identify himself with a name and a password (if any) when connecting to the Gateway.

Select *Guests have individual access privileges* in the *Guest access privileges* section to use this mode of security configuration. If this option is selected you will see a list representing the defined Guests.

Here you can maintain your list of Guests allowed to access the Gateway.

Press the *Add* button to add a new Guest. You can also edit or delete Guests on the list by highlighting the Guest name and pressing the *Edit* or *Delete* buttons.

## 10.7.5 Password

The Gateway can be protected by a password which a Guest has to enter correctly in order to gain access to the Hosts.

For default privileges you can specify one password which every Guest must enter before gaining access to any other Hosts on the network. For individual privileges you can choose different passwords for the different Guests. In the *Enable* section, enable the *Password* checkbox and enter a password in the field provided.

## 10.7.6 Callback

If Callback is enabled, the Gateway will answer incoming calls from a Guest and then hangup and call the Guest back.

The Callback facility serves two purposes:

1. Security: By specifying a Callback number it can be ensured that the Host is only controlled from specific telephone numbers.

2. Phone charges: Callback can be used to reverse phone charges from Guest to Host.

There are three different settings for Callback:

1. No *Callback*: No Callback will be performed.

2. *Callback to*: A Callback is attempted to the specified number.

3. *Roving Callback*: The Guest is prompted for the number to call back to.

#### Default privileges

Set the Callback level in the *Callback* section of the *Default access privileges* dialog.

#### Individual privileges

Callback settings are used for each Guest user. Activate *Edit* for a Guest in the Guest list and set the Callback level for this Guest in the *Callback* section of the resulting dialog box.

### 10.7.7 Host security

The NetOp Gateway also includes a number of Host security features. Use these features to prevent unauthorized access from a Guest who wants to control the Gateway, either from the network or from an external Guest. These features are accessed by activating *Guest access privileges* from the *Configuration* menu.

Configuring Host security is described in detail in section 5.6, ‘Security’.

## 10.8 On-line Choices

The Gateway has the same on-line choices as the Host. Please refer to section 5.9, ‘On-line choices’ for a description of these. Please note that these choices are only relevant when the Gateway is being remotely controlled, not when there is only pass-through sessions to other Hosts.

## 10.9 Command Line Parameters

The Gateway accepts the same command line parameters as the Host program, please refer to section 5.10, ‘Command Line Options’ for a description of these. The command line parameters refer to the Host part of the Gateway.

# Chapter 11
# Communication Profiles

# 11.1 Introduction

All NetOp communication goes via a communication profile. Communication profiles are specific instances of a Communication Device. NetOp 6.5 has a number of devices. Some are networking devices, some are dial-up, point-to-point devices. The most important network devices are: TCP/IP (UDP), IPX and NetBIOS. The most important dial-up devices are TCP/IP (TCP), Windows modem, Serial, ISDN (CAPI 2.0) and Infrared (IrDA).

When you first start NetOp, there is a communication profile created for you based on each device, except TCP/IP (TCP). You will se a profile named TCP/IP for compatibility reasons. This profile is based on the TCP/IP (UDP) device. You can add as many extra profiles as you wish.The following sections provide a detailed description of the NetOp communication profiles.

# 11.2 NetBIOS

## 11.2.1 Description

NetBIOS was once one of the most popular protocols for LAN communication. The NetBIOS protocol is typically used in LAN Server, LAN Manager, LANTastic, and Windows NT Server environments.

## 11.2.2 Device Specific Settings

To communicate with NetOp Remote Control or NetOp for OS/2 Hosts use the *NetBIOS* device. To communicate with DOS Hosts (NetOp 4.3x RemPCs), use the *RemPCNB v4.3* device (this device is only available on NetOp Remote Control Guests).

The communication profile edit dialog contains one specific setting when the communication device is set to NetBIOS - the adapter number. The adapter number is defined in the NetBIOS setup.

NetOp will try to detect which adapter numbers are present on your machine and also tell you which type of NetBIOS is being used. To view this information, press the *List* button in the NetBIOS communication profile setup.

## 11.2.3 Host ID format

When configuring the Host a Host ID can be entered. The Host ID should be a string with a maximum length of 32 characters.

If no Host ID is entered NetOp will use the burnt-in network adapter address (typically the MAC address). To call a Host, which uses the burnt-in address as a Host ID, enter 0x*nnnnnnnnnnnn*, where *nnnnnnnnnnnn* is a 12 digit hexadecimal number

(e.g. 0x080005AF341A).

## 11.2.4 NetOp resource needs

NetOp's NetBIOS resource needs are displayed in the following table.

*n* is the number of simultaneous remote control sessions.

| | **Guest** | **Guest using RemPCNB** | **Host** |
|---|---|---|---|
| **Sessions** | *n* | *n* | *I* |
| **NCB's** | *n+4* | *n+8* | *5* |
| **Name** | *2* | *5* | *2* |

**Names:**

Every NetOp Remote Control Guest or Host adds the group NetBIOS name

DTL_NETOP_ (DTL_NETOP_ followed by six blanks).

To establish a session the NetBIOS command SEND DATAGRAM (command A0 hex) to the group name DTL_NETOP_ must be successful.

Furthermore each Guest and Host adds the unique name DTL_NETOP_*nnnnnn* where *nnnnnn* is 6 bytes representing the PCs MAC address. The main part of the NetOp traffic consists of NetBIOS session traffic between these names.

## 11.3 IPX

### 11.3.1 Description

IPX (Internetwork Packet Exchange) is Novell's network protocol. This protocol is typically used in Novell Netware environments.

### 11.3.2 Configuration

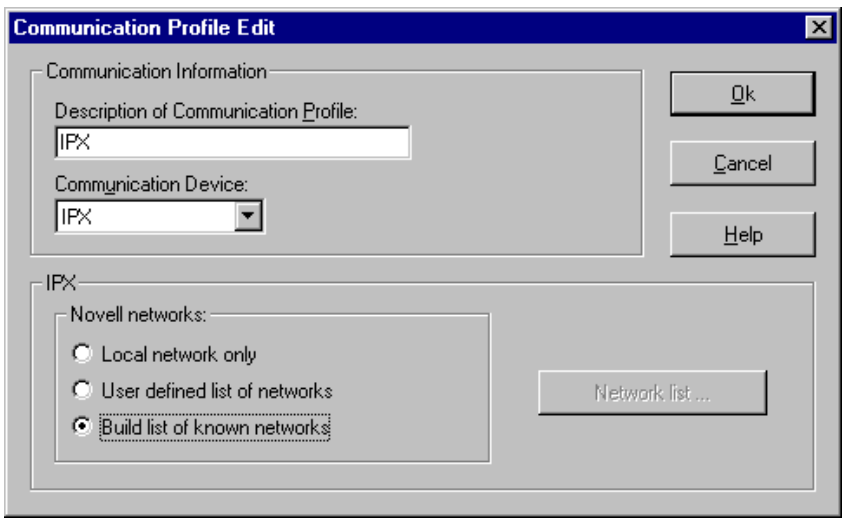
IPX is usually installed as part of a network client. If there are any problems with accessing IPX, please contact your network administrator.

### 11.3.3 Device Specific Settings

To communicate with NetOp Remote Control or NetOp for OS/2 Hosts use the *IPX* device. To communicate with DOS Hosts (NetOp 4.3x RemPCs) use the *RemPCIPX v 4.3* device (this device is only available on NetOp Remote Control Guests).

A Novell network consists of one or more sub-networks. Each of these sub-networks has an 8-digit hexadecimal number. The NetOp Guest must know the number of a subnetwork to communicate with a PC on that network.

The IPX device specific settings deal with interconnected sub-networks (see the following figure):




NetOp provides three alternatives to handling multiple networks:

### Local network only

If this option is chosen, NetOp will only be able to communicate with PCs which reside on the same subnetwork as itself.

### User defined list of networks

If this option is chosen NetOp will be able to communicate with PCs residing on one of the networks which is specified in the Network list (see section 11.3.4, ‘The IPX network list’).

### Build list of known networks (default)

If this option is chosen NetOp communicates with an IPX router or a Netware server to obtain a list of all the interconnected subnetworks.

## 11.3.4 The IPX network list

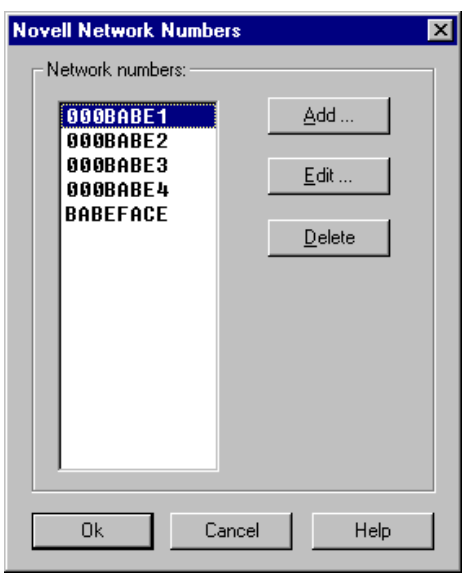
Normally the Guest will automatically communicate with an IPX router or a Netware server to obtain a list of all sub-networks. However there are some situations where this is not desirable:

1.Some Netware installations do not support the automatic building of a subnetwork list.

2. In large complex networks you might want to look for Host PCs on certain subnet-works only, or limit the *call for help* (see section 5.9.3, 'Call for Help') feature to certain sub-networks.

In these situations you can maintain a manual list of networks where you want NetOp to look for PCs:

1. Select *Communication profiles* from the Guest's *Configuration* menu.



2. Select the communication profile you want to use (must have IPX as communication device) and activate the *Edit* button (or press *New* to create a new profile).

3. In the IPX section of the dialog box set *Novell networks* to *User defined list of networks*.

Activate the *Network list* button.

The following dialog box will then appear:

Activate the *Add* button to add a subnetwork to the list. Press *Delete* to delete the selected subnetwork, press *Edit* to modify the number of the selected subnetwork.

To find the network number for a given computer, use Novell's NLIST (Netware 4.x). and USERLIST (Netware 3.x) utilities by issuing the following commands at a command prompt:

**nlist user=***NetwareLoginName* **/a** ENTER

**userlist** /a ENTER

Where *NetwareLoginName* should be substituted with the user's Netware login name. The *Address* field of the resulting listing contains the network number.

## 11.3.5 Host ID format

When configuring the Host, a Host ID can be entered. The Host ID should be a string with a maximum length of 32 characters.

If no Host ID is entered NetOp will use the burnt-in network adapter address (typically the MAC address). To call a Host, which uses the burnt-in address as a Host ID, enter 0x*nnnnnnnnnnnn*. Where *nnnnnnnnnnnn* is a 12 digit hexadecimal number

(e.g. 0x080005AF341A).

### 11.3.6 NetOp resource needs

NetOp uses IPX socket 8641 (hex) when connecting to Hosts. For RemPCIPX connections, NetOp uses socket 8186 and 8187 (hex). The sockets are allocated to Danware by Novell.

In order to connect to a Host at least one IPX broadcast to socket 8641 (hex) has to be able to reach the Host.

## 11.4 TCP/IP (UDP)

### 11.4.1 Description

The Internet Protocol (IP) is the most commonly used network protocol, on the Internet as well as on intranets. On top of IP, programs can use TCP, which is a safe point-to-point protocol, or UDP which is an unsafe network protocol. Here, safe means that the protocol checks for transmission errors. NetOp implements two communication devices on top of IP: TCP/IP (UDP) and TCP/IP (TCP). This is about TCP/IP (UDP).

When you start NetOp 6.5 for the first time, you will see two communication profiles based on IP. These profiles are named Internet and TCP/IP and they are based on the TCP/IP (UDP) device.

Even though UDP is not a safe transport, the NetOp TCP/IP (UDP) communication device is a secure transport. NetOp adds the same checking mechanisms to UDP as it does to for example ISDN, which is also an ‘unsafe’ transport.

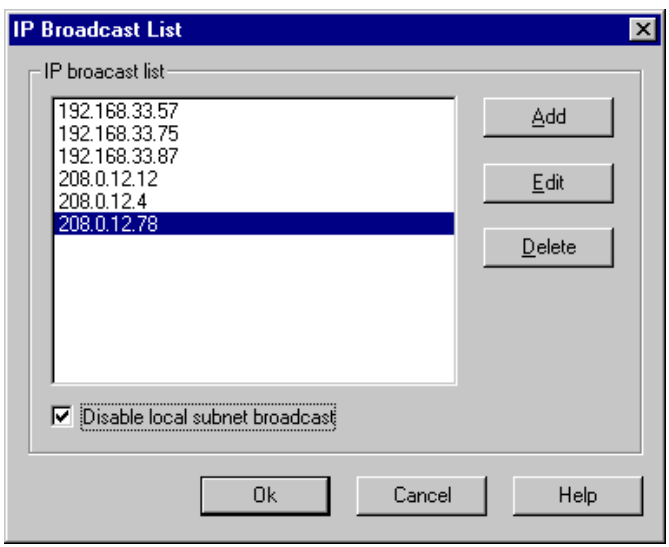
### 11.4.2 Device Specific Settings

There are two device specific settings in the Communication Profile Edit dialog for TCP/IP (UDP) based devices. The first is max packet size or maximum transmission unit (MTU). MTU is the maximum size of data packets attempted transmitted between Host and Guest. If this value is too large for the network to transmit successfully, NetOp will automatically lower the value used, until the transport succeeds. If you experience transmission errors, try lowering the MTU.

The default values for both NetOp TCP/IP devices are set to optimize for a fast local network. That is to use low compression and to use a large MTU. Optimize for Internet communication means that NetOp will now use different default values. Automatic compression now means high compression and the max MTU will default to 512. The default size for graphics buffers is also increased. It is only the defaults, which are changed. If you have set a specific value yourself, that is not changed.

## 11.4.3 IP Address Broadcast List

NetOp's default behavior is to browse for all PCs which are reachable with the reserved IP address 255.255.255.255. You may configure this setting and create your own unique IP address broadcast list by clicking on the *IP Address Broadcast List* button. This will bring up the following dialog box:



### Adding / Deleting IP Addresses

To add an IP address to the automatically updated list of addresses where NetOp should browse for PCs press the *Add* button. In the resulting dialog enter the IP address you wish to add and press *OK*.

