TOTAL CONTROL™

NETServer 3.1

Windows

SOFTWARE INSTALL GUIDE

Table of Contents

Chapter 10 Reference

Chapter 1
Introduction

This chapter contains information on the following:

- What's new in version 3.1?
- The NETServer family of products

What's new in version 3.1?

NETServer manager 3.1 can configure the following new features of the NETServer 3.1 firmware.

- Classless Interdomain Routing via the Netmask table
- RADIUS accounting servers
- IP address spoofing
- Quad modem PPP/SLIP processing
- Randomized hosts
- Logging ICMP messages to Syslog
- Modem Initialization Strings
- PAP enable/disable
- Support for NETServer PRI Call Mapping and Service Profiles

Moreover, the following enhancements have been made to the user interface:

- Save NETServer configuration files to disk
- More intuitive port configuration
- Multiple connection support
- Enhanced performance monitoring

Save To Disk

NETServer manager 3.1 allows you to save a NETServer's entire configuration to a file on your PC's disk. This new feature is especially useful in the following instances:

1. You forget your supervisor password, forcing you to erase your NETServer's flash memory. Restoring a saved configuration file is the only alternative to configuring the box all over again.
2. You want to copy a NETServer's entire configuration to another NETServer (Save, login to the other NETServer, and then Restore).

Note: You can only save the configuration of NETServers with firmware version 3.1 or later

Multiple Connection Support

NETServer Manager now allows you to be connected to several NETServer's simultaneously. To avoid confusion, the IP address of the NETServer you are currently configuring is now displayed as part of the title of most windows.

Enhanced Performance Monitoring

NETServer Manager now features several new status screens, which allow you to view Network Statistics, Network Connections, the IP and IPX Routes table, Port Statistics and Port Sessions.

More Intuitive Port Configuration

NETServer Manager now simplifies port configuration by showing you only the fields which apply to the port type you are configuring. Simply select the port type you want and then click the Configure Port button. NETServer Manager will display a window containing exactly the fields you need to set. Fill them out and save your work. Port configuration is just that simple.

The NETServer Family of Products

The NETServer Manager software can configure several different NETServer platforms ranging from the desktop-size NETServer/2 all the way up to large data center solutions that use the NETServer Card for the Total Control chassis. When configuring these platforms from NETServer Manager, it is important to understand their similarities and their differences.

Despite their differences, most NETServer platforms have a LAN port (Ethernet or Token Ring), a number of modems, and a single external serial port. For the most part, their mission in life is to relay data from the modems to the LAN and vice versa.

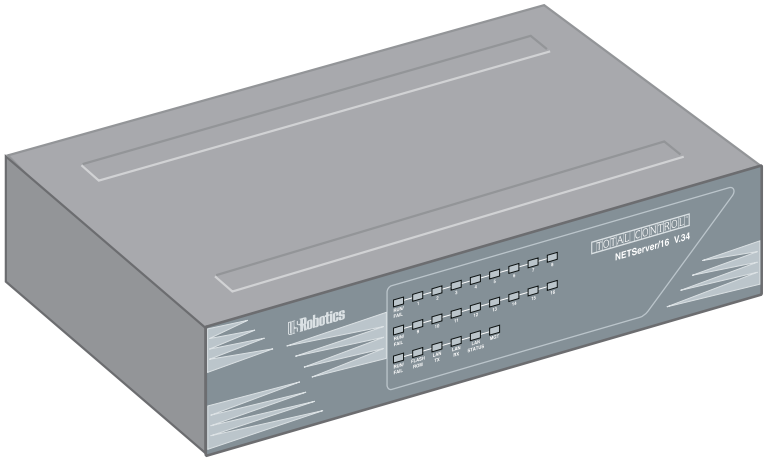
NETServer/2

The NETServer/2 has a single internal modem (Port 0) which is connected to the NETServer using an internal serial interface. An additional modem may be connected to the NETServer/2's external serial port. Such a modem would be addressed as Port 1.

Note: NETServer/2 port numbering is unique. On all other NETServer platforms, the external serial interface is Port 0.

NETServer/8 and NETServer/16

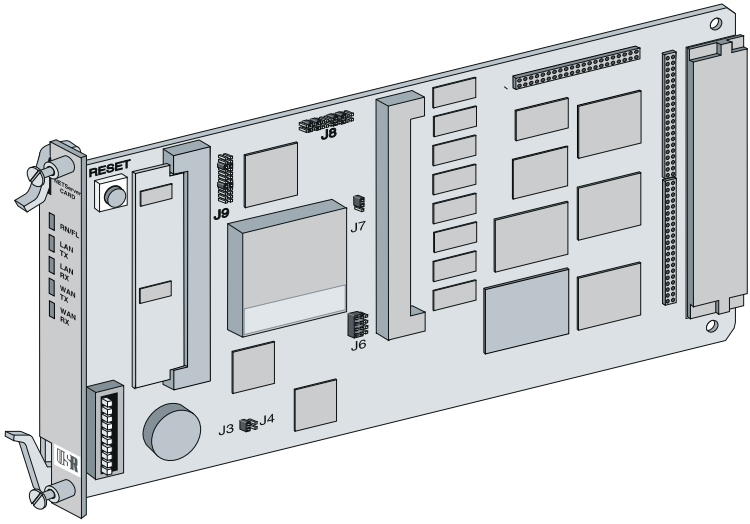
The NETServer/8 has eight internal modems which are referred to as Ports 1 through 8. Like the NETServer 2's internal modem, each of these modems is connected to the NETServer using an internal serial interface. There is also an external serial interface, which can be configured as Port 0.



The NETServer/16 is a NETServer/8 with more internal modems.

NETServer Card

The NETServer card can access up to 60 modems (15 quad modem cards) residing in the Total Control chassis. The serial port marked *CH1* on the NETServer's Network Interface Card (NIC) is configurable as Port 0.



The port number of a modem on a quad modem card can be found using the following formula:

Port Number = [4* (chassis slot -1)] + modem number

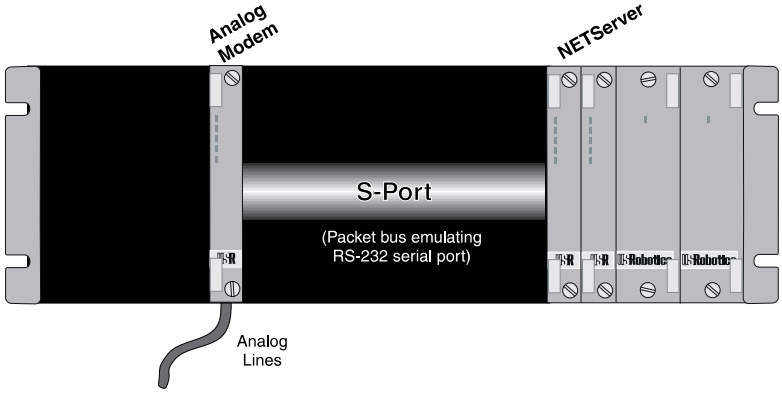
So, modem 2 on a card in slot 7 would be

[4*(7-1)] + 2

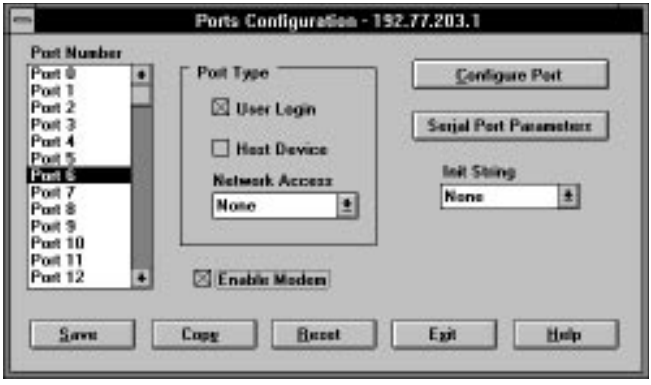
Which yields a port number of

26

Unlike smaller NETServers, the NETServer card is not directly connected to the modems it uses. Instead, the NETServer card forms a virtual serial connection over the chassis packet bus. This allows the packet bus quad modems to be configured and used by the NETServer as if they were ordinary serial modems.

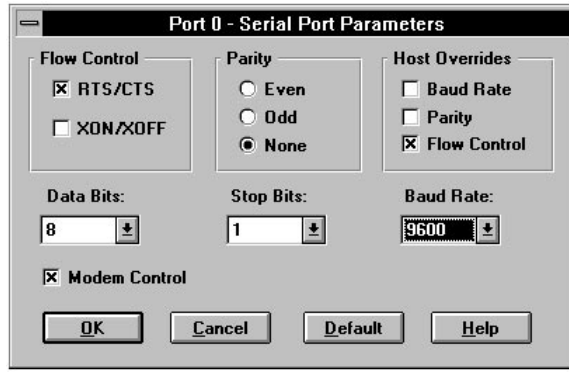


When configuring a NETServer card, you must establish the virtual serial connection to each modem that will be used. This is done by checking the Enable Modem box in the Port Configuration window.