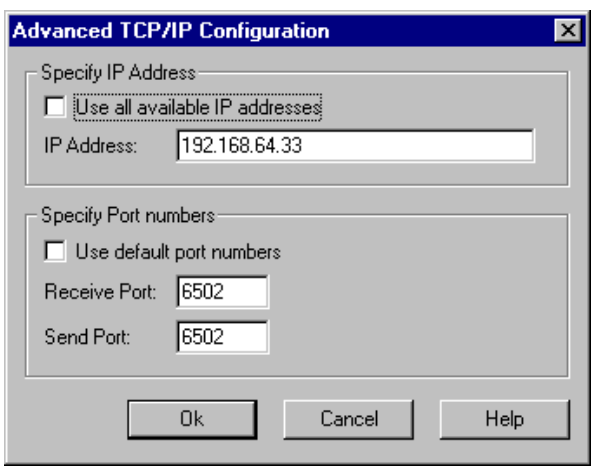
### Disable local subnet broadcast

Selecting this option will prevent NetOp from using the reserved IP Address 255.255.255.255 to send broadcasts on the local subnet. NetOp will only use the IP addresses added to the list by the user for TCP/IP communication. Selecting this option will in some cases reduce bandwidth taken up by broadcasts.

*Note: If this options is selected and no IP addresses have been added to the list, you will only be able to call Hosts using an IP Address or DNS name.*

## 11.4.4 Advanced TCP/IP Settings

Pressing *Advanced* brings up the *Advanced TCP/IP Configuration* dialog box:




In the Advanced TCP/IP Configuration dialog box it is possible to select the IP address for this communication profile. This means that if your computer has more than one IP address you can force NetOp to use a specific IP Address. You may even create a communication profile for each address and use these either simultaneously or one at a time, or use a single profile for all your addresses (this is the default).

You may also change the default (6502) port number to another number by un-checking the *Use default port numbers* check box. The 'Receive' port is your own port number, and the 'Send' port is the port you expect other NetOp machines to receive on.

This option makes it possible to communicate through firewalls and routers that change the port number on the packets that pass through.

Beware, however, that NetOp cannot simultaneously communicate with two machines that have the same IP address as seen from those two machines.

You can specify 0 for the receive port number and have arbitrary numbers assigned automatically.

## 11.5 ISDN

NetOp Remote Control supports two types of ISDN protocols:

#### 16-bit (Windows 3.x)

CAPI version 1.1, profile A (e.g. works with EuroISDN DSS1, German national ISDN 1TR6, French ISDN VN2, Belgian ISDN CT1, etc.) or CAPI 2.0 interface.

#### 32-bit (Windows 95/98 , Windows NT/2000)

CAPI version 2.0.

### 11.5.1 Configuration

ISDN CAPI (Common Applications Programmer's Interface) is a driver provided by your ISDN adapter mfg. (As most adapters support the CAPI interface you should still make sure the particular card you are using offers support for the CAPI version you will use with NetOp).

ISDN CAPI must be installed and loaded before you try to access it from the Guest, the Host or the gateway. If you cannot access ISDN CAPI from NetOp, please verify that a supported version is installed and loaded. Please note that a CAPI.DLL must be present.

For CAPI 2.0 the DLL is called CAPI20.DLL except on Windows NT 3.51 and NT 4.0 where it is called CAPI2032.DLL.

## 11.5.2 Device Specific Settings (CAPI 1.1)

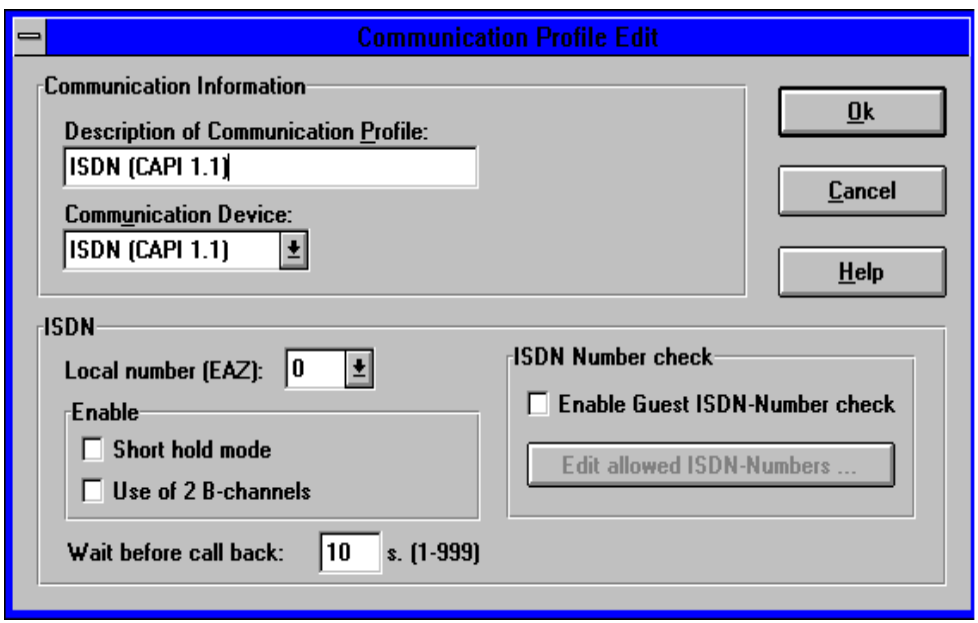
The following figure displays the communication profile edit dialog using the ISDN (CAPI 1.1) specific settings:

### Local Number

Enter the local number (EAZ) as defined in your CAPI setup.

### Short hold mode

Select this to permit the use of short-hold mode. When no data is transferred between the Guest and Host, the line will be disconnected. When activity starts on either the Guest or the Host, the connection will be reestablished. On the Guest there will be an additional *time out* field next to the short hold mode check box. In this field you specify the number of seconds that can pass without activity before the line is taken down.



This setting must be enabled on both Guest and Host to take effect.

### Use of 2 B channels

Select this to permit the Guest to use both B channels. If two B channels are available this will increase the raw data speed from 64 kbit/s to 128 kbit/s.

This setting must be enabled on both Guest and Host to take effect.

### ISDN Number check

If enabled, only those Guests that have an ISDN number matching a number in this list will be able to access this Host.

*This setting is only available on the Host.*

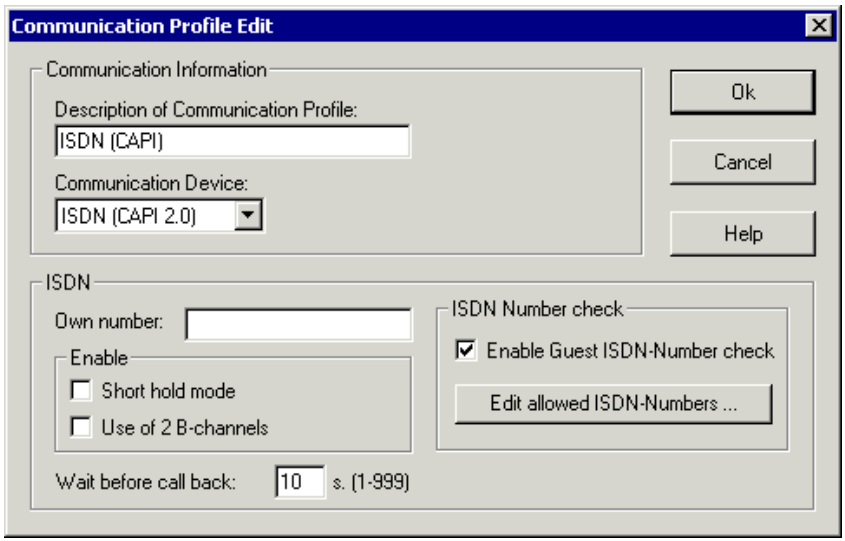
## 11.5.3 Device Specific Settings (CAPI 2.0)

The following figure displays the communication profile edit dialog using the ISDN (CAPI 2.0) specific settings:

In the *Own number* field you must specify as much of the number necessary to uniquely identify the number NetOp is listening on. If no other application using CAPI is listening, you don't have to specify anything unless you are using short hold mode.

If your number is 12345678 you can specify (nothing), 8, 78, 678, etc.

CAPI 2.0 is compatible with CAPI 1.1. This means that you can make connections between CAPI 1.1 and CAPI 2.0.




# 11.6 Outgoing Gateway

## 11.6.1 Description

A 'Gateway' Communication Profile is used if a user wishes to route a NetOp remote control call through an Outgoing Gateway. NetOp will route the call through the networking protocol chosen by the user to the Gateway where the call will be routed onwards through a dial-up protocol.

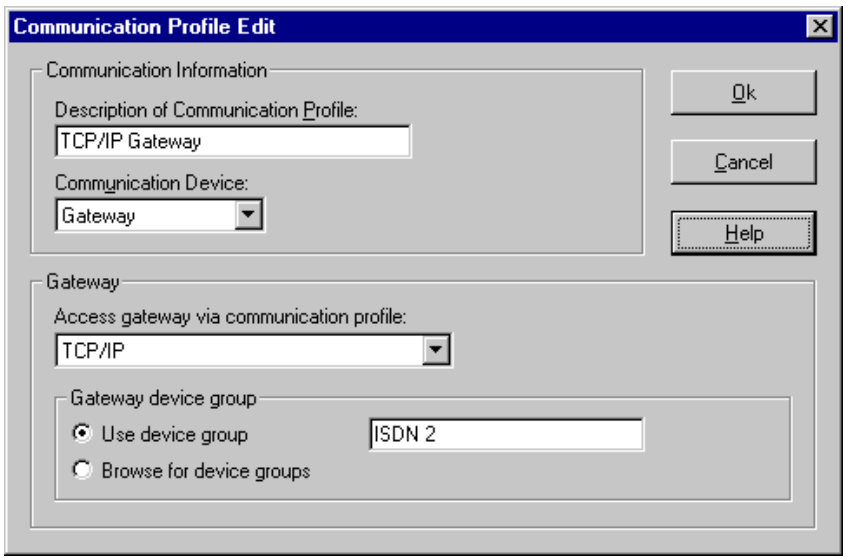
*Note: NetOp's Outgoing Gateway functionality is explained in more detail in chapter 10 'The Gateway'.*

## 11.6.2 Device Specific Settings

The following figure represents the device specific settings shown when editing a 'Gateway' communication profile:

### Access Gateway Via Communication Profile.

In this field specify the networking communication profile used to reach the Outgoing Gateway. You may choose from IPX, NetBIOS, TCP/IP or <any initialized protocol >.




### Gateway Device Group

Use this setting to choose whether NetOp should browse for available device groups on a network, or whether a particular device group should be used. For more information regarding device groups please refer to section 10.6.2.

# 11.7 Using a modem

NetOp offers two ways to communicate via a modem

**Windows Modem** - This communication profile will be available only on 32-bit systems (Windows 2000/NT/98/95).

**Serial** - Available both on 32-bit and 16-bit systems (Windows 3.x).

On both 32 and 16 bit systems NetOp will lead the user through the configuration of the modem the first time it is started. By default NetOp will use Windows Modem on 32-bit systems and Serial on 16-bit systems.

The following sections offer an explanation of both communication profiles.

*Note: Windows Modem and Serial Communication Profiles can communicate with each other.*

# 11.8 Windows Modem

## 11.8.1 Description

The Windows Modem is used to communicate via a modem or another telephony device that has been properly set up in Windows. For the Windows Modem communication profile NetOp uses TAPI or the Telephony API, which is commonly used by programs to make data/fax/voice calls, including the Windows 2000/NT/95/98 applets HyperTerminal, Dial-up Networking, Phone Dialer, and other Win32® communications applications written for Windows 2000, NT, 95 and 98.

## 11.8.2 Startup

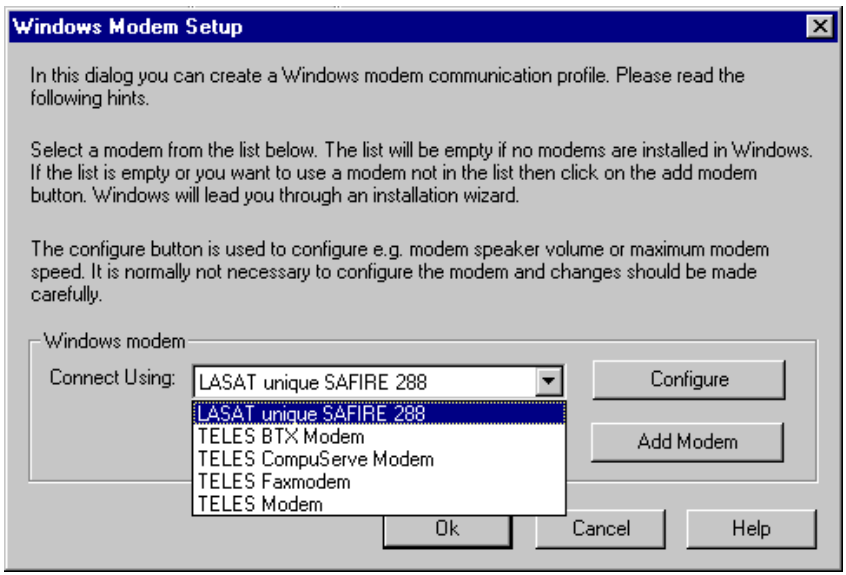
The first time a NetOp module is run a dialog will prompt the user to go through a modem setup. After selecting Yes, the dialog on the opposite page will appear:

### Connect using

The drop down list should contain all modems that have been setup in Windows. Choose one from the drop-down list. The Communication profile you have created will take the name of the modem you have chosen. If the list is empty no modems have been set up in Windows. Click on the *Add Modem* button to have Windows take you through the modem installation wizard.

### Configure

The configure button is used to configure settings such as modem speaker volume, maximum baud rate, etc.



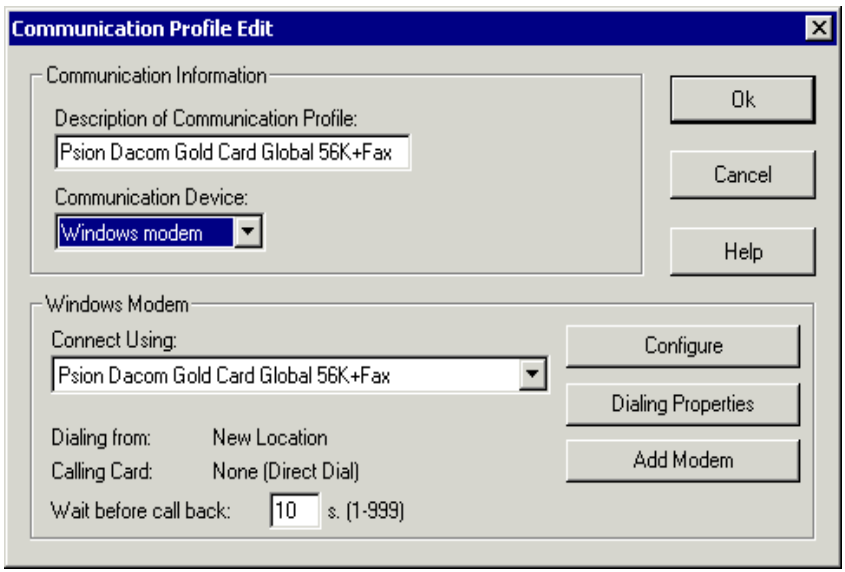

These settings should normally not be changed, and all changes should be made carefully, for more information regarding Windows Modem setup please refer to your operating system documentation and on-line help system.

After you have clicked OK from the Windows Modem Setup dialog box, a communication profile will be created bearing the name of the modem device you have chosen (e.g. Lasat Unique SAFIRE 288).

## 11.8.3 Editing a Windows Modem Communication Profile

To edit an existing Windows Modem communication profile or to create a new Windows Modem communication profile choose the *Configuration* menu, *Communication Profiles* from the main Guest Control Panel. From the resulting dialog you may *Edit* an existing profile or create a *New* profile.

The following dialog will then appear:




As in the initial Windows Modem Setup screen you may choose a device from the *Connect Using* drop down list or choose to configure the particular modem or view it's dialing properties. To add a new modem click on the *Add Modem* button.

It is possible to create multiple *Windows Modem* communication profiles each containing a different device that has been set up in Windows.

### Wait before call back

Specify the number of seconds to wait before calling back if call back is selected

*Note: If you experience trouble using a particular modem make sure that it has been properly setup in Windows, and all drivers have been installed. A good test of this is to try and use the particular modem with either the Phone Dialer, HyperTerminal, or one of the other dial-up networking applets available in windows.*

# 11.9 Serial

## 11.9.1 Description

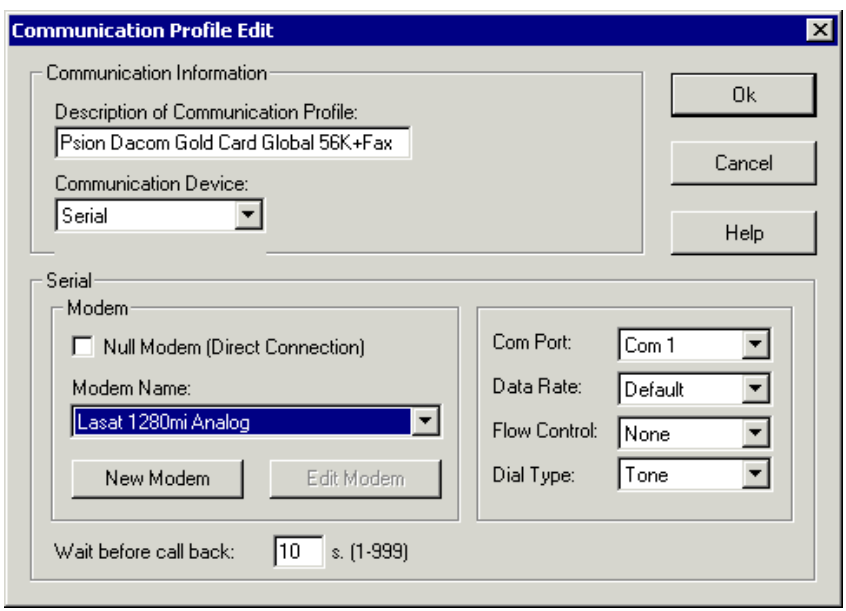
The Serial communication profile is available for users of 16-bit (Windows 3.x) and 32-bit (Windows 2000/NT/95/98) operating systems. However users of Windows 2000, NT, 95 and Windows 98 should normally use the Windows Modem communication profile for modem communication, and use the Serial Communication Profile if problems are experienced using Windows Modem or if the particular device being used does not support TAPI.

Use the serial device to communicate using the RS-232C interface – typically with a modem over telephone lines or with a null-modem cable.

NetOp accesses the COM port through the driver specified by the COMM.DRV key in the [boot] - section of the SYSTEM.INI file (typically COMM.DRV).

## 11.9.2 Device Specific Settings

The following shows the communication profile edit dialog with serial as the communication device:



### Modem

Check *Null Modem* if the Guest and Host are directly connected with a cable.

Choose a modem from the *Modem name* list. If your modem is not in the list choose *Hayes compatible* (2400 bps or slower) or *Hayes compatible fast* (9600 or faster), or click *New Modem* to add a new modem definition (see section 11.9.3 , 'The Modem Database').

### COM Port

Specify which COM port your modem is connected to (COM1-COM9).

### Data Rate

Should normally be *Default,* which means that NetOp will use the speed defined for the chosen modem in the modem database.

If connection is often lost, try lowering the data rate.

### Flow Control

Specifies whether NetOp should use hardware flow control (RTS/CTS). Normally *Flow Control* should be set to *Default*. Doing this results in NetOp reading the flow control setting from the modem definition.

### Dial Type

Choose *Tone* if this is supported by the phone system. Otherwise choose *Pulse*.

### Wait before call back

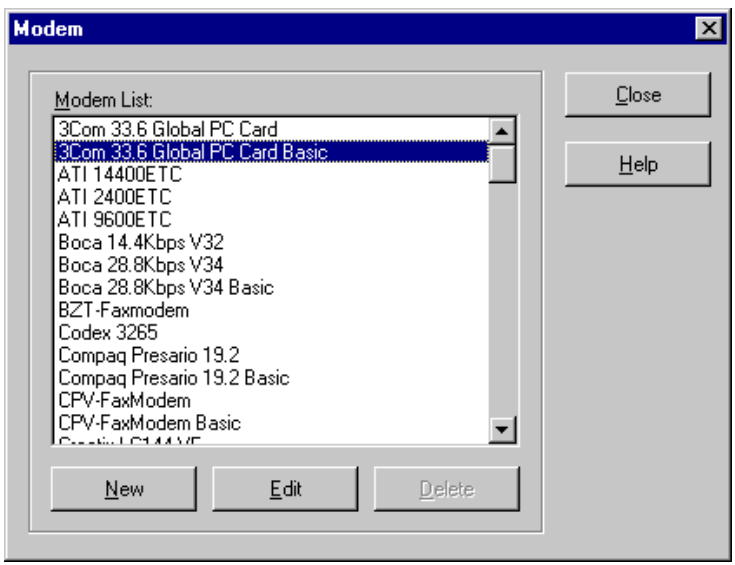
Specify the number of seconds to wait before calling back if call back is selected

## 11.9.3 The Modem Database

When communicating with a Host via a serial communication profile you typically need to take the specific brand and type of modem into consideration.

NetOp handles this by supplying an open modem database. The database initially contains a number of modems defined by Danware but can be supplemented with your own definitions.

To access NetOp's modem database choose *Modem database* from the *Configuration* menu, this activates the dialog box shown in the following figure:




The list shows you the existing records in the database, they are always sorted alphabetically.

### Searching

You can search for a record by pressing a key. For example pressing A will move you to the first record starting with the letter 'A' (or 'a').

### Inserting

If you activate the *New* button (or press ALT+N), you will add a new record to the database. Its contents will be similar to the selected record's (except for the name which will be blank), you will be presented with the edit entry dialog (see the following figure).

### Deleting

You delete records by clicking the *Delete* button (or by pressing ALT+D on your keyboard.

### Editing

If you activate the *Edit* button (or press ALT+E) you will edit the selected record. A new dialog box will appear (see the following figure).

For some modems the string *Fixed* will be displayed in the lower right corner of the edit dialog. This means that the current modem strings have been defined by Danware and cannot be changed. To alter the settings for a fixed modem string, make a copy of the modem definition and make the desired changes to the copy:

1. Select the modem which is to be changed from the modem list.

2. Activate the *New* button.

3. Enter a name for the copy of the modem definition.

This modem definition will not be fixed and any desired changes can be made to it.

## 11.9.4 How to Define New Modems

The most important part of defining a modem for NetOp is the setup strings (SETUP1 and SETUP2). NetOp does not distinguish between these two strings. You can just consider them as two lines for your setup string.

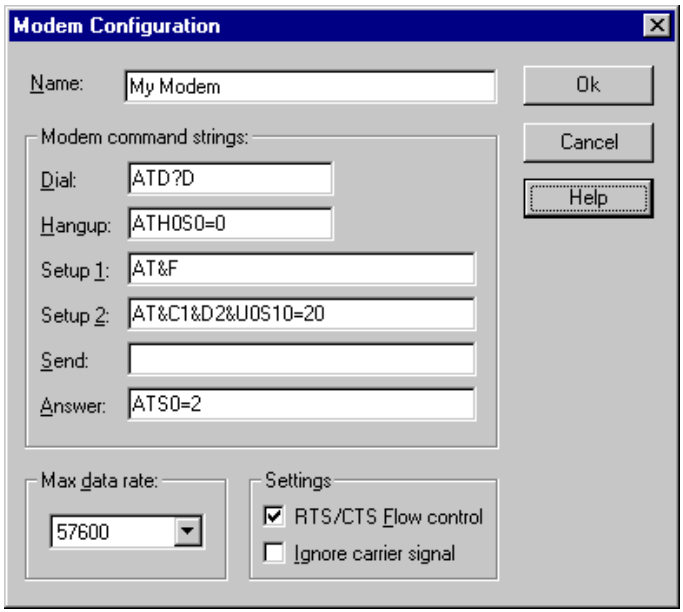
You should use the following general approach when constructing the setup string:

1. Load the modem's factory settings (usually AT&F).

2. Specify that if the DTR signal is lowered the modem should disconnect and return to command mode (usually AT&D2 ).

3. Specify that the CD signal should track the state of the carrier (usually AT&C1).

4. Specify that the modem should use local echo (usually ATE1).




5. If the modem is capable of RTS/CTS flow control, this should be enabled using the appropriate AT command. Also enable RTS/CTS flow control in the settings section of the modem dialog box.

6. Specify that the DTE/DCE rate should be fixed at the DTE speed.

7. If your modem is equipped with error correction and/or data compression, these should be enabled.

8. Instruct the modem to hangup after loss of carrier (usually by setting the modem's S10 register. E.g. ATS10=20, causing the modem to hangup if carrier is lost for a duration of 2 seconds).

The Dial string should usually be ATD?D. This instructs NetOp to use ATDT if tone dial is chosen by the user and ATDP if pulse dial is chosen.

The Hangup string is usually ATH0S0=0. H0 tells the modem to go on hook, S0=0 tells the modem not to answer incoming calls.

The Send field is sent to the modem after setup1 and setup2 but only by the Guest. Usually this field should be left empty.

The answer field should usually contain the string ATS0=<number of rings>, e.g. ATS0=1, this instructs the modem to answer incoming calls after <number of rings> rings.

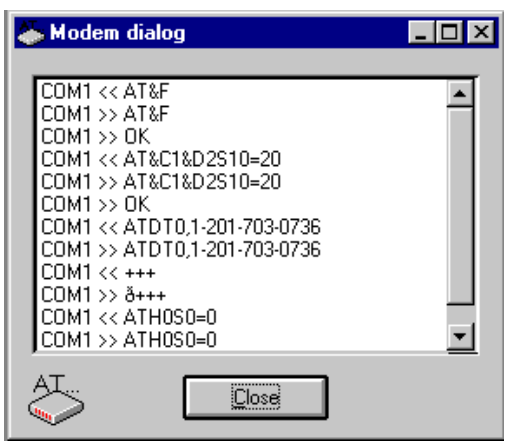
Set *Max Data Rate* to the maximum DTE supported by your modem. Please note that you should be careful with high baud rates on slow computers. You might get better performance by setting the baud rate to 19200 rather than 57600 on a slow PC.

Enable *RTS/CTS flow control* if this is supported by your modem. You might need to enable the RTS/CTS flow control in your modem with AT command, which should be included in SETUP1 or SETUP2.

Please note that you can override the data rate and flow control defined for the modem in device specific settings for serial.

## 11.9.5 The modem dialog

NetOp contains a facility, which lets you monitor all commands sent from the Guest to the modem(s) and the modem's responses. An example of the modem dialog is displayed in the following figure:



Each line has the form

COM*x* << *command*

indicating that *command* was sent to the serial port COM*x* (where *x* is a number between 1 and 9), or:

COM*x* >> *response*

indicating that *response* was received from the serial port COM*x*.

Please note that most responses are duplicates of the preceding command, this is because NetOp requires the modem to have local echo enabled, making the modem echo every command back to the PC.

## 11.10 TCP/IP (TCP)

### 11.10.1 Description

The main purpose for introducing this device is to let you comminicate via TCP ports, to contact a gateway via the Internet and browse for hosts behind the gateway, revealing those machines which are not directly on the Internet.

The Internet Protocol (IP) is the most commonly used network protocol, both on the Internet and also on intranets. On top of IP, programs can use TCP, which is a point-to-point protocol with secure packet transfers and UDP, which is an insecure network protocol. NetOp implements two communication devices on top of IP: TCP/IP (UDP) and TCP/IP (TCP). This is about TCP/IP (TCP). You will need to use this device to connect via a TCP port. By default there is no profile based on TCP.

To create a communication profile using the TCP/IP (TCP) device, click Configuration, Communication Profiles and New. Then select device type TCP/IP (TCP) and give your new profile a name, for example TCP. The configuration of TCP/IP (TCP) is the same as for TCP/IP (UDP), except that this profile only uses the fixed receive port number when listening. It always calls on an arbitrary port number. This means that you cannot set the receive port number to 0 in the user interface.

### 11.10.2 Device Specific Settings

The settings available for TCP/IP (TCP) are a subset of those for TCP/IP (UDP): The major difference is that you cannot browse, since TCP gives you a point-to-point connection exactly like a telephone conversation. Accordingly, there is no Edit broadcast list button. For all other settings, refer to TCP/IP (UDP).