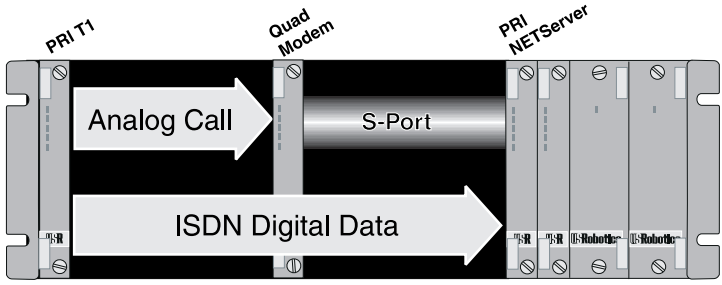
Note that this box will only appear when a packet bus port is selected in the Port Number box. It does not appear for Port 0, which is a real serial port, or for any port on the smaller NETServer platforms.

Similarly, when you click on Serial Port Parameters, not all the fields in the window that appears are configurable for a packet bus port, which is after all, only emulating a serial connection.



NETServer PRI Card

In addition to all the functions of the basic NETServer card, NETServer PRI also supports dial in over primary rate ISDN. To do this, NETServer PRI works in conjunction with a primary rate ISDN trunk line (PRI T1/E1) card.



Calls signaled as voice grade audio are forwarded to a modem, which answers the call just as it would in a non-ISDN chassis setup.

However, when a call is signaled as ISDN data, the data is forwarded directly to the NETServer. Because there is no modem involved in this type of call, there is no modem port that can be configured beforehand. The NETServer dynamically allocates bandwidth for each ISDN call and frees those resources when the call is torn down.

From a configuration standpoint, this means that any quad modems used for a given application must still be set up in the Port Configuration window. However, the ports created for ISDN service are essentially configuration free. To configure an ISDN applications, go to the appropriate application chapter and skip port configuration.

Chapter 2
Installation

This chapter contains information on the following:

- Preliminary setup for IPX-only networks
- Installing the NETServer Configuration Manager on a Windows PC.
- Logging in to the NETServer Configuration Manager
- Things we recommend you do right away

Before you begin

Before you proceed, you must complete the *Minimum Configuration* section in the NETServer Command Reference.

IPX only Networks - Before you do anything else

The NETServer Manager is a TCP/IP application. It does not talk IPX. To get this program working on an IPX only network, you have to load the TCP/IP protocol stack on one or more machines.

What machine(s) will I load the software on?

The simplest way to get the NETServer Manager running on an IPX only network is to load it only on PCs that are on the same network segment as the NETServer is (in other words, they share an IPX Network Number). Since this does not require that your network actually route IP packets, the TCP/IP stack needs to be loaded only on the PCs that will be running the NETServer software. The section titled *Additional Setup for an IPX only PC*, later in this chapter, gives instructions for loading the TCP/IP stack once the NETServer software has been installed.

If there are routers (or servers performing routing functions) between the NETServer and the PC on which you want to run the NETServer Manager, you must configure these routing devices to route IP packets. Otherwise, they will simply discard NETServer Manager's IP packets before they get to the NETServer. To configure these routing devices for IP routing, consult the documentation that came with them.

Installing the Management Software

1. Load the Installation Disk in the floppy drive.

a. From the Program Manager File Menu, select Run.

b. Type the following:

(If the diskette is in a drive other than a:, substitute the appropriate drive letter)

2. The NETServer Manager Installation window appears.

The install utility will want to create the directory C:\NETSRVR and install the files in it.

Either accept the default directory the install program suggests or type in another drive and directory. Click OK or press the Enter key when you are finished.

3. You will then be asked if you want to add a new program group to your Windows Program Manager. Click on the Yes button or press the Enter key.

4. The Program Manager appears briefly, as does the newly created program group. The installation window reappears.

5. When the installation is complete, click the OK button or hit the Enter key. You will then be returned to the Windows Program Manager.

Make sure you have the right version of WinSock.

The NETServer software talks to WinSock, which adds a TCP/IP applications interface to Windows. There are several versions of the WINSOCK.DLL file out there. You must be sure that you are using the version of WinSock that goes with your IP drivers. In other words, if you are using Novell's LAN Workplace, use Novell's version of WinSock. If you are using Chameleon's IP drivers, use Chameleon's version of WinSock, etc.

The NETServer comes with Novell's LAN Workplace IP drivers. When you install the NETServer Windows software, the installation program will install Novell's version of WinSock.

If you are using someone else's IP drivers, you must go back and install the appropriate version of WinSock after you have finished loading the NETServer software on your machine. Make sure the WinSock files are installed in the same directory that you installed the NETServer software in.

Additional setup for an IPX only PC.

You must load TCP/IP on any PC that will run the NETServer software.

Step 1 - TCP/IP AUTOEXEC.BAT settings

The PC must be using ODI drivers. You cannot load the IP stack on a PC running IPX.COM. Instead of the older configuration, the PC's AUTOEXEC.BAT file must contain the following lines:

a. Run LSL.COM note that the NETServer manager installation program copied a version of this into the same directory it installed the NETServer software in (\NETSRVR). Example:

```
lsl
```

b. Load your network interface card driver. TCP/IP setup requires the Ethernet_II or the Token-Ring_SNAP frame type. If your network is not using one of these frame types, your NIC driver must be a promiscuous mode driver (support multiple frame types concurrently). Since most current network interface card drivers *are* promiscuous mode drivers, if you make sure you have the most recent version of your NIC driver, you should be all right.

```
NE2000
```

c. Load TCP/IP. The version provided with the NETServer is from Novell's LAN Workplace. The NETServer Manager installation program also copied this file into its own directory (\NETSRVR). Setup example:

```
TCPIP
```

If the PC will also run IPX, you must include two more lines:

a. Load IPXODI. This file is available from Novell. Example:

```
ipxodi
```

b. Load NETX or VLM. These files are also available from Novell. Note that VLM is the more recent version of this driver. If you are still using NETX, we recommend upgrading to VLM. Example:

```
VLM
```

Step 2 - NET.CFG setup

You now have to add some TCP/IP parameters to the PCs NET.CFG file.

a. Find the "Link Driver" section of the NET.CFG file. As a minimum, NET.CFG must have a link driver section for each MLID the PC is using. For Ethernet networks, you must use must the Ethernet_II frame type (though you may include other frame types).

```
Link Driver <driver name>
    Frame Ethernet_II
    <other frame types being used>
```

For Token Ring networks, you must use must the SNAP frame type (though you may include other frame types).

```
Link Driver <driver name>
    Frame Token-Ring_SNAP
    <other frame types being used>
```

b. Find the "Link Support" section of the NET.CFG file. As a minimum, this section must exist and must contain the following lines:

```
Link Support
    Max Boards  1          (or more)
    Buffers  8  1500       (or more)
    Mempool  4096          (or more)
```

c. Find the "Protocol TCPIP" section. As a minimum, this section must exist and must contain the following lines:

```
Protocol TCPIP
    ip_address             <an IP address for the PC>

    ip_router              <IP address>
```

(the PC's default IP gateway - could be NETServer)

ip_netmask <NETServer's netmask>
tcp_sockets 8
udp_sockets 8
raw_sockets 1

Logging in to the NETServer

1. Double-click on the Windows management software icon from the U.S. Robotics NETServer program group.

   The Login window appears:

2. Type in the IP address of the NETServer and press the Enter key.

   (If the Login window does not appear, select Open Connection from the File menu.)

3. Type in the NETServer's password (default is no password).

4. If you want the Windows software to "remember" this NETServer, click on the Remember new NETServers box. The Windows software adds this NETServer to the list of NETServers.

   The next time you log in, you need only click on the scroll arrow and select the IP address of the NETServer you want to log in to.

5. Click on the Login button and wait for the Configuration manager to establish a connection with the NETServer.

If the connection is not successful, select Open Connection from the File menu and try logging in again.

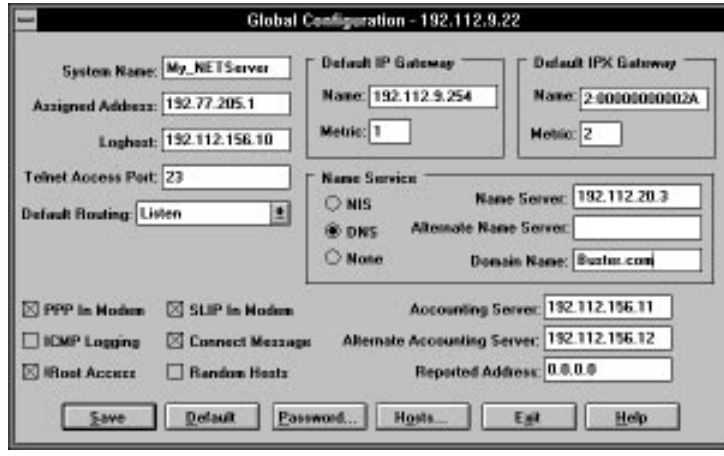
Things we recommend you do right away

This section continues basic configuration of the NETServer. It configures the same items covered in the *Recommended Global Configuration* section in Chapter 2 of the NETServer Command Reference.

The following is a list of the fields we recommend that you configure. They can all be found in the Global Configuration window.

- *Password*
- *IP or IPX Gateway*
- *Name Service*

Select Global from the Table menu. The Global Configuration window appears:



Password

This password will be used to log in to the NETServer from Windows or from the command line software. The default is none. The password can be any combination of up to 15 ASCII characters.

> **Do not forget your password.** If you do, you will have to erase *all* configuration information saved in flash memory. Remember to save a copy of the NETServer's configuration to disk so you don't risk having to start the configuration process all over again.

Default IP and IPX Gateways

If the NETServer does not know where to send a packet, it forwards the packet to the default gateway specified here. Default gateways must be on the same subnet as the NETServer.

***Name** (IP)*

This is the IP Address or name of the Default IP Gateway.

***Name** (IPX)*

This is the full IPX node address of the Default IPX Gateway. It is written in hexadecimal format as shown below.

8 digit network number:12 digit node MAC address

Metric

You must also enter a metric (hop count) for each type of default gateway. Possible values range from 1 (default) to 15. Note that since the actual metric of a default gateway is only 1 hop, the value entered here is used to control the perceived cost of the gateway to other routers on your network. For example, a high metric will limit the number of hops that the route is broadcast and may cause other routers to see it as a less preferable route.

If the NETServer is configured to listen for IP default route broadcasts (see *Default Route* in Chapter 10), the IP Default

Gateway can be overridden by a default route broadcast with a lower hop count.

Name Service

These fields configure the name service your network uses. A name service allows you to use host names rather than just IP addresses. The default is *none.*

NIS The network uses the Network Information Service (NIS). NIS is sometimes referred to as YP (Yellow Pages).

DNS The network uses the Domain Name Service (DNS).

None The network does not use a name service.

If you select DNS or NIS, you must also enter the Name Server and Domain Name.

Name Server

This is the IP address of the server providing the name service.

Alternate Name Server

This allows you to specify the IP address of an alternate name server.

Domain Name

This is the name of the domain that the NETServer belongs to. Both the primary and the alternate name servers must belong to the same domain.

Save your work

Save your configuration changes by clicking on the Save button.

NOTE: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes to flash memory. To save the changes permanently to flash memory from Windows, you must also select Save to FLASH from the File menu.

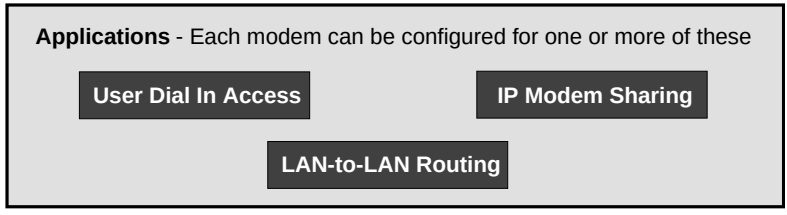
Chapter 3
The Basics

This chapter provides information on the following:

- How to set up applications
- The main window and menu options
- Software configuration tables

How to Setup Applications

There are basically three applications the NETServer is designed to handle: user dial in access, modem sharing, and LAN-to-LAN routing. All other applications are variations on one of these themes.



Configuration for each of these applications is a two step process:

1. Configure one or more modem ports to support the application. Note that a port may be configured to support multiple applications at the same time.
2. Add user table or location table entries or both, depending on the application.

Where do I go from here?

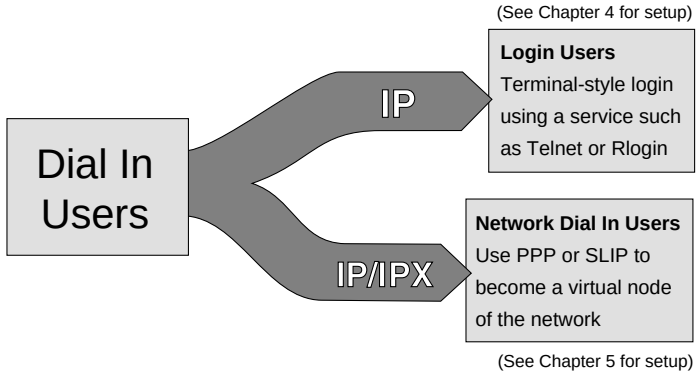
Each of these applications has a section of this manual devoted to its setup. If you want to begin configuration immediately, you may go to one of the chapters listed below:

Application	*Section*
User Dial In Access	Chapters 4 and 5
LAN-to-LAN Routing	Chapter 6
IP Modem Sharing	Chapter 7

Note that there are actually two Chapters for user dial in access. They cover two very different types of user: login users and network dial in users.

Login Users

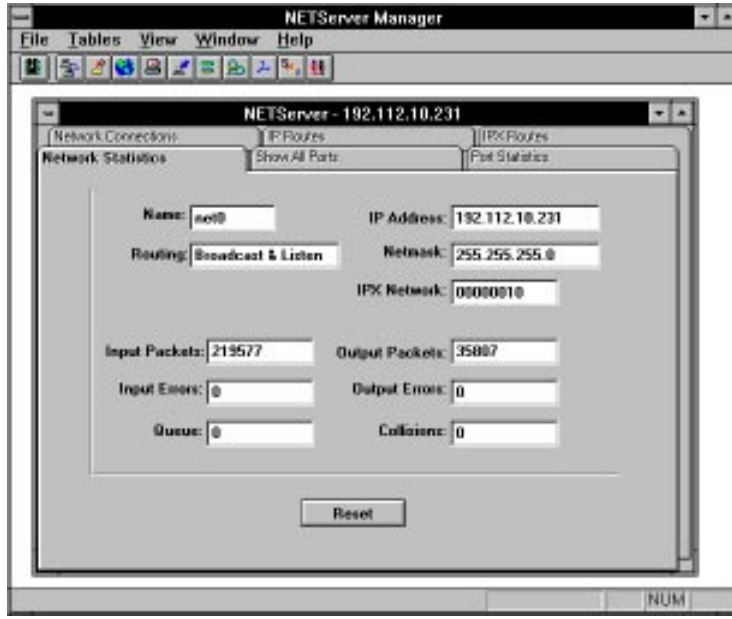
These are users requesting terminal access to an IP host. They dial into the NETServer and are connected to the requested host with a login service such as Telnet or Rlogin. Note that these users don't need an IP address, since they aren't actually attaching to the network.



Network Dial In Users

These users actually pretend to be nodes, complete with addresses, on the network. They do this by using PPP or SLIP to send network packets over the phone lines. Since all IPX users attach to the network and have addresses, all IPX users are of this type.

NETServer Manager's Main Window



NETServer Manager Main Window

The main window contains a a menu bar, a toolbar, a status bar, and at least one NETServer status window.

The Status Bar

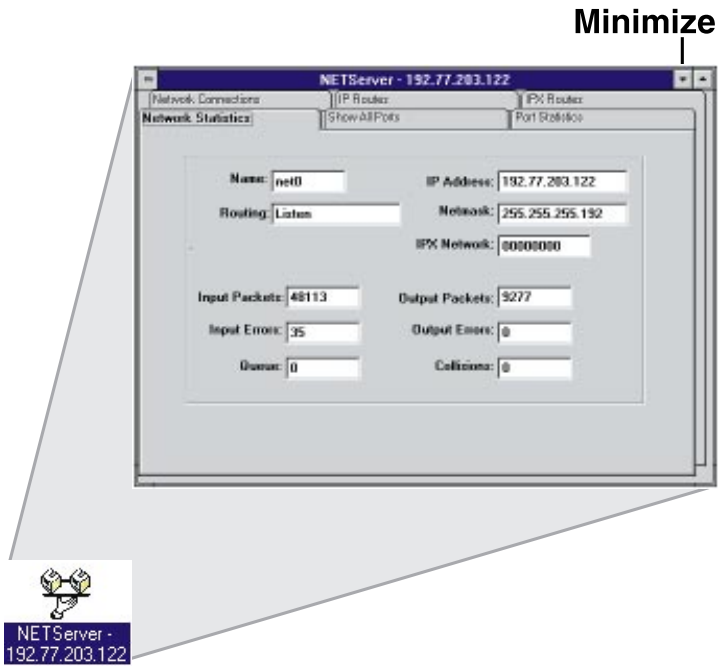
The Status Bar is located on the bottom of the application's main window. In addition to the keyboard status indicators that are standard in most Windows applications, it sometimes displays short descriptions of menus and options selected.

NETServer Status Windows

A NETServer status window will be displayed for each NETServer that the manager software is currently connected to. To open connections to additional NETServers, select Open Connection from the File menu.

Any configuration performed in NETServer Manager will affect the NETServer whose IP address is displayed at the top of the currently active status window. To switch between NETServers, click on the status window of the NETServer you wish to configure.

Note: You may wish to get the NETServers you are not currently configuring out of the way by minimizing their status windows.



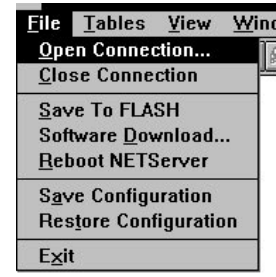
Each NETServer status window displays information on any one of six subjects (selected by clicking on the appropriate tab). These informational displays are covered in Chapter 9.

The Menu Bar

The main window has six menus: *File, Tables, View, Statistics, Window,* and *Help.*

The File Menu

The File Menu allows you to establish connections with additional NETServers as well as saving configuration to disk or to the NETServer's flash memory.