#### TCP and the Gateway

Just like you can dial in to a gateway via phone or ISDN, you can also “dial in” via TCP. Follow these steps in your gateway

1: Create a TCP/IP (TCP) profile as described above and name it TCP

2: Assign the profile a device group name, for example TCP

3: Assign this new profile a correct NetOp Net number

4: Check this new profile in the main window

5: Check TCP/IP (UDP) or IPX with a net number as described in the Gateway Section

6: Press “Wait for call” and contact the gateway via a corresponding TCP profile on a guest

## 11.11 Infrared (IrDA)

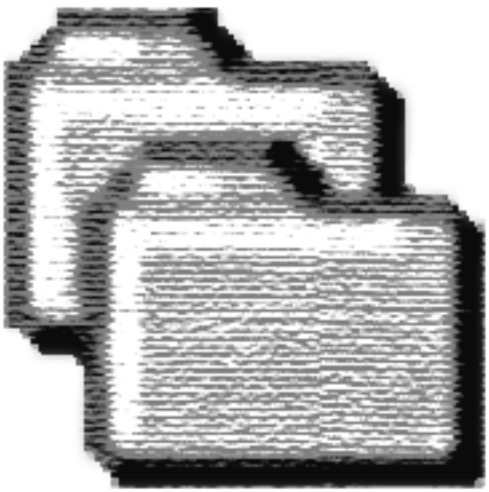
### 11.11.1 Description

Windows 98 and Windows 2000 support communication via infrared light, the method you are familiar with from your TV remote control. Infrared transmission is attractive because you need no cables, and you can get speeds up to 4 megabit per second today, at the release of NetOp 6.5. The limitation is that you can only communicate over a shorter distance.

### 11.11.2 Device Specific Settings

All settings of the infrared communication is done via Windows’ dialogs. Make sure Windows signals a working communication before trying with NetOp.

# Chapter 12
# Appendix



# 12.1 Tables

**Table 12-1 NetOp system requirements**

| | | |
|---|---|---|
| **Hardware** | **Computer** | IBM PS/PC with an Intel 80386 processor or higher or 100% compatible.<br>Recommended 16MB of available memory or higher for Guest.<br>Recommended 8MB of free memory or higher for Host. |
| | **Modem** | Null modem or modem with support for the AT command set. |
| | **ISDN** | Any ISDN adapter with support for the CAPI interface. |
| | **Video** | Any graphics adapter supported by Windows. |
| | **Disk Space** | Guest, Host, Log Server, Access Server and Gateway less than 4.5 MB each. |
| **Software** | **Windows** | Windows 3.1x, Windows 95, Windows 98, Windows NT 3.51 / 4.0 (Intel) or Windows 2000. |
| | **TCP/IP** | Must be WinSock 1.1 compatible. |
| | **NetBIOS** | IBM, Microsoft, Novell or compatible. |
| | **IPX** | Netware Windows Client or compatible. |
| | **ISDN** | CAPI 2.0: CAPI20.DLL or CAPI2032.DLL must be available.<br>CAPI 1.1: CAPI.DLL must be available. |
| | **Infrared** | Windows 2000 or 98 with IrDA enabled |

**Table 12-2.1 Events to log from Guest**

| Type | Description |
|---|---|
| CALL HOST | Call host |
| HANGUP HO | Hangup host |
| START HELP | Help provider start |
| STOP HELP | Help provider stop |
| DEF HELP N | Help provider name defined |
| DEL HELP N | Help provider name deleted |
| HELP RECV | Help request received |
| HELP CANC | Help request cancelled |
| FILE RECV | File received |
| FILE SENT | File sent |
| RESTART | Host Restarted |
| CONN LOST | Connection lost |
| PW REJECT | Password rejected |
| CA REJECT | Confirm access denied |
| SES_REC_STARTED | Session recording started |
| SES_REC_STOPPED | Session recording stopped |
| AC_LOGIN | Access Server login |
| AC_LOGOFF | Access Server logoff |

**Table 12-2.2 Events to log from Host**

| Type | Description |
|---|---|
| START HOST | Host started |
| STOP HOST | Host stopped |
| START REMO | Start of remote control |
| STOP REMO | Stop of remote control |
| START CB | Call back |
| HOST HELP | Help request sent |
| HO HELP CA | Help request cancelled |
| IND ON | Individual security enabled |
| IND OFF | Individual security disabled |
| GR DEFINED | Security group added |
| GR REMOVED | Security group deleted |
| GR CHANGED | Security group changed |
| GU DEFINED | Guest group added |
| GU REMOVED | Guest group deleted |
| GU CHANGED | Guest group changed |

**Table 12-2.2 Events to log from Host (Continued)**

| Type | Description |
|---|---|
| PW DEFINED | Password enabled |
| PW REMOVED | Password disabled |
| PW CHANGED | Password changed |
| CALLBA ON | Call-back enabled |
| CALLBA OFF | Call-back disabled |
| CALLBA CHG | Call-back changed |
| CONF AC ON | Confirm access enabled |
| CONF AC OF | Confirm access disabled |
| FILE RECV | File received |
| FILE SENT | File sent |
| BOOT | Host booted |
| CONN LOST | Connection lost |
| PW REJECT | Password rejected |
| CA REJECT | Confirm access denied |

**Table 12-3 NetOp File Manager HotKeys**

| Hotkey | Description |
|---|---|
| F5 | Copy File(s) |
| F6 | Move File(s) |
| F7 | New Folder |
| F8 | Delete |
| F10 | Close |
| SHIFT+F1 | Properties |
| + | Select By |
| - | Deselect By |
| * | Invert Selection |
| CTRL+R | Refresh |
| ALT+F1 | Switch to the right window pane |
| ALT+F2 | Switch to the left window pane |

**Table 12-4.1 NetOp Scripting Global settings**

| Command | Description |
|---|---|
| Script | Start a script |
| scriptend | End the current script |
| set AtEnd=restart | Restart script when finished |
| set Copy=G_H | Transfer from Guest to Host |
| set Copy=H_G | Transfer from Host to Guest |
| set Delta=no | Do not use Delta file transfer |
| set Delta=yes | Use Delta file transfer |
| set KeepPartial=no | Do not keep partialy transferred files |
| set KeepPartial=yes | Keep partialy transferred files |
| set OverwriteExisting=no | Do not overwrite/delete existing files |
| set OverwriteExisting=yes | Overwrite/delete existing files |
| set OverwriteHidden=no | Do not overwrite/delete hidden files |
| set OverwriteHidden=yes | Overwrite/delete hidden files |

**Table 12-4.1 NetOp Scripting Global settings (Continued)**

| Command | Description |
|---|---|
| set OverwriteReadOnly=no | Do not overwrite/delete read-only files |
| set OverwriteReadOnly=yes | Overwrite/delete read-only files |
| set OverwriteSystem=no | Do not overwrite/delete system files |
| set OverwriteSystem=yes | Overwrite/delete system files |
| set OnComError=exit | End script on a communication error |
| set OnComError=NextHost | Call next Host in script on communications error. |
| set OnComError=*n* | Retry Host *n* times on a communication error (where *n* is a number from 1-9) |
| set OnError=Exit | End script on transfer error |
| set OnError=NextHost | Call next Host in script on transfer error |
| set OnError=NextFile | Go to next file in script on transfer error |
| set OnError=*n* | Retry Host *n* times on a transfer error (where *n* is a number from 1-9) |

**Table 12-4.2 NetOp Scripting Commands**

| Command | Description |
|---|---|
| call c:\netop\phbook\host1.dwc | Call the Host represented by the c:\netop\phbook\host1.ncf *:DWC entry |
| set Copy=G_H | Transfer from Guest to Host |
| set Copy=H_G | Transfer from Host to Guest |
| clone "Source" "Target" | Clone a source and target directory. |

**Table 12-4.2 NetOp Scripting Commands (Continued)**

| Command | Description |
|---|---|
| clone "Source" "Target" /s | Clones directories and sub-directories except empty ones. |
| clone "Source" "Target"[/ *X* | Clone where X equals an overiding Global Setting (without the SET command). |
| copy "Source" "Target" | Copy "source" to "target". |
| copy "Source" "Target" /d=YYYY-MM-DD | Copy files newer than the specified date (Written as Year-Month-Day). |
| copy "Source" "Target" /s | Do not copy empty directories. |
| copy "Source" "Target" /h | Copy both hidden and system files. |
| copy "Source" "Target" /u | Copy only files that already exist in the target directory. |
| copy "Source" "Target" /*X* | Copy where X equals an overiding Global Setting (without the SET command). |
| run "C:\Prog\ProgName.bat" | Run the program "C:\Prog\ProgName.bat". |
| run "C:\Prog\ProgName.bat" /Guest | Run the program "C:\Prog\ProgName.bat" on the Guest. |
| run "C:\Prog\ProgName.bat" /timeout=60 | Run the program "C:\Prog\ProgName.bat" , with a delay of 60 seconds.<br>0=No Delay<br>1000=Wait for application to end |
| sync "Source" "Target" | Synchronize the "source" and "target" directories. |
| sync "Source" "Target" /d=YYYY-MM-DD | Synchronize files newer than the specified date (Written as Year-Month-Day). |
| sync "Source" "Target" /s | Do not synchronize empty directories. |
| sync "Source" "Target" /h | Synchronize both hidden and system files. |
| sync "Source" "Target" /u | Synchronize only files that already exist in the target directory. |
| sync "Source" "Target" /oneway | Transfer files one way. |
| sync "Source" "Target" /*X* | Sync where X equals an overiding Global Setting (without the SET command). |
| wait HH:MM:SS YYYY-MM-DD | Wait untill Hours:Minutes:Seconds in Year-Month-Day before going on to the next operation in script. |
| wait HH:MM:SS /delay | Wait for Hours:Minutes:Seconds before going on to next operation in script. |

**Table 12-4.3 NetOp Scripting Syntax Errors**

| Error | Description |
|---|---|
| 101 | Unterminated string "STRING |
| 102 | Over 512 Characters long |
| 103 | Invalid Character |
| 201 | an invalid boolean parameter value<br>(e.g. set Overwritehidden=YES) |
| 202 | a line without a command<br>(e.g. source=12 target=20) |
| 203 | too many commands defined |
| 204 | unknown command |
| 205 | an invalid enumeration parameter value |
| 206 | an integer parameter value is out of range |
| 207 | too many parameters |
| 208 | unknown parameter name<br>set junkfood=12<br>sync a b /wipe |
| 209 | syntax error |
| 300 | a "set" command occurs before a "script" command |
| 301 | the script ended whithout a "ScriptEnd" command |
| 302 | a transfer command occurs before a "Call" command |
| 303 | a "Call" command occurs before previous call was ended |

**Table 12-4.4 NetOp Scripting - Log Errors**

| Error Number | Description |
|---|---|
| 1 | Syntax Error. |
| 2 | Invalid command at this time (Actions are not placed in a valid order). |
| 5 | Operation cancelled by user. |
| 10 | Log file open, (could not write to the Log File). |
| 12 | The Host does not allow you transfer files from it. |
| 13 | The Host does not allow you to transfer files to it. |
| 33 | Path does not exist. |
| 34 | File does not exist. |
| 35 | File already exists. |
| 36 | File is marked as "Read Only". |
| 37 | File is marked as "Hidden". |
| 38 | File is marked as "System". |
| 39 | A newer file exists. |
| 40,41 | Could not read the specified file. |
| 42 | Skip File. |
| 43 | The file is locked by another application. |

*Note: If the error you receive does not appear in the table below, it is an internal Windows error or an application error.*

**Table 12-4.5 NetOp Scripting - Log Actions**

| Action | Description |
|---|---|
| FILE ROPEN | READ operation performed on file. |
| FILE WOPEN | WRITE operation performed on file. |
| FILERCLOSE | READ operation completed. |
| FILEWCLOSE | WRITE operation completed. |
| FILE DEL | File deleted. |
| DIR DEL | Directory deleted. |
| LOG OPEN | Log file opened. |
| LOG CLOSE | Log file closed |
| ERROR | Error during transfer. |
| CALL | Particular Host called. |
| CALLEND | Disconnected from Host. |

## 12.2 Silent Install and NetOp Deployment

To use the silent install feature use the -s switch with the SETUP.EXE program (i.e.. Type **setup -s**). A source file called SETUP.ISS will have to be created, before running the setup program and a log file will be generated after the installation called INSTALL.LOG.

Below is a sample SETUP.ISS file that uses the same format as Windows INI files with sections, keys and values. The value options are 1=enable 0=disable.

The first three sections should not be changed. These are defined by Danware for use with the install program.

```
[InstallSHIELD Silent]
Version=5.10.000
File=Response File

[Application]
Name=NetOp Remote Control
Version=6.50.00
Company=Danware Data A/S

[DlgOrder]
Count=0

[INSTALL]
;Install Host files
HOSTFILES=1
;Install Guest files
GUESTFILES=1
;Update previous installation if one is found
UPDATE_INST=1
;Uninstall previous installation if one is found
UNINSTALL_INST=1
;Destination directory for NetOp files, default is most recent directory
DIRECTORY=C:\NETOP
```

```
;Licensed to
LICENSEDTO=Your Name
;Serial number for the Guest
GUESTSERIALNR=Your license
;Serial number for the Host
HOSTSERIALNR=Your license
;Windows folder for program items, default is the most recent folder
FOLDER=NetOp Remote Control
;Configure the Host with options found in the HOST section
CONFIGURE_HOST=1
;Reboot the machine after the installation has completed, default is automatic
BOOT=2

[HOST]
;Display notification msg. after connection: 0:No, 1:Yes
AFTER_CON_DISP_MSG=0
;Enable msg. password after connection: 0:No, 1:Yes
AFTER_CON_MSG_PW_ENABLE=0
;Let the user configure the modem at first program start: 0:No, 1:Yes
ASK_FOR_MODEM=1
;Authentication MAC/IP address (optional)
AUTHENTCATION_ADDR=Your Access Server's IP address (or MAC)
;Authentication key (required if you want to use an Access Server)
AUTHENTCATION_KEY=Your Access Server Key
;Name of communication profile to activate at starup
COMPROF=A profile name
```

;Call back number for default access privileges

DEF_CALL_BACK_NUMBER=A telephone number

;Confirm access for default access privileges: 0:Never, 1:Always, 2: Only when logged in

DEF_CONFIRM_ACCESS=0

;Password for default access privileges. An empty string or no line means no password

DEF_PASSWORD=A password

;Display guest name in title bar: 0:No, 1:Yes

DURING_CON_DISP_GUEST_NAME=1

;Interval for playing sound during connection. Accepted values: 10 through 60 seconds

DURING_CON_PLAY_INT=0

;Play sound during connection: 0:No, 1:Yes

DURING_CON_PLAY_SOUND=0

;Enable full duplex for audio chat: 0:No, 1:Yes

ENABLE_FULL_DUPLEX=1

;Environment variable name to be used for Host name

ENVIRONMENT_VAR=An environment variable, for example USERNAME

;Show file transfer status: 0:No, 1:Yes

FILE_TRANSFER_STATUS=0

;Guest Access Method:

0:Grant all Guests default access privileges

1:Grant each Guest individual access privileges using NetOp authentication

2:Grant each Guest individual access privileges using Windows authentication

3:Use NetOp Access Server on Guest side

4:Use NetOp Access Server on Host side

GUEST_ACCESS_METHOD=0

;Help request communication profile

HR_COMPROF=A profile name

```
;Help provider
HR_HELP_PROVIDER=A help provider name
;Add help request icon to the tray: 0:No, 1:Yes
HR_ICON_TO_TRAY=0
;Help request phone number
HR_PHONE_NUMBER=A phone number
;Help request problem description.
HR_PROBLEM_DESCR=A string of your choice.
;Help request timeout. Accepted values 0 thrught 60. 0 means wait forever
HR_TIMEOUT=0
;Communication profile to use with help request: 0:Use current, 1:Use specific
HR_USE_WHAT_COMPROF=0
;Action taken when number of passwords is exceeded: 0:Hangup, 1:Disable, 2:Boot
ILLEGAL_PASSWORD_ACTION=0
;Load program with Windows: 0:No, 1:Yes
LOAD_WITH_WINDOWS=0
;Log off after hangup: 0:No, 1:Yes
LOG_OFF_AFTER_HANGUP=0
;MAC/IP address check: 0:No, 1:Yes
MAC_ADDR_CHECK=0
;Maintenance password
MAINT_PASSWORD=A password
;Maximum number of invalid passwords: Accepted values 0(=unlimited) trhough 100.
MAX_ILLEGAL_PASSWORDS=3
;Minimize user interface at program startup: 0:No, 1:Yes
MIN_AT_STARTUP=0
```

;Minimize user interface on connection: 0:No, 1:Yes

MIN_ON_CONNECTION=0

;PC Name/Host ID

NAME=A name

;Naming method: 1:Enter, 2:Environment variable, 4:Computer name

NAMING=4

;Message password after connection

ON_AFTER_MSG_PASSWORD=A password

;Display notification message on connection: 0:No, 1:Yes

ON_CON_DISP_MSG=0

;Message password upon connection

ON_CON_MSG_PASSWORD=A password

;Enable “message on connection” password : 0:No, 1:Yes

ON_CON_MSG_PW_ENABLE=0

;Play a sound on connection: 0:No, 1:Yes

ON_CON_PLAY_SOUND=0

;Protect security configaration files

1:No

2:When connected

3:When connected and waiting for call

PCT_FILES=0

;Protect guest access privileges with maintenance password: 0:No, 1:Yes

PCT_GUEST_ACCESS=0

;Protect other configuration with maintenance password: 0:No, 1:Yes

PCT_OTHER_CONF=0

;Protect program exit with maintenance password: 0:No, 1:Yes

PCT_PROGRAM_EXIT=0

;Prefix computer name with work group name: 0:No, 1:Yes

PREFIX_WITH_WORKGROUP=0

;Public host name: 0:No, 1:Yes

PUBLIC_HOST_NAME=1

;Restart after hangup: 0:No, 1:Yes

RESTART_AFTER_HANGUP=0

;Send keep alive messages: 0:No, 1:Yes

SEND_KEEP_ALIVE=0

;Silence level for audio chat: Accepted values 0 trhough 60

SILENCE_LEVEL=58

:;Line hold for audio chat: Accepted values 0 through 20

SOUND_HOLD=17

;Stealth mode, invisible host: 0:No, 1:Yes

STEALTH_MODE=0

;User interface is top most window: 0:No, 1:Yes

TOP_MOST_WINDOW=0

;Wait for call at program startup: 0:No, 1:Yes

WAIT_FOR_CALL=0

;Computername separator used with PREFIX_WITH_WORKGROUP

WINDOWS_NAME_SEP=\

The values listed are the default values for a new, fresh installation. If you are updating, existing values are kept, if the corresponding line is omitted. You can place comments in the file by writing a semicolon in column 1. You can also configure silent install to copy files after the installation is completed.

Files that should be copied is specified in the section [COPY_FILES]. COPY_COUNT specifies the number of files to be copied. COPY1 is the first file, COPY2 is the second file, etc. You cannot specify a path with this parameter, only the filename you may also choose to use the DOS “wildcard format”. Files are copied from the silent install directory to the installation target directory or any directory if specified. You can use wild cards in this parameter to copy groups of files.

Example:

[COPY_FILES]

COPY_COUNT=2

COPY1=i:\install\netop\comprof.ndb c:\netop

COPY2=i:\install\netop*.dat c:\netop

The following option is available for use with the NetOp installation program, setup.exe. This private option must appear before any other options.

**-L<Path>** To control where the INSTALL.LOG file is placed use -LPath as an argument to SETUP.EXE. -LPath will create INSTALL.LOG in the Path directory.

The following options are also available for use with the NetOp installation program, setup.exe. These options are general InstallShield options

**-s**

The -s option causes setup.exe to run a silent installation.

**-SMS**

The SMS switch prevents a network connection and the SETUP.EXE from closing before the installation is complete. This switch works with installations originating from a Windows NT server over a network. Please note that SMS must be uppercase; this is a case-sensitive switch.

**-f<path\CompiledScript>**

The alternate compiled script can be specified using his option. Unless the compiled script (or *.INS file) also resides in the same directory as that of SETUP.EXE, the full path to the compiled script must be specified. _SETUP.DLL must also reside in the same directory as your .INS file. For example, setup -ftest.ins will launch SETUP using TEST.INS instead of SETUP.INS.

**-f1<path\ResponseFile>**

The alternate location and name of the response file (.ISS file) can be specified using this option. If this option is used when running InstallSHIELD Silent, the response file is read from the directory/file specified by<path\ResponseFile>. If an alternate compiled script is specified using the -f switch, the -f1 switch entry must follow the -f switch entry.

**-f2<path\LogFile>**

The alternate location and name of the log file created by InstallSHIELD Silent can be specified by using this option. By default, SETUP.LOG log file is created and stored in the same directory as that of SETUP.EXE. If an alternate compiled script is specified using the -f switch, the -f2 switch entry must follow the -f switch entry.

## 12.2.1 Using Silent Install from Netware Login Scripts

To distribute NetOp Hosts to Windows PC's from a Netware login script, the following tasks must be completed:

Copy the NetOp Remote Control install files to SYS:PUBLIC\INSTALL\NETOP

Create a SETUP.ISS file in SYS:PUBLIC\INSTALL\NETOP

Create NOWSETUP.BAT in SYS:PUBLIC\INSTALL\NETOP (see below)

Create a Netware group called NETOP_HOSTS

Edit the Netware login script (see below)

Add members to the Netware group NETOP_HOSTS. The used paths and locations can be changed accordingly.

### NETWARE LOGIN SCRIPT

```
IF MEMBER OF "NETOP_HOSTS" THEN BEGIN
        SET HOSTNAME ="%LOGIN_NAME"
```

```
        MAP ROOT I:=SYS:PUBLIC\INSTALL\NETOP
        EXIT "NOWSETUP"
END
```

**NOWSETUP.BAT**

```
@ECHO OFF
IF EXIST "C:\NETOP\COMPROF.NDB" GOTO INSTALLED
CLS
ECHO The NetOp Host will be installed on your PC.
ECHO When finished your PC will restart.
ECHO Press Ctrl+C to terminate.
PAUSE
CLS
I:\SETUP.EXE -SMS -S
:INSTALLED
MAP DEL I:
EXIT
```

## 12.2.2 NetOp Deployment Utility

From a computer running Windows NT or Windows 2000, the NetOp Deployment Utility (NDU) allows you to configure and install NetOp programs on a selection of remote computers.

NDU can install onto networked Windows 2000 and NT PCs that does not already have NetOp modules installed. Furthermore, NDU can install onto PCs running Windows 2000, NT, 98 and 95 if a version 6 Host is running.

NDU is installed as a separate program, but licensed with the NetOp Guest, which must be installed on the PC where you will deploy from. NDU will automatically start the Guest before initiating deployment.

NDU starts a silent installation on each remote computer. Silent install runs in batch without prompting for mouse or keyboard input. This means that there need not be anybody present at the remote computers. Using the NT remote service, nobody even needs to be logged in to the computer.

Silent install does not mean invisible install. If you wish an invisible installation, check the box in the options dialog.

### 12.2.3 Two Deployment Methods

NDU has two different deployment methods: “NT remote service” and “NetOp Scripting”. The two methods reflect two technically very different possibilities.

The NT remote service method works between networked Win 2000 / NT computers. This method uses the fact that 2000/NT users who have administrator rights on a remote 2000/NT computer can start a service there. So in this situation, just select the computers to install on and press the install button. No NetOp products need to be installed in advance on the remote computers.

The NetOp scripting method uses NetOp technology for communicating between computers. This allows you to reach any computer you can connect to with NetOp scripting, enabling you to reach Windows 2000, NT, 98 and 95 PCs. You can also reach computers, which are not in your network. This method requires that a NetOp 6.x host is running on the target computer.

### 12.2.4 Deploying the Different NetOp Modules

NDU is primarily designed to install a NetOp Host program. The settings in the options dialog reflect most of the options available in the NetOp Host. This dialog will warn you when it detects that your settings will result in a Host installation, which you cannot connect to afterwards.

You can also install NetOp Gateways, Log Servers and Access Servers. Since these programs are in fact “extended hosts”, you enter a license key for that product, and install it as if it were a standard Host. Then you remote control the deployed module and configure it manually.

It is also possible to deploy a NetOp Guest by checking the “install guest” checkbox and entering a valid guest license key. Guest program options cannot be set on the remote computer. This must be done locally on the Guest.

NetOp Deployment Utility will install NetOp 6.5 and later versions.

### 12.2.5 Installing the Deployment Utility

When installing, you can select between Install and Update. The first time you install NDU, you must push the Install button, which will install everything, that is needed for NDU to run, including a.o. Visual Basic runtime libraries and MS Data Access.

This button will unpack the full set of NDU installation files, and run the setup program. Here you may uncheck MS Data Access if you have that installed already.

If you reinstall or update NDU, you should push the Update button, because that is much faster. This button will unpack a minimal set of NDU installation files, and run the setup program, skipping the reinstall of all runtimes

The default for NDU is to have the program files in a directory separate from the rest of NetOp, while the default group named “NetOp Remote Control” is shared. We do not recommend that you install NDU in the same directory as the rest of NetOp.

## 12.3 The NETOP.INI File

NetOp utilizes a file called NETOP.INI. This file is normally located in the Windows directory. NETOP.INI contains specialized configuration information. Normally you do not need to edit the NETOP.INI file.

NETOP.INI uses the standard Windows .INI format with sections, keys and values. It is a plain text file, which can be edited with a standard text editor like Notepad or WordPad. The NETOP.INI file contain a.o. these sections:

**[GUEST]:** This section specifies options specific to the Guest.

**[HOST]:** This section specifies options specific to the Host.

**[ISDN]:** This section specifies options specific to the ISDN CAPI profile

**[DTL]**: Used for miscellaneous special troubleshooting settings

## 12.3.1 The Guest and Host Sections

If the NETOP.INI file exists and contains a Guest or a Host section the corresponding NetOp module will look for the entry DataPath=. If this entry exists NetOp will look for its datafiles (*.NDB) in the specified directory. If you experience problems transferring Host keyboard flags to the Guest create this entry on the Guest:

[GUEST]

SetKbdFlags=0

or this entry on the Host:

[HOST]

TransferKbdFlags=0

If the Host has an ATI graphics card and you need it to blank the screen you may have to add:

[HOST]

ATIScreenBlanking=yes

In some rare cases you may need to delay the load of the Host in order for a protocol to initialise prior to the Host:

[HOST]

StartComDelay=n ;where n is in milliseconds

If you experience problems on a PC having multiple CPUs you may solve the problem by instructing NetOp to only use one CPU:

[HOST]

OneCPU=1

If a Guest calls a Host which is already being controlled by another Guest the Host will normally report the MAC/IP address or the Guest ID of the Guest controlling it to the rejected Guest. The rejected Guest will in turn display the identity of the controlling Guest. For security reasons you can instruct the Host not to report the identity of the controlling Guest. This is done by

[HOST]

ReportGuestName=NO

## 12.3.2 The ISDN Section

If you run ISDN CAPI and need a dial prefix to get an outside line e.g. “0” you can specify this as follows:

[ISDN]

DialPrefix=0

## 12.3.3 The DTL section

This section of the NETOP.INI file is used for troubleshooting or performance tuning. If you are not experiencing any problems, please do not make any modifications within this section.An example is

[DTL]

TIMEOUTTIMES=*n*

where *n* is a value between 0-50. This key allows you to increase the number of timeout retries that occur before a connection is lost. NetOp will always use 10 time-outs before hanging up the connection. Use this key to add a number of time-outs to the default 10.