Open Connection

Select this to log into a NETServer. You can open connections to additional NETServers and keep multiple connections open as long as your system has additional TCP sockets available. See *NET.CFG setup* in Chapter 2 for information on TCP socket configuration.

Note that most windows in the Configuration Manager software will display the IP address of the NETServer you are currently configuring.

Close Connection

Click this to log off the currently selected NETServer. If you have made any changes to the NETServer's configuration, you will be asked if you want to save your changes permanently to flash memory before you exit the program. If the NETServer is rebooted before you save to flash, these changes will be discarded.

Save to FLASH

Select this to save all of your configuration changes to the NETServer's Flash memory.

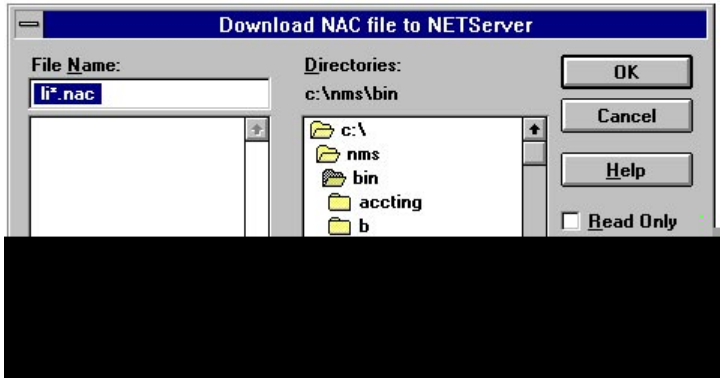
Note: When you click on a window's Save button, you are not saving to flash memory. You are saving the changes you have made to the NETServer's RAM, and if you reset the NETServer before you save the changes to flash memory, you'll lose those changes.

Software Download

This menu selection downloads a new executable image of the NETServer's system software. The file it transfers is named as follows:

de??????**.nac**	NETServer/2 firmware
pn??????**.nac**	NETServer/8 or NETServer/16 firmware
le??????**.nac**	NETServe card firmware (Ethernet)
lt??????**.nac**	NETServer card firmware (Token Ring)
li??????**.nac**	NETServer PRI card firmware

?????? is a 6 digit version number for the file. The number is divided into three groups of two digits each. So, li030122.nac is NETServer PRI version 3.1.22.



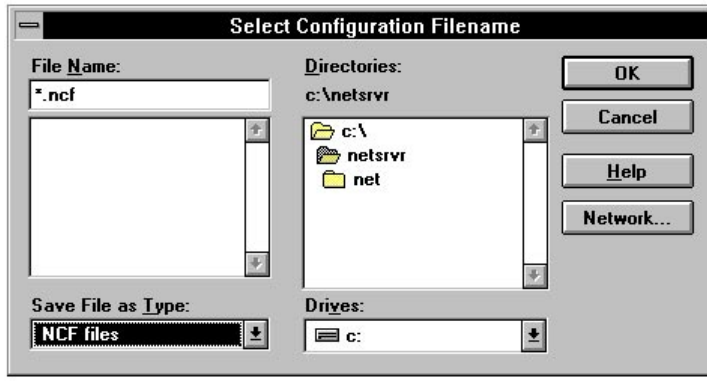
Reboot the NETServer

Select this to reboot (or restart) a NETServer from the Windows software. Note that LAN port configuration is the only configuration change which requires rebooting a NETServer.

Save Configuration

This option allows you to save a NETServer's entire configuration to your computer's hard drive. This can be extremely handy in the following instances:

1. You forget your !root password, forcing you to erase your NETServer's flash memory. Restoring a saved configuration file is the only alternative to configuring the box all over again (this is possible because the !root password is not saved).
2. You want to copy a NETServer's entire configuration to another NETServer (Save, login to the other NETServer, and then Restore).



Note that this option saves the current settings in NETServer manager. Unless you have just selected the save to flash option, these settings could be different from the actual configuration of the NETServer you are logged into.

Restore Configuration

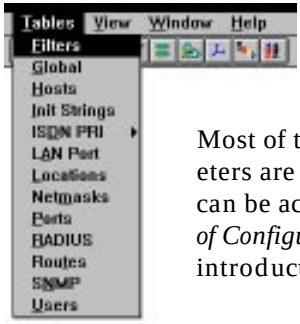
This option is used to load saved configuration files.

Exit

Select this when you want to exit the Windows management software.

If you have made any unsaved changes to a NETServer's configuration, you will be asked if want to save your changes to flash memory before you exit.

The Tables Menu



Most of the NETServer's configurable parameters are located in one of several tables which can be accessed through this menu. See *Overview of Configurable Tables*, later this chapter for an introduction to each table.

The View Menu

The View Menu has two options: Toolbar and Status Bar. By default, both should be visible (a check is beside each one). To remove either window, select on the one you

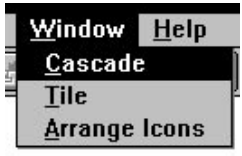
one of them from the the View Menu and click wish to deactivate.

The Window Menu

The Window Menu has three options:

Cascade & Tile — If you have more than one window open, you can select Cascade or Tile to arrange them on the window.

Arrange Icons — This options may be used to organize Program Manager icons on the window.



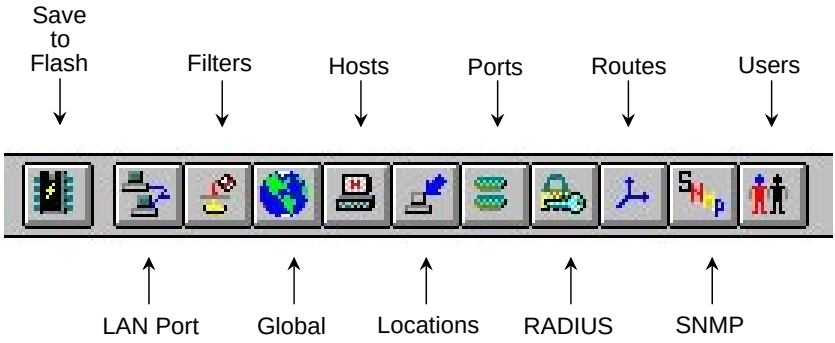
The Help Menu

This menu has three options:

Contents	Produces a contents page which allows you to search for help on specific topics.
About NETServer Manager	Brings up a short informational window about the NETServer Manager software.
Help	Tells you how to use Windows help systems like this one.

The Toolbar

The Toolbar contains several icons, the first of which saves your changes (if any) to the NETServer's flash memory.



Toolbar Icons

All the other icons on the Toolbar bring up windows that you could also select by clicking on the Tables menu. For example, if you clicked on the last icon on the right, you would bring up the User Configuration window. Selecting Users from the Tables menu would have the same effect.

Overview of Configurable Tables

This section contains a brief description of each of the NETServer's internal databases.

Filter Configuration 

The packet filters created with this option control which packets are permitted to pass through given interfaces. Packet filters created in the Filter Configuration window are used in the following Tables:

LAN Port (Net0) Configuration	To control what packets may pass through the LAN interface to the local network (output filter) or from it (input filter).
Location Table	To control what packets are received from a dial out location (input filter) and what packets are sent to it (output filter).
Ports Table	To control what hosts login users can access, or if an S-Port is set to Hardwired (dedicated serial connection), to control what packets are received through the port (input filter) and what packets are sent (output filter).
User Table	For a Login User, to control what hosts the user can access. For a Network User, to control what packets are received from the user (input filter) and what packets are sent to the user (output filter).

See Chapter 8 for additional information on packet filters.

Global Configuration 

The Global Configuration window lets you configure parameters that apply to all ports, such as the Name Service your network uses (if any), default IP and IPX route information, and so on. You can also specify which host will be the Default Host for login users to establish a session with, as well as the password for the supervisor account.

Host Configuration 

The hosts table is used to translate names of local hosts to IP addresses and vice versa. This allows users and administrators to type host names rather than addresses.

This is especially useful if the network uses IP and does not have a name service such as NIS or DNS. If your network has a name server, the NETServer tries to match the host name with an IP address using the Hosts Table before using the name server.

Note that IPX networks do not use this table since SAP provides the functionality of a name service.

Initialization Strings

Initialization strings can be sent to a modem port each time the port is reset (a port resets itself each time the modem disconnects). Initialization scripts for modems most often contain the AT commands needed to configure the modems for use in a given application.

ISDN PRI

The following two tables exist only on NETServer cards with the primary rate ISDN option. When an ISDN call comes in, the NETServer creates a virtual port for the session and configures it based on the signaling information provided by ISDN. On rare occasions, some of this information may become lost or corrupted due to problems with telco switches along the way. If you suspect that calls are being signaled improperly, you can use the two tables to force a specific configuration.

Call Mapping Table

Entries in this table allow you to dictate which service profile will be used based on the number users are dialing (DNIS), the number users are calling from (ANI), or both. The profiles themselves are defined in the Service Profile Table.

Service Profile Table

This table lets you create and configure ISDN "service profiles." Service profiles can be thought of as configuration templates for an ISDN session. Once configured, a profile can be attached to specific phone numbers (using the Call Mapping Table).

LAN Port Configuration

LAN Port Configuration deals with the LAN interface. These settings reflect how the LAN attached to the NETServer is configured and include, for example, what protocol your local network is using (IP, IPX, or both).

Location Table 

The location table stores information about remote sites that the NETServer needs to dial out to. The table is used during LAN-to-LAN routing, to tell the NETServer how to dial out to and communicate with a remote location. It is also used for dialing back network dial in users. Each location is configured with parameters such a what addresses and which protocol to use for the connection. A dial script for each location contains instructions on how to dial out to and sometimes even how to log into a remote host.

Netmasks Table

The netmasks table is used when you want to employ Classless InterDomain routing (also called Supernetting). Supernetting is a specialized IP addressing technique used by some Internet service providers. The technique requires that special netmasks be defined using the netmasks table.

See Appendix A of the NETServer *Command Reference* For more information on supernetting.

Port Configuration 

The Ports Table controls the NETServer's S-Ports (modems and the external serial port).

Port Type

Three fields determine which type of services a port will perform: User Login, Host Device, and Network Access. The default configuration is:

Host Device	Disabled
User Login	Enabled
Network	Dial In

User Login

A user login port services login users. As explained at the beginning of this chapter, login users are provided terminal access to hosts on the network, but do not actually become nodes on the network.

Host Device

Host device ports are used for IP modem sharing. A TCP port number is assigned to the modem, allowing users and applications to talk directly to its command line.

Network Access

Network ports are used for routing network (IP and IPX) packets via a serial communications protocol (PPP or SLIP). Both LAN-to-LAN routing and network dial-in users require this kind of connection. There are three types of network port: dial in, dial out, and hardwired. A fourth setting, network dial in and dial out allows the port to perform both of these functions.

Dial In Network dial in ports service network dial in users and remote routing devices that dial in to form a routing connection.

Dial Out Network dial out ports are used to initiate dial up routing connections and to dial back network dial in users.

Hardwired A hardwired port is a serial port that is connected to another device via a serial cable (this is only possible the external serial port). Note that both Host Device and User Login must be disabled on Hardwired ports.

RADIUS Configuration 

If your network has a RADIUS authentication server, the RADIUS Table lets you configure the NETServer to communicate with it (RADIUS accounting servers are configured in Global configuration).

When a user dials in from a remote site and logs in with a user name and password, the NETServer first checks to see if user is part of its Users Table. If the user is not, and the NETServer is properly configured, it will check with the RADIUS server.

Routes Table Configuration 

The routes table contains both static and dynamic routing information. Dynamic routes are updated by RIP broadcasts received from other routing devices on the network. Static routes are routes added to the table by hand. A static route to a given location will override a dynamic route that RIP generates.

Static routes to a given location are required when the location is not running RIP or when the NETServer is not listening for RIP broadcasts on the given interface. Without RIP protocol messaging, the NETServer cannot gather information on the location of other routers, gateways, and remote hosts and must know exactly where to send a packet.

SNMP Configuration 

The NETServer provides support for using the Simple Network Management Protocol (SNMP) and industry standard MIB-II variables. These variables are fully described in your MIB-II documentation.

The SNMP Configuration Table lets you configure what SNMP servers (if any) are permitted to make SET and GET requests, as well as the Read and Write Communities.

Users Table Configuration 

The User Table contains authentication and configuration information for two types of users: Login Users and Network Users. Note that you cannot have a login user with the exact same name as a network user.

Login Login users are remote users dialing in to request terminal service from an IP host. Once such a user is authenticated, he or she is connected to a host with a login service such a Telnet or Rlogin.

Network Network users are remote users dialing in to become a virtual node of the local network. Such a user may be an individual attaching to the network or an entire LAN dialing in to route packets onto the local network.

Keep in mind that entries in the user table will usually override the settings for the port the user is connected to.

Chapter 4
Terminal Server Setup

If you have workstations or terminals at a remote site that require access to a host on the local network, you can configure the NETServer to function as a terminal server.

Terminal or Workstation Setup

1. The remote user should get the following information from the NETServer's system administrator:
   - The user name and password that he or she will use.
   - The telephone number of the NETServer that the user must dial into.
   - Depending on setup, the terminal or workstation user may also need to know the IP address or name of each host he or she may log in to.
2. The dial in workstation or terminal should be configured for the following communications parameters:
   - 8 bits, No parity, and 1 stop bit
   - Hardware (RTS / CTS) flow control
   - Normal Carrier Detect
   - Hang up and reset when DTR drops

   Note that although these settings are the defaults, you can change the NETServer's communications parameters if you want to. See *Port Configuration, Communications Parameters* in Chapter 10 for more information.

NETServer Terminal Server Setup (Overview)

A. Find out what kind of terminals are being used (or what kind of terminal will be emulated). If you don't know the terminal emulation to use, you can also choose to go with standard Network Virtual Terminal emulation (ASCII only dumb terminal).

B. Make sure that the hosts support the login service(s) that you will use to log into them. Virtually all IP machines support Telnet. Rlogin is standard to most UNIX machines and has spread to some other IP machines. PortMux requires that a host have the PortMux daemon (*in.pmd*) running. A UNIX version of the PortMux daemon is available on the U.S. Robotics web site.

   A fourth service, Netdata, does not require that the host be running a "Netdata" service. Instead of talking to such a service, Netdata (also called Clear TCP) exchanges data directly with a given port number on the host. Netdata does, however, require that the specified TCP port number actually be an accessible process or device on the host.

C. Configure a port for a connection. See *Configuring a Port*, later in this chapter. This includes setting a default login service and default hosts for the port, as well as configuring a login message (banner) and login prompt. The default login message is none, or no login message. The default login prompt is *login:*.

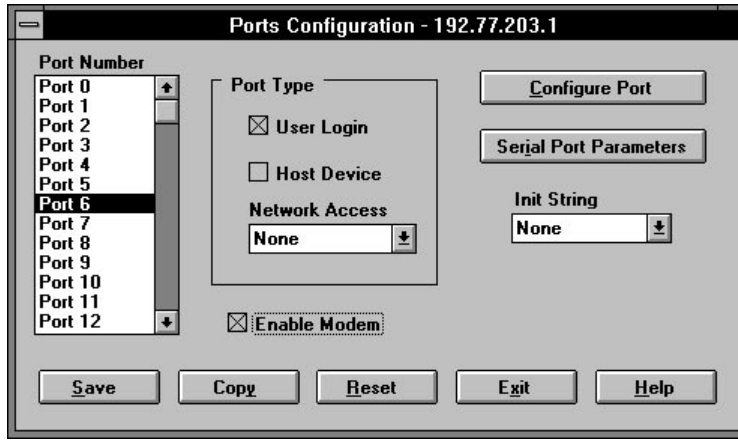
D. Create a user entry in the User Table for the remote user. See *Adding the Login User to the User Table*, later in this chapter. Login user accounts define hosts and login services for individual users.

Terminal Server (Detailed Setup)

The following section gives details on configuring the NETServer as a terminal server from Windows.

Configuring a Port

To be used for terminal service, a port must be configured for User Login. Select *Port* from the Table menu. The Port Configuration window appears. Select (click on) the port you want to configure from the list on the left side of the window.



Port Configuration window

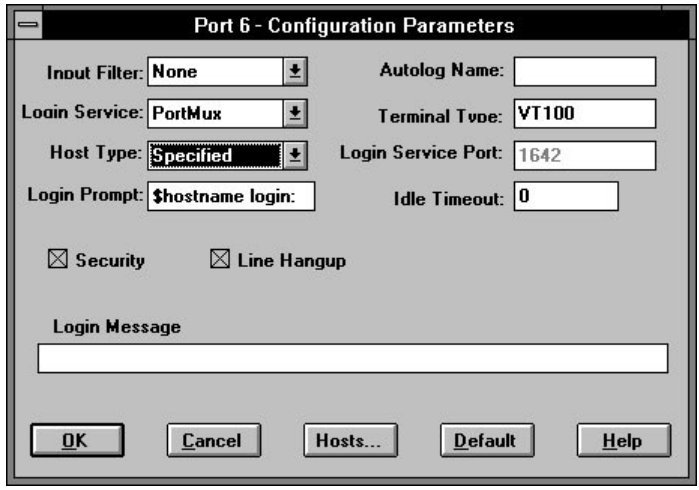
Step 1 - Enable the modem (NETServer card only)

Packet bus quad modems in the Total Control Chassis must be enabled before they can be used. To do this, click on the *Enable Modem* box. This option will not appear on non-packet bus ports.

Step 2 - Set the port type to User Login

Enable User Login on the selected port by clicking on the appropriate box under *Port Type*. Note that you will not be allowed to do this if Network Access is set to Hardwired.

Click on the *Configure Port* button. You will now see the Login Parameters window. Note that the appearance of this window varies since it displays only the options for the port type or types you have selected.



Login Port Parameters

Step 3 - Configure security (Pass-thru login)

The check box marked *Security* determines what the NETServer will do with users who are not in its User Table.

Checked — Check with the RADIUS security server (if present). The connection is terminated for all users who are not in either the NETServer's user table or the RADIUS database.

Not Checked — Do not consult RADIUS. Pass a user not in the NETServer's user table on to the default host for the port he or she is connected to.