## 12.3.4 Example

A sample NETOP.INI file (with comments preceded by ;):

[GUEST]

;The Guest should look for data files in the directory

;F:\SHARED\NETOP\DATA\GUEST

DataPath=F:\SHARED\NETOP\DATA\GUEST

;The Guest should save the screen cache file in a different

;directory F:\SHARED\NETOP\GUEST\CACHE

CachePath=F:\SHARED\NETOP\GUEST\CACHE

;The Phonebook path is located in this directory

```
;F:\SHARED\NETOP\PBOOK
Phonebookpath=F:\SHARED\NETOP\PBOOK
;The History path is located in this directory
;F:\SHARED\NETOP\HIST
Historypath=F:\SHARED\NETOP\HIST
;The Recording path is located in this directory
;F:\SHARED\NETOP\REC
Recordpath=F:\SHARED\NETOP\REC
;The Script path is located in this directory
;F:\SHARED\NETOP\SCRPT
Scriptpath=F:\SHARED\NETOP\SCRPT
[HOST]
;The Host should look for data files in the directory
;F:\SHARED\NETOP\DATA\HOST
DataPath=F:\SHARED\NETOP\DATA\HOST
```

## 12.4 Scripting

### 12.4.1 The NetOp Script File

The following is an example of a NetOp Scripting File. It may be saved as an *.DWS or *.TXT file. For information regarding each command please refer to tables 12-4.1 and 12-4.2.

```
; This comment must be present at the beginning of the file and preceded by a ';'
;Start the Script
Script
;Restart the script when finished
set AtEnd=restart
```

```
;Transfer files from Guest to Host
set Copy=G_H
;Enable Delta File Transfer
set Delta=yes
; Keep partially copied files
set KeepPartial=yes
;Confirm when overwriting/deleting existing files or folders
set OverwriteExisting=yes
;Confirm when deleting hidden files
set OverwriteHidden=yes
;confirm when deleting read-only files
set OverwriteReadOnly=yes
;confirm when deleting system files
set OverwriteSystem=yes
;create a log file - C:\netop\script.log
set Log=c:\netop\script.log
;End the script on a communications error
set OnComError=exit
;Retry operation 2 times on a transfer error
set OnError=2
;Call the Host represented by the ”c:\netop\phbook\host1.DWC” *:DWC entry
call c:\netop\phbook\host1.dwc
;clone the c:\netop directory on both Guest and Host. Exclude empty directories, and do
not overwrite system files.
```

```
clone “c:\netop” “c:\netop” /s /OverwriteSystem=no
;end the current call
callend
;Call the Host represented by the ”c:\netop\phbook\host2.dwc” *:DWC entry
call c:\netop\phbook\host2.dwc
;wait until the date specified above
wait 17:12:05 1998-04-28
;copy the f:/backup directory into the g:\products directory, include hidden files, and skip to
the next file on a transfer error.
copy “f:\backup” “g:\products” /h /OnError=NextFile
;end the current call
callend
;Call the Host represented by the ”c:\netop\phbook\host3.dwc” *:DWC entry
call c:\netop\phbook\host3.dwc
;delay all script operations for 1 hour.
wait 01:00:00 /delay
;synchronize the g:\files and b:\files directory /copy only  files that already
;exist in destination.
sync “g:\files” “b:\files” /u
;run the program c:\winnt\backup.bat and do not wait for the program to ;end.
run “c:\winnt\backup.bat” /nowait
;end the current call
callend
;end the current script
scriptend
```

## 12.4.2 The NetOp Script Log

The log file contains the following sections (left to right).

**Date** - date of Action

**Time** - Time of action.

**Error** - Error if any (for more information regarding error numbers please refer to table 12-4.4).

**Extended Info** - Extended Windows or application error information.

**Action** - Type of action.

The following is an example of a Log file generated by the NetOp Scripting Utility:

; C:\NETOP\Netop.log opened on the date and time specified.

19981002,11:28, 0, 0,LOG OPEN ,C:\NETOP\Netop.log

;C:\NETOP\Netop.log specified as the log file.

19981002,11:28, 0, 0,SET ,Set Log=C:\NETOP\Netop.log

; Called the Host associated with the C:\NETO\NTserver.dwc entry.

19981002,11:28, 0, 0,CALL ,call C:\NETO\NTserver.dwc

; The file c:\autoexec.bat was copied to d:*.*

19981002,11:28, 0, 0,COPY ,copy c:\autoexec.bat d:*.*

; The READ operation performed on C:\AUTOEXEC.BAT has been competed.

19981002,11:28, 0, 0,FILERCLOSE,c:\AUTOEXEC.BAT

; The WRITE operation performed on D:\AUTOEXEC.BAT has been completed.

19981002,11:28, 0, 0,FILEWCLOSE,d:\AUTOEXEC.BAT

; The copy operation has been completed

19981002,11:28, 0, 0,COPY END ,copy c:\autoexec.bat d:*.*

; The call has been completed

19981002,11:28, 0, 0,CALLEND ,Callend

; Log file has been closed

19981002,11:28, 0, 0,LOG CLOSE ,

## 12.5 The NetOp Scripting ActiveX Control

NFMScrpt.ocx is installed in your Windows system32 directory when you install a NetOp Guest. It allows you to access the Guest's scripting capabilities from any programming or scripting tool which supports ActiveX automation. One commonly used tool is Microsoft Visual Basic (VB). The OCX is tested with VB, and examples in this section will be written mostly in VB. An example of a VBscript using a excerpt of the commands available is

```
Rc = Script.Initialize()
Rc = Script.Call("MyDesktop")
Rc = Script.IncludeSubdirectories(True)
Rc = Script.Synchronize("c:\MyDocuments\*.*", "c:\MyDocuments\*.*")
Rc = Script.Hangup()
Rc = Script.Uninitialize()
```

Scripts as simple as this are more easily created and executed with the Script editor in the NetOp guest program. Say however, you wish to retry all or parts of your operations repeatedly until they have all succeeded, you must make a more complex algorithm, which this editor is not designed for. With the NFMscrpt ocx you can improve the above script to for example:

```
Rc = Script.Initialize()
CallAgain:
    Rc = Script.Call("MyDesktop")
    Rc = Script.IncludeSubdirectories(True)
    RcSync = Script.Synchronize("c:\MyDocuments\*.*", "c:\MyDocuments\*.*")
    Rc = Script.Hangup()
    if (RcSync<>0) Then
        WriteLog ("Failed. Trying again in 30 seconds")
        WaitSeconds(30)
```

```
        GoTo CallAgain:
    End If
    Rc = Script.Uninitialize()
```

## 12.5.1 Creation and Deletion

An NFMscript object is created and eventually destroyed with the means of the programming tool. With VB, you can use the visual way by right clicking the object toolbar (the one on the left side), and choose Components. A dialog with all available OCXs appears. Check the box with "Danware NetOp File Manager Script", and press OK. A script icon will be added to your toolbar. Click this icon, then click the location in the Form where you wish the NFM script object placed, and drag it out. The default visual representation is a treeview showing commands as they execute, so even though the control initially shows up blank, it may be an idea to give it a reasonable size.

Assume you have named your NFMScript object - “Script”. Script.ClearLog() can be used to clear the treeview log window. If you do not wish any visual feedback, you can make the script invisible. You can also choose another reporting mode than ReportLog().

```
Set  Script.Visible = False
Rc = Script.ReportSilent()
Rc = Script.ReportStatus()
Rc = Script.ReportLog()
```

The OCX can handle any number of simultaneous NFMscript objects, but the NetOp Guest will limit you toa maximum of 10 active objects at a time. The 11th and all further objects can be created, but will always return error codes from all methods.

## 12.5.2 Startguest, Initialize and Uninitialize

The NFMscrpt.ocx is only another way of wrapping up the NetOp guest. Therefore, the NetOp Guest program has to be running when the ocx executes. The simplest way is to start it manually before starting the program or script you are writing using Nfmscrpt.ocx

You may however want to hide the NetOp guest program, and consider it an invisible service which is needed to run with your application. If you wish that you can call the StartGuest() function

In VB you would typically do that in the Form_Load() function for your initial form

```
Sub Form_Load()
Dim Rc As Long
Again:
Rc = Script.StartGuest(True)
if (Rc < -12 Or Rc > -11) Then
        MsgBox("Can't start NetOp Guest, please exit Host")
        GoTo Again
End If
End
```

If NetOp is installed and is working properly, the most likely reason for not being able to start the guest program is that the host is running. You must manually stop the Host. When the guest has started, you can send commands to it from any NFMscript object you have created. The first command any object should send is the Initialize command, which creates connection between the object and the Guest. This will typically happen as a reaction on the click of a button.

```
Sub  Button_Click()
Rc = Script.Initialize()
if (Rc <> 0) Then
        MsgBox("No connect. Is NetOp Guest Running?")
        GoTo EndButtonClick
End If
'< ... do your stuff ...>
Rc = Script.Uninitialize()
EndButtonClick:
End
```

One reason the Initialize might fail and return non zero, might be that the Guest program could not start. It is good practise to call Uninitialize() when you are returning from your subroutine. This way you will free the connection to the guest to be used for others. If you forget to Uninitialize(), it will be done implicit for you if you call Initialize() again, but you will be blocking 1 out of 10 connections to your guest in the meanwhile.

Uninitialize() returns 0 on success and a nonzero code on error. You need not take any specific action if an error is returned. When your application exits, it is good practice to call FreeGuest(), which will do all needed clean up. Your program will work OK without a call to FreeGuest(), but you will be relying on the program exit to clean everything up.

*Note: If you are writing a script for browser use (i.e. Internet Explorer), do not call FreeGuest(), as you are not the one to decide when Internet Explorer exits.*

```
Sub StopButton_Click()

Rc = Script.FreeGuest()

Stop

End
```

### Summary

StartGuest() may be called once at program start, no matter how many NFMscript objects you wish to create. FreeGuest should be called on exit, and never in browser scripts. Initialize() must be called before any other command. The one exception is StartGuest().

After Uninitialize(), no other commands but FreeGuest() will succeed until the next Initialize(). You can have any number of Initialize() ... Uninitialize() sessions on the same object.

## 12.5.3 Call and Hangup

The next thing you have to do is to call a NetOp host program running on another computer. The Call() command will establish this connection for you. If it fails, it will return a nonzero error code. If it succeeds, it will return 0. The argument to Call() is a String which is the name of the NetOp phonebook (.DWC) file. In this file is stored the name of a computer and the parameters for how to connect to it. The phonebook files are the ones shown in the NetOp Guest programs Phonebook tab control. Say you have a phonebook file named "Venus.dwc":

```
Sub Button_Click()

Rc = Script.Initialize()
```

```
Rc = Script.Call("Venus")
if (Rc <> 0) Then
        MsgBox("Venus not responding")
        GoTo EndButtonClick
End If
'< ... do your stuff ...>
Rc = Script.Hangup()
Rc = Script.Uninitialize()
EndButtonClick:
End
```

It is good practise to call Hangup() before you make your next Call(). If you happen to make a new Call() before Hangup() on the first one, it will be hung up automatically. One good reason not to omit calling Hangup is to save money on your telephone bill. You can make as many Call()'s and Hangup()'s you might wish on the same object.

Please be aware that the argument to Call() is NOT the name of the computer you wish to call. It is the name of a phonebook file. As such files often reside in the NetOp phonebook directory, you need not specify a path if you have the file there. As the NetOp default for phonebook filename extension is ".DWC", you need neither pass that, so the three calls below do the same, but the two last are independent of where NetOp is installed.

```
Script.Call("C:\program files\netop remote control\phbook\venus.dwc")
Script.Call("venus.dwc")
Script.Call("venus")
Script.Call("*")
```

The fourth call does not know which phonebook file it wants to use. The "*" parameter will cause a file selection box to pop up, where the end user can select a *.DWC file in the phonebook directory.

### Traversing the Phonebook

If you wish a control which makes the phonebook files available as other than the independent popup file selection box made with Script.Call("*"), you can traverse the phonebook directory like for example below, where a combo box is used.

```
Sub Combo1_Dropdown()
Dim More As Boolean
        More = Script.PhonebookSetFirst()
        Do While (More)
            Combo1.Add(Script.PhonebookGetName())
            More = Script.PhonebookGetName()
        Loop
End Sub
Sub Combo1_Click()
        Script.Call(Combo1.Value)
        Script.Hangup()
    End Sub
```

If you wish to traverse only a subset of all your phonebook connections, place the ones you wish to expose in a subfolder named for example"offices", using the Phonebook tab control in the NetOp Guest program, then use:

```
Script.PhonebookSetSubfolderFirst("offices")
```

### Summary

Call() must be called to connect to a Host. After a successful Call() you can execute other commands. Do Call("*") to enable dynamic selection.

When done with the Host, call Hangup(). After a Hangup(), no commands which need host access will succeed.

You can have any number of Call() ... Hangup() connections on the same object.

## 12.5.4 Transferring Files

After a Call() and before a Hangup(), you can call the file transfer commands which are:

```
Script.CopyFromHost   (RemoteFileFilter, LocalDirectory)
Script.CopyToHost    (LocatFileFilter, RemoteDirectory)
Script.CloneFromHost   (RemoteDirectory, LocalDirectory)
Script.CloneToHost   (LocalDirectory, RemoteDirectory)
```

**Script.Synchronize (LocalDirectory, RemoteDirectory)**

**Script.SynchronizeOneway (LocalDirectory, RemoteDirectory, Direction)**

Remote indicates files on the remote computer where the NetOp Host program runs, Local is the machine where your NFMscript application and the NetOp Guest run.

File filters must be legal Windows file filters like "C:\winnt*.exe". The name of one single file like "C:\config.sys" is also a legal file filter. Blanks are allowed in names. The functionality of these commands is described in the Chapter on scripting from inside NetOp.

The dialogs of NetOp are not shown during the execution of the commands unless the command need it's end user to take a decision, for example if a file should be overwritten or not. But if you call for example CopyToHost() on a very large file via a slow telephone line, your application is not locked. In your script program:

- All events are still processed so any button can be pressed
- Progress of commands can be caught and monitored
- Cancelling commands is build-in, and can even be customized

### Important

The methods in an NFMscript object are not reentrant. In order to keep your application alive and responsive, all messages are processed while the method waits for NetOp to finish processing the method. This makes it possible for you to call the same method again while the first call your made has not returned yet. Such a call will not work correctly, but return a busy code. It is your application's responsibility to ensure that methods in the NFMscript objects are not reentered into. One very useful exception to this rule is the three cancel methods.

### Cancel

If you have chosen to have your NFMscript visible in your application, your end user can press the escape key in the script log window. This fires the internal OnCancel() event. The built-in action on that event is that a messagebox pops up with a choice of four actions:

**Continue (Action 0)**

**Cancel Command (Action 1)**

**Cancel Call (Action 2)**

**Cancel Script (Action 3)**

Continue, will cause the script to continue as has nothing happened. In fact, the NetOp Guest is never notified. All three other NFMscript cancel replies will send a Cancel() command to NetOp. NetOp will in turn, as promptly as possible cancel the last command it was sent from your script, and that script function will return with an error. What will happen next is different for each of the three cancel replies.