Step 4 - Create default user settings for the port

If you disabled security in Step 3, port defaults *must* be set to tell the NETServer what to do with users not in the user table. If Security is enabled, these settings are optional.

Port Default - Login Service

The NETServer uses the service specified here to connect users not in its user table with a host. The setting is only used if the Security box is not checked. Note that a dial in terminal or workstation does not need to know how to use this service since it talks directly to the NETServer, not the host.

Telnet Supported by most TCP/IP computers, Telnet lets the user log in to hosts that support it. If you set a terminal type (see *Term Type* below), Telnet will pass that information along. Otherwise, it negotiates a standard, Network Virtual Terminal interface.

Rlogin Although Rlogin was originally a (BSD) UNIX only protocol, it is now supported by some non-UNIX machines as well. Unlike Telnet, Rlogin allows a user logged into a host to access their accounts on other (trusted) hosts without reentering a password. Rlogin requires that you specify a terminal type. See *Term Type* below.

PortMux (Default) PortMux multiplexes many Telnet sessions into a single data stream that's more efficient to transmit and requires fewer connections. PortMux requires that the host be running a special PortMux daemon (in.pmd). A UNIX version of the PortMux daemon is available on the U.S. Robotics web site. Note that this daemon also allows the host to use NETServer ports set to Host device as pseudo TTYs (see Chapter 7).

Netdata Unlike Telnet, Rlogin and PortMux, Netdata is not actually a login service. Netdata is a clear TCP socket interface to the TCP port specified in the Login Service Port field. 8-bit data is relayed with no intermediate processing. This is the preferred setting for applications that require a socket interface.

Port Default - Host Type

This is the host for users whose user table entries contain a host type of *Default*. If Security was not checked in step 3, this is also the host for users not in the user table. Host Type can be set to *Default*, *Prompt*, or *Specified*.

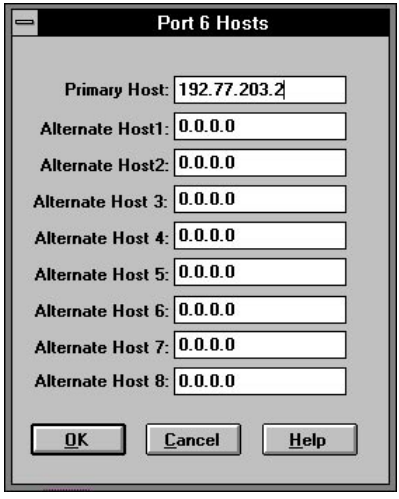
Default (Default) Users are passed on to the Default Host defined in the Global Configuration table. If the Global Default Host is not available, users are passed on to one of the Global Alternate Hosts (if specified).

Prompt As soon as a user connects with the NETServer, he or she is given a *Host:* prompt. Users type the name or IP address of the host they want.

> **Note:** Since the host prompt appears before the login prompt (before the NETServer knows who the user is), even users who have a host specified in the user table will be prompted for a host. However, a host specified in the user table will always override the value entered here.

Specified Users are connected to a specific host other than the global default. If you select this option, you must enter the address of the port default host and each of the port alternate hosts you wish to use. To do this, click on the Hosts button. The Hosts window appears:

Hosts window



Port Default - Terminal Type:

This sets the login user's TERM environment variable (what kind of terminal is being used) for the session. Each UNIX host has a list of possible values for this field in either its termcap or its terminfo database. Select the terminal type that best suits the terminal(s) that will be used.

Specifying a terminal type is only required if Login Service is set to Rlogin. However, Telnet and PortMux will also use term type info if it is provided. If no terminal type is entered, Telnet and PortMux assume dumb terminal mode (standard network virtual terminal).

Step 5 - Optional Friendly Stuff

The following two parameters allow you to customize the port's printed response to dial in users.

Login Message

In this field, you can enter a message (banner) that users will see prior to login. The login message can be up to 240 characters in length and does not need to be surrounded by quotation marks (if you use quotes, they will be included in the message). Use the carat (^) to designate the start of a new line.

Example:

U.S. Robotics^NETServer

Login Prompt

You can also enter a customized login prompt for each port. If you put the word *$hostname* in the prompt, the NETServer will substitute the name of the port's default host. The default prompt for user login ports is *$hostname login:*. If you use quotation marks, they will be included in the prompt.

Note: Many automated login scripting systems expect a login prompt to end in ***login:***. Putting any character after the colon (including quotation marks!) will cause some login scripts to crash.

Step 6 - Save your work

Click OK to return to the Port Configuration window

With the port you just configured selected, Save your changes by clicking on the Save button. Then, reset the port by clicking on the Reset button.

Note: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes permanently. To save the changes permanently to flash memory from Windows, you must select Save to FLASH from the File menu.

Adding a Login User to the User Table

Users for terminal server applications are configured as login users. Select User from the Tables menu. The User Table Configuration window appears:

Step 1 - Create a new User Table entry

Click on the New button. The Network User Parameters window appears. This is the default type of user.

Click on User Login to change the User Type. The window changes to display Login User Parameters.

Login User Parameters Window

Enter a User Name

Type the name of the remote user in the *User Name* field. If the user's Login Service will be set to Rlogin, the user name must be the same as the user's name on the UNIX host to be logged into.

Set the User's Password

Click on the Password button.

The *User Password Validation* box appears. There are two blank fields to type the password in. Type the password in the first field. Then press the Tab key or click on the second field to advance the cursor. Type the password again. When finished, press the Enter key or click on the OK button.

Step 2 - Configure the user

You must specify a login service for each user. Specifying a host for each user is optional if you have either a port default or a global default host defined.

Login Service

The NETServer uses the service specified here to connect with the host. Note that the remote terminal or workstation does not need to know how to use this service since it talks directly to the NETServer, not the host.

Telnet (Default) Supported by most TCP/IP computers, Telnet lets the user log in to hosts that support it. If you set a terminal type for the port, Telnet will pass this information on to the host, otherwise, it will negotiate a standard Network Virtual Terminal connection.

Rlogin Although Rlogin was originally a (BSD) UNIX only protocol. It is now supported by some non-UNIX machines as well. Unlike Telnet, Rlogin allows a user logged into a host to access their accounts on outer (trusted) hosts without reentering a password. Rlogin requires that you specify a terminal type for the port.

PortMux PortMux is similar to Telnet except that it multiplexes many Telnet sessions into a single data stream that's more efficient to transmit and requires fewer connections. PortMux requires that the (UNIX) host be running a special PortMux daemon (in.pmd), which is available on the U.S. Robotics web site. Note that this daemon also allows the host to use NETServer ports set to Host device as pseudo TTYs (see Chapter 7).

Netdata Unlike Telnet, Rlogin and PortMux, the Netdata client does not need a corresponding server on the host Netdata is a direct connection to the TCP port number specified in Access Port . No intermediate processing is performed. The NETServer will simply relay all data directly from the login user to the destination port and vice versa.

Access Port

This is the TCP port number that the login service will access on the host. You do not have to set this unless you choose Netdata as the login service.

Host

This tells the NETServer which host the user will be logging in to. The options are *default*, *prompt* or a specified IP address

Default (Default) The user is passed on to the default host for the port he or she is connect to.

Prompt The user is given a *Host:* prompt. Users type the name or IP address of the host they want.

Note that if the port default host type is also prompt, the host prompt appears before login. Otherwise, the host prompt appears after login.

Specified The user is connected to a specific host other than the default host. Type in the IP address of the specific host.

Step 3 - Configure for dialback use?

Normally, after a user enters his or her user name and password, the connection to the host proceeds. When a dialback user enters his or her user name and password, the NETServer hangs up and dials the user back. To configure a dialback user, click on the Dialback button in the upper-right corner of the window and then enter a value in the Dialback Number box.

Dialback Number

The dialback number can be any valid string of up to 32 characters. If you want to use AT commands in this string, begin the string with "AT". Otherwise, the NETServer will expect only a phone number.

The two lines below actually do the same thing. The difference is that other AT commands could also be inserted in the second line.

5551000
atdt5551000

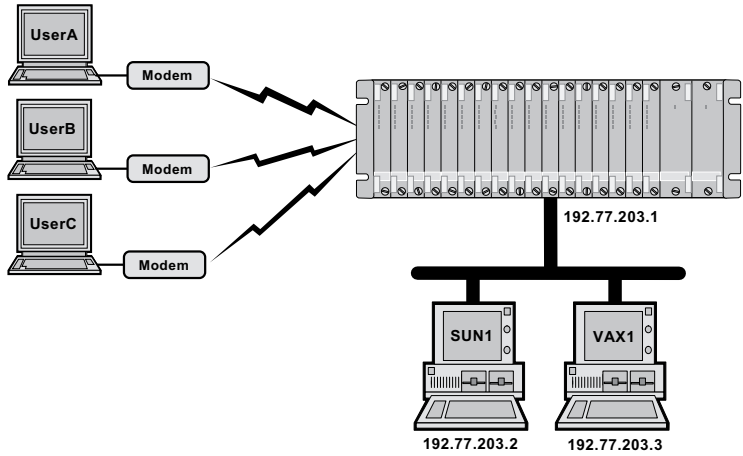
Step 4 - Save your work

When finished, click on the OK button to return to the User Table Configuration window. Save your changes by clicking on the Save button.