Choosing Cancel Command will cause the next script command to be issued to NetOp. Only one single script command was stopped. Cancel Command is intended for use when for example one large irrelevant file blocks a useful transfer of many files.

Cancel Call will cause all further script commands to be ignored until the next Hangup command. All commands from the current one and till next Hangup will simply return successfully without doing anything. Cancel Call addresses the situation where you for example picked the wrong computer to connect to.

Cancel Script works the same way, but until the next Uninitialize command. It is intended for use when you want to stop everything and evaluate what to do next.

If you wish to have your own interface to cancelling, you can use the three equivalent cancel commands from the script interface. Since all events are still being processed during the execution of a command like CopyToHost(), all buttons will respond at any time. From your own cancel button, call

**Script.CancelCommand() or**

**Script.CancelCall() or**

**Script.CancelScript()**

for example like this, if you designed a button named CancelButton:

```
Sub CancelButton_Click()
        Script.CancelCall()
    End Sub
```

If you wish to use the internal cancel event, but construct your own actions on that event, fill in the OnCancel() event which the OCX will fire on your script application before putting up its message box.

You can for example do like this to make the user dialog less complex by allowing only CancelScript:

```
Private Sub Script_OnCancel(Action As Long)
rc = MsgBox("Cancel ?", vbYesNo)
If rc = vbYes Then Action = 3
If rc = vbNo Then Action = 0
End Sub
```

In the parameter Action you return 0 for continue, 1 for cancel command, 2 for cancel call and 3 for cancel script. Action will arrive to you with a value of -1. If you do not change that value, the built in message box above will pop up, otherwise not.

### Adding an Option Dialog

In parallel with OnCancel(), you will find OnRbuttonDown(). A difference is that this event has no default action. It only does what you program. The parameter is to there allow future extensions. For forwards compatibility, return a zero for no action.

```
Private Sub Script_OnRbuttonDown(Action As Long)
rc = MsgBox("Include Subdirectories", vbYesNo)
If rc = vbYes Then Script.SetIncludeSubdir(True)
If rc = vbNo Then Script.SetIncludeSubdir(False)
Action = 0
End Sub
```

## Monitoring Progress

You can at any time query the progress of a script command. It is however your application's responsibility to find a suitable place in your code to do it from. The NFM-script exposes the function:

```
Script.GetProgress()
```

which returns a percentage between 0 and 100. To use this from VB, instance a timer and a progress bar. You can for example get the progress bar from one of the Microsoft common controls OCXs.

```
    Sub Button_Click()
        rc = Script.Call(..)
        Timer1.Interval = 500
        rc = CopyToHost(....)
        Timer1.interval = 0
        Script.Hangup()
End Sub
Sub Timer1_Timer()
        ProgressBar1.Value = Script.GetProgress()
EndSub
```

## Settings

The NetOp scripting has many parameters to the file transferring commands. All these have been made available as methods named Set<NameOfItem>() in the OCX.They are:

```
SetOverwriteReadonly(BOOL YesNo)
SetOverwriteHidden(BOOL YesNo)
SetOverwriteSystem(BOOL YesNo)
SetOverwriteExisting(BOOL YesNo)
SetRetriesOnTransferError(long Retries)
SetRetriesOnConnectError(long Retries)
SetDeltaFileTransfer(BOOL YesNo)
```

**SetCrashRecovery(BOOL YesNo)**

**SetCompression(long Level)**

**SetConnected(BOOL conn)**

**SetIncludeEmptyDir(BOOL YesNo)**

**SetIncludeSubDir(BOOL YesNo)**

**SetIncludeHiddenAndSystem(BOOL YesNo)**

**SetIncludeOnlyNewer(BOOL YesNo, DATE DateTime)**

**SetIncludeOnlyExisting(BOOL YesNo)**

You may ask why these are methods and not properties, since all they seem to do is set the value of a variable. The reason is that some of them needed to be implemented as sending real commands to NetOp, while others just set a value to be used as an option to another command. For consistency, all settings are implemented as methods.

### Execute

Many methods in the Nfmscrpt.ocx correspond to a command in the NetOp script command language, which is the syntax you see in the NetOp Guest's script editor dialog and also in the OCX's log window. If you wish, you can send commands directly in that command language using:

**Rc = Script.Execute(String Command);**

The purpose of this OCX is however to relieve you of the burden of a lot of string formatting and event handling, so this entry is only published as an extra service for unforeseen circumstances.

## 12.5.5 Examples

In the NetOp installation directory, you will find a file named Examples.zip. Unzip this file to get the source code and executables for the examples. You will find:

### Hello World Script

HelloWorldScript.exe is the simplest possible example. When you press the start button, it will copy a file to a host computer. The Visual Basic project HelloWorldScript.vbp is included in the installation:

```
Private Sub Command1_Click()
        Dim Rc As Long
        Rc = HelloScript.Initialize
        Rc = HelloScript.Call("*")
        'Move some arbitrary file across. This one is always there
        Rc = HelloScript.CopyToHost(HelloScript.GetInstallDir() + "\netop.fac", "c:\*.*")
        Rc = HelloScript.Hangup
        Rc = HelloScript.Uninitialize
End Sub
Private Sub ExitButton_Click()
        HelloScript.FreeGuest
        Stop
End Sub

Private Sub Form_Load()
        HelloScript.StartGuest (True)
End Sub
```

## Visit all Hosts Script

This example is a bit more feature rich. In the beginning we declare a logical variable and we start the NetOp Guest when the program starts up. Next we cycle through the available phonebook files in the phonebook root directory and write their names in the log. We are namely intending to visit all these hosts one by one.

```
Dim More As Boolean
Private Sub Form_Load()
        Script.StartGuest True
        More = Script.PhonebookSetFirst
```

```
Do While More
        Script.WriteLog "Will visit " + Script.PhonebookGetFilename
        More = Script.PhonebookSetNext
Loop
End Sub
```

There is a button labelled “Start Visit”. When that is clicked, we show a dialog in which we will show what we are doing with that host while doing a CopyToHost() operation. When we are finished we stop the dialog and hide it.

```
Private Sub StartButton_Click()
        StartButton.Enabled = False
        StopButton.Enabled = True
        Script.Initialize
        More = Script.PhonebookSetFirst
Do While More
        rc = Script.Call(Script.PhonebookGetFilename)
        VisitDialog.Show
        Script.CopyToHost Script.GetInstallDir + "\netop.fac", "c:\*.*"
        VisitDialog.Animation1.AutoPlay = False
        VisitDialog.Timer1.Interval = 0
        Script.Hangup
        VisitDialog.Hide
        More = Script.PhonebookSetNext
Loop
        StopButton.Enabled = False
        StartButton.Enabled = True
        Script.Uninitialize
End Sub
```

The dialog shows the .avi file with the filecopy animation which also explorer does. The dialog has a timer which updates a progress bar.

```
Private Sub Form_Load()
        Caption = VisitForm.Script.PhonebookGetFilename
        Timer1.Interval = 100
        Animation1.Open "d:\netop\v60\filecopy.avi"
        Animation1.AutoPlay = True
End Sub
Private Sub CancelButton_Click()
        VisitForm.Script.CancelCall
        Hide
End Sub
Private Sub Timer1_Timer()
        ProgressBar1.Value = VisitForm.Script.GetProgress
        ProgressBar1.Refresh
End Sub
```

## Keep Synchronized Script

This is example showing timing and repetition using the Wait…() functions. At startup, start the Guest and set the initial parameters for the interface and the internal variables:

```
Dim Rc As Long
Dim TryAgain As Boolean
Private Sub Form_Load()
        Script.StartGuest (True)
        TryAgain = True
        StartTime.Value = Now
        ‘ StartDate.Value = Today
End Sub
```

The WaitUntil() function holds execution until the date and time entered into the Microsoft DTPicker controls StartDate and StartTime. Call("*") leaves it up to the end user to pick a phonebook file in a FileDialog, then Synchronize() synchronizes the contents of two directories. If the interface's checkbox is checked, the program will try repeat the Call() and Synchronize() periodically until you actively stop it. While inactive, the program will hide itself.

```
Private Sub StartButton_Click()
        Rc = Script.Initialize
        Rc = Script.WaitUntil(StartDate.Value, StartTime.Value)
Again:
        Rc = Script.Call("*")
        If (Rc <> 0) Then GoTo Done
        Rc = Script.Synchronize("C:\reports\*.*", "c:\reports\*.*")
  If (Rc <> 0) Then MsgBox ("This example assumes a directory C:\REPORTS")
  Rc = Script.Hangup
  If (Repeat.Value = Checked And TryAgain) Then
        If (MsgBox("Now sleep: " + CStr(Interval.Value), vbOKCancel) _
        = vbCancel) Then GoTo Done
        KeepInSyncForm.Hide
        Script.Wait (Interval.Value)
        KeepInSyncForm.Show
        GoTo Again
        End If
Done:
  Rc = Script.Uninitialize
End Sub
```

The button labelled Stop will cancel the repeating cycles:

```
Private Sub StopButton_Click()
        Script.CancelScript
        TryAgain = False
End Sub
```

The button labelled Clear will clear the log. This can be useful if it becomes very long.

```
Private Sub ClearButton_Click()
            Script.ClearLog
            Script.WriteLog ("Ready")
End Sub
```

The Exit button will free the guest and stop the program.

```
Private Sub ExitButton_Click()
            Script.FreeGuest
            Stop
End Sub
```

If you hold down the right mouse button, you can clear the log.

```
Private Sub Script_OnRbuttonDown(Action As Long)
  If (MsgBox("Clear Log?", vbYesNo) = vbYes) Then
            ClearButton_Click
            Action = 0
  End If
End Sub
```

## 12.5.6 Reference

The following tables represent all the API methods:

*Note: All Nfmscript methods which return a Long, return zero for success (Unless otherwise specified).*

**Table 12-6 The NFMScript Methods**

**Table 12-6 The NFMScript Methods (Continued)**

**Table 12-6 The NFMScript Methods (Continued)**

**Table 12-6 The NFMScript Methods (Continued)**

**Table 12-6 The NFMScript Methods (Continued)**

**Table 12-6 The NFMScript Methods (Continued)**

**Table 12-6 The NFMScript Methods (Continued)**

| Method | Description |
|---|---|
| Call (Filename As String) As Long | Call a phonebook entry. See also Hangup() and CancelCall(). If Initialize() was not called, it will be called implicitly. That will in turn call StartGuest() if the guest is not already running. If another Call() is currently active, it will be hung up. If you wish two simultaneous Call()'s you must use two Nfmscript objects. |
| CancelCall () As Long | Cancel the Call() which is currently active. Typically called asynchronously from a separate button. The current method (for example CopyFromHost) will be cancelled, and return an error code. All following methods will return immediately with no error, until your program executes the next Hangup() or Call() method. |
| CancelCommand () As Long | Cancel the method call which is currently active. Typically called asynchronously from a separate button. The current method (for example CopyFromHost) will be cancelled, and return an error code. All following methods will execute as if nothing had happened. |
| CancelScript () As Long | Cancel the Call() which is currently active. Typically called asynchronously from a separate button. The current method (for example CopyFromHost) will be cancelled, and return an error code. All following methods will return immediately with no error, until your program executes the next Uninitialize() or Initialize() method. |
| ClearLog () As Long | Clears the script object's log window. |
| CloneFromHost (RemoteDir As String, LocalDir As String) As Long | Clones the directory RemoteDir to the LocalDir directory. A Call() must be open to the computer with the RemoteDir.<br>**RemoteDir**<br>A directory on the remote computer where the NetOp Host runs. Must end with "*.*".<br>**LocalDir**<br>A directory on you local computer where the NetOp Guest runs. Must end with "*.*". |
| CloneToHost (LocalDir As String, RemoteDir As String) As Long | Clones the directory LocalDir to the RemoteDir directory. A Call() must be open to the computer with the RemoteDir.<br>**LocalDir**<br>A directory on your local computer where the NetOp Guest runs. Must end with "*.*".<br>**RemoteDir**<br>A directory on the remote computer where the NetOp Host runs. Must end with "*.*". |
| CopyFromHost (RemoteFilter As String, LocalDir As String) As Long | Clones the files matching RemoteFilter to the LocalDir directory. A Call() must be open to the computer with the RemoteFilter.<br>**Remote Filter**<br>A valid file filter on the remote computer where the NetOp Host runs. An example could de "C:\DATA*.XLS"<br>**Local Dir**<br>A directory your local computer where the NetOp Guest runs. Must end with "*.*". |

| Method | Description |
|---|---|
| CopyToHost (LocalFilter As String, RemoteDir As String) As Long | Clones the files matching LocalFilter to the RemoteDir directory. A Call() must be open to the computer with the RemoteDir.<br>**Local Filter**<br>A valid file filter on your local computer where the NetOp Guest runs. An example could de "C:\DATA*.XLS"<br>**RemoteDir**<br>A directory on the remote computer where the NetOp Host runs. Must end with "*.*". |
| DirGetName () As String | Returns the name of the current subdirectory from DirSetFirst/Next(). |
| DirSetFirst (Directory s String) As Boolean | Initializes the directory search entries, so next call to DirGetName() will return the name of the first subdirectory of "Directory" on the remote computer. You must have an open Call() to that computer. If there are no such subdirectories, the return value is False. On success, the return value is True.<br>**Directory**<br>A directory on the currently Call()'ed remote computer. |
| DirSetNext () As Boolean | Advances to the next directory search entry, so next call to DirGetName() will return the name of the next subdirectory. If there are no more subdirectories, the return value is False. On success, the return value is True. |
| DriveGetName () As String | Returns the name of the current disk drive from DriveSetFirst/Next(). |
| DriveSetFirst () As Boolean | Initializes the disk drive entries, so next call to DriveGetName() will return the name of the first disk drive on the remote computer file, you currently have made a Call() to. If there are no disk drives, the return value is False. On success, the return value is True. |
| DriveSetNext () As Boolean | Advances to the next disk drive entry, so next call to DriveGetName() will return the name of the next disk drive. If there are no more drives, the return value is False. On success, the return value is True. |
| Execute (Command as String) As Long | Execute a script editor command. The format of these command resemble the Nfmscript methods, and are documented in Table 12-4.2<br>**Command:**<br>The command to execute |
| FileGetAccessed () As Date | Returns the last access date for the file selected with FileGetFirst/Next() |
| FileGetArchive () As Boolean | Returns the archive flag for the file selected with FileGetFirst/Next() |