Note: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes permanently. To save the changes permanently to flash memory from Windows, you must select Save to FLASH from the File menu.

IP Terminal Server Case Studies

The following examples set up users to log into the two hosts in the illustration below



IP Terminal Server - Case Studies

Example 1

UserA, UserB, and UserC are all Login Users with entries in the user table. An application on VAX1 is connected to a dial-up information database that is open to the public (those not in the user table).

Before you begin

Make sure the NETServer is properly configured.

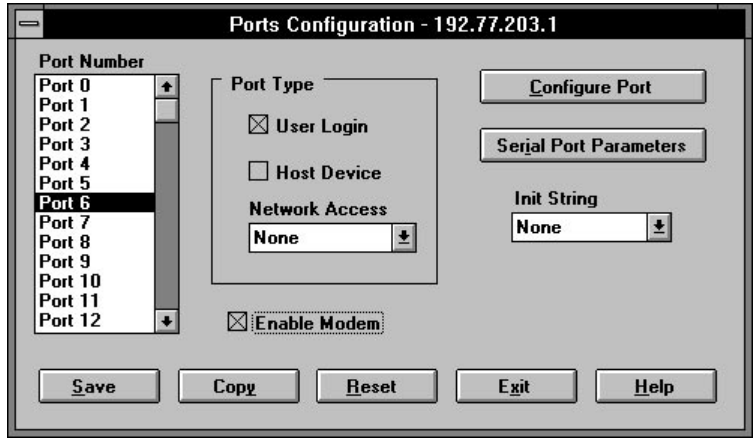
- the NETServer must have an IP address assigned to its LAN port
- the NETServer's LAN port netmask must match the one being used on the local network.

See *LAN Port Configuration* in Chapter 10 for instructions on how to set these parameters.

This example also assumes that SUN1 is the NETServer's global default host. To configure this, select Global from the Table menu. When the Global Configuration window appears, click on the Hosts button. Type 192.77.203.2 in the Primary Host box and then click OK. When you return to the Global Configuration window, Click Save.

Port Setup

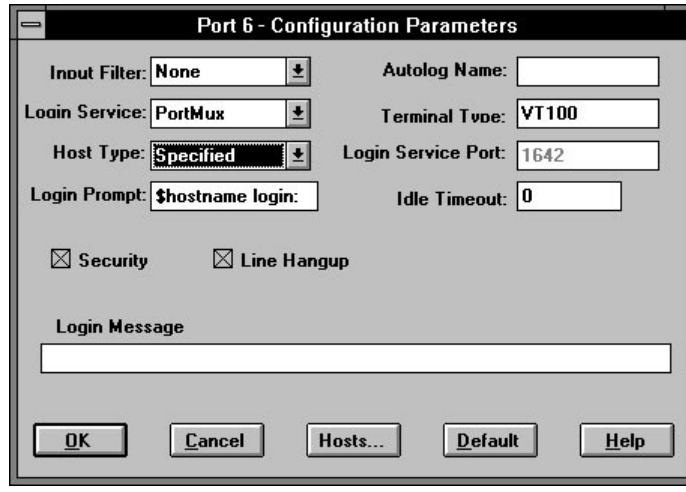
The NETServer will ports 6, 7 and 8 for this application. Select Ports from the Table menu. The Port Configuration window will appear.



Port Configuration (Example)

1. Select port 6 by clicking on it in the Port Number box
2. Since our example illustration shows a NETServer chassis, port 6 must be connected to the packet bus. Click on the Enable Modem box. Note that this step is not necessary on other NETServer platforms.
3. To configure the port type, enable user login, disable Host Device and set Network Access to None.

4. Click on the configure port button. The Configuration Parameters window appears:



Port 6 will be used exclusively by users who already have user accounts. We want the NETServer to perform its own security checks and hang up on anybody not in the User Table or in the RADIUS server's database. Note that since we have three user accounts but only two ports used for this purpose, only two of the three users may be logged in at any one time.

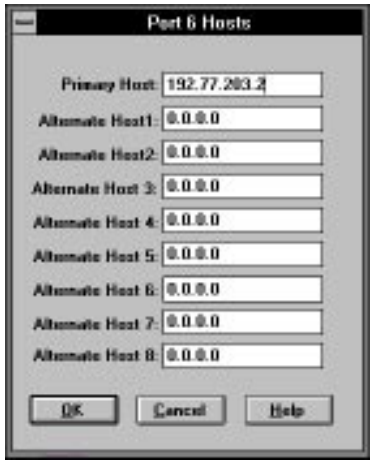
5. Disable pass-thru login by clicking on the Security box.

Users will be logging in with terminals emulating VT100s. Note that since Security is enabled, the Login Service shown in this window is unimportant (it will never be used).

6. Enter VT100 in the Terminal Type box.

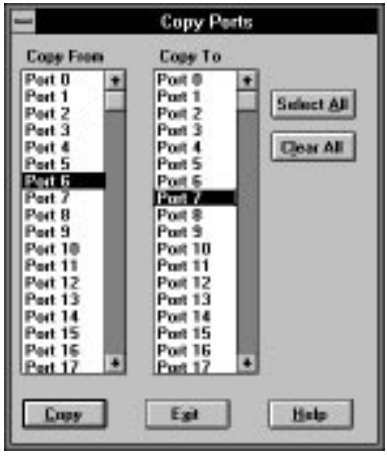
Users connecting to this port will be logging into SUN1 unless their user table entries specify a different host. SUN1 also happens to be the NETServer's global default host.

7. Set the Host Type box to Specified.
8. Click on the Hosts button. The Port Hosts box appears.
9. Type 192.77.203.2 in the Primary Host box. Click OK.



Note: Since SUN1 is the global default host, an alternative to entering a primary host for the port is to simply set the Host Type box to Default.

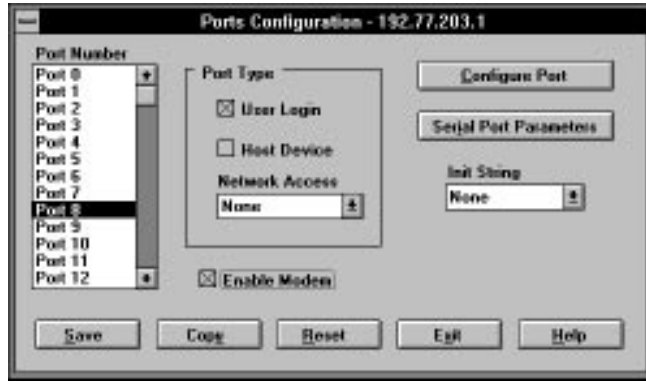
10. When the Port Parameters window reappears, Click OK.
11. With Port 6 still highlighted in the Port Configuration window. Click Save to save its configuration. Then click Reset.



Since Port 7 will be used for the same application, its configuration will be identical to Port 6.

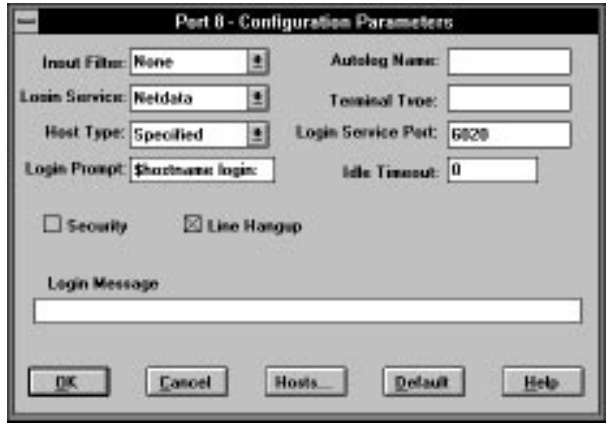
12. Click on the Copy button. The Copy Ports window appears.
13. Select Port 6 on the left and Port 7 on the right.
14. Click Copy
15. Click OK to return to the Port Configuration window

Port 8 will be used as a public information line. We want anybody to be able to dial into it.



16. Enable the modem and set the port type as shown above.

17. Click on the Configure Port button. The Port parameters window appears:



18. Allow users not in the user table to connect to a host. To do this, make sure the Security box is *not* selected.

Users connecting to the info line will form a socket connection to a database application running on VAX1 and will have no other access to VAX1. Note that since Netdata is a socket interface rather than an actual login service, it will not relay terminal type information to the host. Instead, it will relay exactly what the application outputs.

19. Select Specified in Port 1's Host Type box. Click on the Hosts button and enter VAX1's IP address (192.77.203.3) in the Primary Host box. Click OK
20. Set the Login Service box to Netdata.
21. In the Login Service Port box, enter the TCP port number of the application users will be connected to (In this case, we'll say it's at Port 6020).
22. Click OK.
23. When the Port Configuration window reappears, Click Save and then Reset.

User A Setup

User A will be logging in to SUN1 with Rlogin. Since SUN1 is the port default host, User A needs only a User name, a password and a login service in the User Table.

1. Select User from the Tables menu. The User Table Configuration window appears. Click on the New button. The Network User Parameters window appears.
2. Click on User Login to change the User Type. The window changes into the Login User Parameters window.