| Method | Description |
|---|---|
| FileGetCreated () As Date | Returns the create date for the file selected with FileGetFirst/Next() |
| FileGetHidden () As Boolean | Returns the hidden flag for the file selected with FileGetFirst/Next() |
| FileGetModified () As Date | Returns the modified date for the file selected with FileGetFirst/Next() |
| FileGetName () As Date | Returns the name of the file selected with FileGetFirst/Next() |
| FileGetReadonly () As Boolean | Returns the readonly flag for the file selected with FileGetFirst/Next() |
| FileGetSize () As Long | Returns the size of the file selected with FileGetFirst/Next(). If the size is above 2GB, -1 will be returned. |
| FileGetSystem () As Boolean | Returns the system flag for the file selected with FileGetFirst/Next() |
| FileSetFirst (FileFilter As String) As Boolean | Initializes the file entries, so next call to FileGet.() will return a property of the first file on a remote computer matching the given file filter. If there are no entries, the return value is False. On success, the return value is True. There must be an open Call () on the remote computer<br>**File Filter:**<br>A legal file filter on the remote computer like for example "C:*.*" |
| FileSetNext () As Boolean | Advances to the next file entry, so next call to FileGet..() will return the name of the next remote file. If there are no more files, the return value is False. On success, the return value is True |
| FreeGuest () As Long | Frees connection to NetOp Guest DLLs and does other clean up. Not mandatory, but it is good practice to call this before your application exits. Do not use this method in conjunction with browser scripts. |
| GetInstallDir () As String | Returns the NetOp install directory on your local computer where the NetOp Guest program runs. |
| GetPhonebookDir () As String | Returns the phonebook directory. The NetOp.ini PHONEBOOKPATH and DATAPATH settings are respected. |
| GetProgress () As Long | Get the progress of the current method. Typically only useful with Copy, Clone and Synchronize methods. Returns the percentage 0-100 where 100 means done. Useful if you place it in a timer and feed the result into a progress bar. |

| Method | Description |
|---|---|
| Hangup () As Long | Hang the current Call() up. |
| Initialize () As Long | Initializes a session with a NetOp Guest. Check the return code to be zero before calling other methods. See also Uninitialize(). If the NetOp Guest is not already running, StartGuest() will be called implicitly. |
| PhonebookGetFilename () As String | Returns the name of the current phonebook file. If there are none, the string returned is "No Phonebook Entries or Error" |
| PhonebookSetFirst () As Boolean | Initializes the phonebook entries, so next call to PhonebookGetFilename() will return the name of the first phonebook file. If there are no entries, the return value is False. On success, the return value is True. |
| PhonebookSetNext () As Boolean | Advances to the next phonebook entry, so next call to PhonebookGetFilename() will return the name of the next phonebook file. If there are no more files, the return value is False. On success, the return value is True. Can be used with both PhonebookSetFirst() and PhonebookSetSubfolderFirst(). |
| PhonebookSetSubfolderFirst (Folder As String) As Boolean | Initializes the phonebook entries, so next call to PhonebookGetFilename() will return the name of the first phonebook file is a specific subdirectory of the phonebook directory. If there are no entries, the return value is False. On success, the return value is True. |
| RunLocal (Command As String) As Long | Runs an operating system executable file with parameters on your local computer.<br>**Command:**<br>The name of a bat, com or exe file. If you wish to use shell commands, use must give the name of the shell executable. For NT and Win95 this is "cmd.exe", so you can use "cmd /c dir c:*.*" or "cmd /k rename autoexec.bat autoexec.old". |
| RunRemote (Command As String) As Long | Runs an operating system executable file with parameters on a remote computer. A Call() must be open to that computer. Please note that the outcome this is dependent of the setup of the remote computer environment, and 100% independent of your local computer.<br>**Command:**<br>The name of a bat, com or exe file. If you wish to use shell commands, use must give the name of the shell executable. For NT and Win95 this is "cmd.exe", so you can use "cmd /c dir c:*.*" or "cmd /k rename autoexec.bat autoexec.old". |
| SetCompression (Level As Long) As Long | Set the compression level.<br>**Level:**<br>An integer number. 0 means no compression, >0 means compression. |

| Method | Description |
|---|---|
| SetCrashRecovery (YesNo As Boolean) As Long | Instructs NetOp whether or not to try apply crash recovery. If a call() is interrupted, a partial file can be kept on the target disk. Only useful if delta file transfer is on, so this method will implicitly set delta file transfer to True.<br>**YesNo**<br>If True, partial files will be kept on the target disk, and delta file tranfer will be set, so the valid part need not be retransmitted next time you come back. If False, partial files will be cleaned up automatically if you loose your connection. |
| SetDeltaFileTransfer (YesNo As Boolean) As Long | Instructs NetOp whether or not to try apply Delta File Transfer, the method to try minimize the amount of data transferred unnecessarily. This state is also set by SetCrashRecovery(True), but not cleared by SetCrashRecovery(False).<br>**YesNo**<br>If True, delta file transfer will be applied when applicable. If False, all file transfers will unconditionally transfer all bytes in all files. |
| SetIncludeEmptyDir (YesNo As Boolean) As Long | Instructs NetOp whether or not to include empty directories in file transfer operations.<br>**YesNo**<br>If True, empty directories are included. If False, they are not included |
| SetIncludeHiddenAndSystem (YesNo As Boolean) As Long | Instructs NetOp whether or not to include hidden and system files in file transfer operations.<br>**YesNo**<br>If True, hidden and system files are included. If False, they are not included. |
| SetIncludeOnlyExisting (YesNo As Boolean) As Long | Instructs NetOp whether or not to include only files which already exist with the same name on the target computer in file transfer operations.<br>**YesNo**<br>If True, only files which already exist with the same name on the target computer are transferred; no new files will be created. If False, all files are transferred whether they exist in advance or not. |
| SetIncludeOnlyNewer (YesNo As Boolean, Date As Date) As Long | Allows you to set a limit to how old files you wish to include in file transfer operations.<br>**YesNo**<br>If True, only files which are newer than Date are transferred. If False, all files are transferred no matter what date they were last modified.<br>**Date**<br>Files with a modify date older than this will be excluded if YesNo is True. |
| SetIncludeSubDir (YesNo As Boolean) As Long | Instructs NetOp whether or not to include subdirectories of the directories/file filters given as source in file transfer operations.<br>YesNo |

| Method | Description |
|---|---|
| SetOverwriteExisting (YesNo As Boolean) As Long | Set the action you wish when trying to overwrite existing files<br>**YesNo**<br>If True, existing files will be overwritten without warnings. If False, existing files will cause a prompt in a dialog. |
| SetOverwriteHidden (YesNo As Boolean) As Long | Set the action you wish when trying to overwrite hidden files<br>**YesNo**<br>If True, hidden files will be overwritten without warnings. If False, hidden files will cause a prompt in a dialog. |
| SetOverwriteReadonly (YesNo As Boolean) As Long | Set the action you wish when trying to overwrite readonly files<br>**YesNo**<br>If True, readonly files will be overwritten without warnings. If False, readonly files will cause a prompt in a dialog. |
| SetOverwriteSystem (YesNo As Boolean) As Long | Set the action you wish when trying to overwrite system files<br>**YesNo**<br>If True, system files will be overwritten without warnings. If False, system files will cause a prompt in a dialog. |
| SetReportLog () As None | Make the logging of events in the object's log window be the default treeview representation. |
| SetReportSilent () As None | Disable the logging of events in the object's log window |
| SetRetriesOnConnectError (Retries As Long) As Long | Set the number of times you wish the file call method to automatically retry making the connection before returning<br>**Retries**<br>An integer number between 0 and 9 inclusive. |
| SetRetriesOnTransferError (Retries As Long) As Long | Set the number of times you wish the file transfer methods to automatically retry an operation before returning<br>**Retries**<br>An integer number between 0 and 9 inclusive. |
| StartGuest (Minimized As Boolean) As Long | Starts the NetOp guest executable. If it is already started, StartGuest() will just return with no error. If the NetOp Host is running, StartGuest() will return an error code.<br>Minimized<br>If True, the guest will be attempted started up minimized.<br>**Return Codes -11 and -12 mean success**<br>**-11 -** Started OK<br>**-12 -** Already started |
| Synchronize (LocalDir As String, RemoteDir As String) As Long | Synchronizes two directories. A Call() must be open to the computer with the RemoteDir.<br>**LocalDir**<br>A directory on your local computer where the NetOp Guest runs. Must end with "*.*".<br>**RemoteDir**<br>A directory on the remote computer where the NetOp Host runs. Must end with "*.*". |

| Method | Description |
|---|---|
| SynchronizeOneWay (SourceDir As String, TargetDir As String, ToHost As Boolean) As Long | Synchronizes two directories, but moves files one way only. A Call() must be open to the remote computer.<br>**SourceDir**<br>the directory where the files origin from. It can be local or remote depending on ToGuest. Must end with "*.*".<br>**TargetDir**<br>The target directory. It can be local or remote depending on ToGuest. Must end with "*.*".<br>**ToHost**<br>If True, files are only transferred from Guest to Host. If False, it is reverse. |
| .Uninitialize () As Long | Uninitializes a session with a NetOp Guest. Initialize() must be made again before calling other methods. Uninitialize is not mandatory, but a good practice. |
| Wait (Period As Date) As Long | Waits a period, then returns<br>**Period**<br>The interval you wish the method to wait before returning. If you have only a number of seconds the WaitSeconds() function is easier because it does not require a Date variable. Not that if you have AM-PM time representation, an interface showing 12:00:01 AM will cause a wait of 1 second, not 12 hours and 1 second. |
| WaitSeconds (Period As Long) As Long | Waits a number of seconds, then returns<br>**Period**<br>The interval you wish the method to wait before returning. |
| WaitUntil (Date As Date, Time As Date) As Long | Waits until a given local time and date, then returns. For easier use with the MS DTPicker object, this method has two parameters. You can have two DTPickers, one for date and one for time.<br>**Date**<br>The date you wish the method to wait until before returning. If this vaiable has a Time part, it will be ignored.<br>**Time**<br>The time on the above date when the method will return. If this variable has a Date part it is ignored |
| WaitUntilAnyDay (Time As Date) As Long | Waits until next time the clock passes a given local time, then returns. This method is intended for applications, which want to repeat an operation at a given time every day.<br>**Time**<br>The time on any date when the method will return. If this variable has a Date part it is ignored. |
| WriteLog (Text As String) As Long | Writes a text in the script object's log window, if it is in the SetReportLog() status, which is the default.<br>**Text**<br>A string to be appended to the current treeview item in the log. |

# Chapter 13
# Troubleshooting

## 13.1 The Nature of Remote Control

Remote control requires a program to interact closely with the operating system in order to pick up screen information and deliver keyboard and mouse input. This all has to be done so the PC, the operating system and the program(s) running are affected as little as possible.

This process is sensitive to new hartdware devices and drivers and to operating system service packs and other updates. It is also sensitive to tricks applications may play.

Should you run into problems with a specific hardware or software, we will appreciate hearing from you. We are very interested in investigating such problems in order to come up with a solution either immediately or as a part of a future release.

## 13.2 Answers to Common Problems

Please feel free to visit our homepage at www.danware.com, for up-to-date information and technical support.

**The Host screen does not update correctly**

Sometimes the *Transfer Host screens as commands* method yields incorrect results. Try switching to the *Transfer Host screen as bitmap* method (changed from the Host options dialog box on the Guest). Remember to hang-up and reconnect before changes take effect. If this option is selected, try to improve performance by using the screen caching utility in the *Compression* section of the *Host options* dialog.

Sometimes you can solve screen update problems by just minimizing and restoring the Host window (this forces NetOp to redraw the Host screen).

**Problems with communication between Guest and Host**

Windows sometimes needs to be restarted in order for the communication devices to function properly. If you are having trouble connecting or loose connection, try to restart Windows on Guest and Host.

**I cannot connect to a Host using IPX on a Novell Network**

Be sure that both machines are using the same frame types. If you are using Novell IPX, the frame type will be specified in the NET.CFG file. If you are using Windows IPX, the frame type is usually found in the PROTOCOL.INI file. The only situation when the frame types can differ is when a routing mechanism exists to route the IPX packets. Usually the frame type 802.2 is used within a Netware 4.x environment and 802.3 within a Netware 3.x environment.

**Sometimes screen updates freeze**

This is usually because some other application running on the Host PC prevents the NetOp Host from transmitting data to the Guest. Common solutions to this problem are:

1. In many cases NetOp recovers automatically in approximately 10 seconds.

2. If you loose the connection due to a time out, wait a moment and then call again.

3. Do not use ALT+TAB when controlling a full screen DOS box and do not try to access the Hosts floppy drive when the drive is empty.

4. If the other application crashed, try not to use it in the future while controlling the Host PC.

**NetOp has trouble communicating via TCP/IP**

Some networks might have problems handling NetOp's default maximim packet size. If the built-in automatic packet size correction feature should fail, try lowering this value on both Guest and Host. Choose *Communication profile* from the *Configuration menu,* select your TCP/IP profile and edit the MTU field, try 512 bytes. If this is successful try to increase performance by experimenting with higher values.

**I cannot get a connection between my modems.**

For some modems the error correction and data compression are not compatible. Try disabling these two features of the modems (by changing your modem setup strings). Try lowering the data rate.

You will notice that some modems in the database are called 'Basic' (i.e.. Compaq Presario 19.2 Basic). Modems with the 'Basic' name added have data compression and error correction disabled, so there is no need to change the modem strings.

**The Host screen is shown as a black screen**

TCP/IP: Try to decrease the MTU size to 512 bytes. Some networks (including the Internet) will not transfer packets that are bigger.

IPX: Set MaxPackSiz=512 in the IPX section of the NETOP.INI file.

Disable hardware acceleration on the graphics adapter (try bitmap mode).

Make sure that you are using the newest version the graphics driver.

## 13.3 Technical Support

In case you require technical assistance you should always seach the support pages on WWW.DANWARE.COM for a possible solution to your problem.If there is no solution to your problem here, you should contact your local NetOp distributor. If you are attached to the Internet, you may use the On-line Help button in the Help menu of your NetOp Host or Guest.

# Index

## A



## B



## C

## D



## E



## F

## G



## H

## I



## K



## L



## M



## N

## S

## T



## U



## W



## Z