Setup for User A

4. Type UserA in the Name box.
5. Click on the Password button.

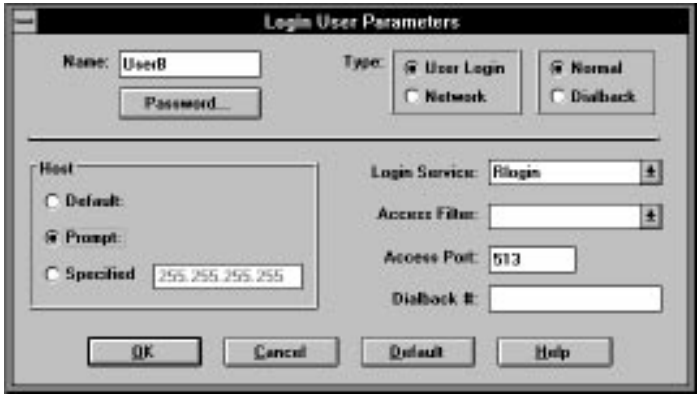
When the *User Password Validation* box appears, type the password *UserAPw* in the first field and then click on the second password field. Verify by typing *UserAPw* a second time. Click OK to exit the Password window.

6. Select Rlogin in the Login service box
7. Click OK.

User B Setup

User B can log into either SUN1 or VAX1. After he or she types the correct user name and password, User B will be prompted for a host name or IP address.

1. Click on the New button.
2. When the Network User Window appears, click on User Login to change the User Type. The window changes into the Login User Parameters window:



User B Setup

3. Type UserB in the Name box.
4. Click on the Password button. When the *User Password Validation* box appears, type the password *UserBPw* in the first field and then click on the second password field. Verify by typing *UserBPw* a second time. Click OK to exit the Password window.
5. Select Prompt (by clicking on it) in the Host box.
6. Select Rlogin as the login service.
7. Click OK

User C Setup

UserC is a dialback user. When he or she enters the correct user name and password, the NETServer will hang up and dial the user back at 9, 555-1000. User C will use the port default host (SUN1).

1. Click on the New button. The Network User Parameters window appears.
2. Click on User Login to change the User Type. The window changes to display Login User Parameters.

User C Setup

3. Type UserC in the Name box.
4. Click on the Password button. When the *User Password Validation* box appears, type the password *callmeback.* Verify by typing it a second time. Press Enter or Click OK when you are finished.
5. Click on the Dialback button in the upper right corner of the window and Enter 9,555-1000 in the Dialback Number box.
6. Select a Login Service of Rlogin
7. Click OK.

Save your work

Click on the Save Button.

Example 2

Suppose you have a lot of potential users, but only a couple of hosts, each of which has its own login security already set up for each of its potential users. It may be easier to assign generic user names for each host and let the hosts take care of user authentication. In this example, SUN1 is a generic user name for users of a Sun host. VAX1 is a generic user name for users of a VAX host.

1. From the Table menu, Select Ports
2. Select Port 6, enable User Login, enable the modem, and then click on the Configure Port button.
3 Enter *Which Computer?* in the Login Prompt box and enable security.
4. Click OK.
5. When the Port configuration window reappears, click Save and then Reset. Close the Ports window.
6. Select Users from the Table menu
7. Click on the New button. The Network User Parameters window appears.
8. Click on User Login to change the User Type. The window changes to display Login User Parameters.
9. Type SUN1 in the Name box. *Do not Enter a Password!*
10. Click Specified in the Host box and enter SUN1's IP address (192.77.203.2).
11. Select Telnet in the Login Service box.
12. Click OK.
13. Click on the New button. The Network User Parameters window appears.
14. Click on User Login to change the User Type. The window changes to display Login User Parameters.
15. Type VAX1 in the Name box. *Do not Enter a Password!*
16. Click Specified in the Host box and enter VAX1's IP address (192.77.203.2).
17. Select Telnet in the Login Service box.

18. Click OK.

19. Click on the Save button.

When dialing into the NETServer, the user receives a “Which Computer” prompt. If the user enters SUN1, a connection is established with the Sun, which proceeds to authenticate the user with its own security information. Since no terminal type has been defined either port, all users will be defaulted to dumb terminal emulation. The same would be true of the VAX.

Chapter 5
Network Dial In Access

Network dial-in users establish PPP or SLIP connections with the NETServer and the local network. Unlike the dial in users covered in the previous chapter, this kind of user is connecting to the network as a virtual node rather than simply acting as an input/output device (terminal) for an existing network node. IPX dial in users are all of this type.

Dial In User Setup

The instructions below are required by all remote users dialing in to the NETServer.

1. The remote user's computer must have communications software that supports PPP or SLIP connections.
2. A PPP or SLIP protocol driver must be loaded on the remote user's computer for PPP or SLIP connections.
3. Set the user's modem (or ISDN terminal adapter) to 8 data bits, No parity, and 1 stop bit.

> **Note:** These are the default settings only. If you want to, you can change what communications settings the NETServer uses on each port. See *Port Configuration, Serial Communications Parameters* in Chapter 10.

NETServer Setup for Network Dial In (Overview)

These steps configure a NETServer for users to dial in to.

> **Note:** This is a special case of LAN-to-LAN routing in which the dial in network has only one node (an end user). For an additional perspective on how the NETServer handles Dial In, you may wish to study Chapter 6.

Prework

Get the following information (Note that not all fields apply to all applications):

IP parameters

- The dial in user's IP address.

  Note that if the dial in user's IP address is not important, the NETServer may be told to simply assign a PPP user an address each time he or she dials in. PPP addresses can also be negotiated by the NETServer and the dial in user's machine.
- The connection protocol (PPP or SLIP) that the dial in user will employ.
- The dial in user's netmask.
- The dial in user's Maximum Transmission Unit (MTU, the largest packet size that the system will transmit) if applicable; both local and remote MTUs must match.
- Whether or not the dial in user is configured for Van Jacobson compression.

IPX parameters

IPX remote access sessions must use the PPP protocol and an MTU of 1500. Note that when you assign an IPX Network number to the user, the NETServer will automatically set these things for you. Get the following information:

- A unique IPX Network Number that will represent the link between the remote user and the local network for the duration of the connection.

Configuration

A. Configure at least one port for a network dial in connection. See *Configuring a Port*, later in this chapter, for details.

   Optional Port Configuration: Create a login message (banner) that the user will see before logging in ("Hi", "Welcome", "Login or go away!", etc.). By default, there is no such message. You can also customize the login prompt.

B. Decide whether the dial in user is a normal user or a dialback user. If the he or she is a dialback user, you must create a Location Table entry for that user.

> **Note:** Configuring the Location Table is not covered in this chapter. For detailed information on the Location table see Chapter 10. For a Location Table walk-through, see *Adding a Remote Device to the Location Table* in Chapter 6.

C. Create an entry in the User Table for each dial in user. See *Adding a Remote User to the User Table*, later in this chapter.

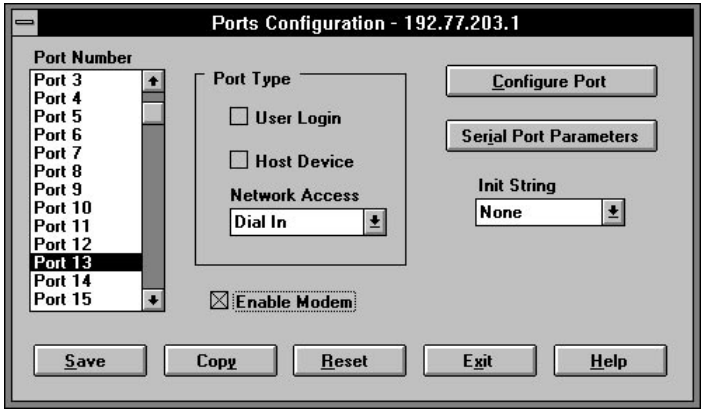
NetServer Dial-In (Detailed Setup)

To set up the NETServer software for this application, you must do the following:

- Configure at least one port
- Add users

Configuring a Port

Ports used for this type of dial in access should be configured as Network ports that allow dial in. Select Port form the Table Menu. The Port Configuration window appears:



Step 1 - Enable the modem (NETServer card only)

Packet bus quad modems in the Total Control Chassis must be enabled before they can be used. To do this, click on the Enable Modem box. This option will not appear on non-packet bus ports.

Step 2 - Port Type

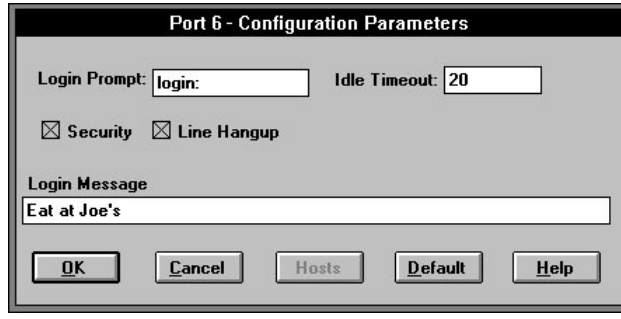
Usually, ports used for this application should be configured as network dial in ports (set the Network field to Dial In). If you will be configuring dialback users or will also be using the port for dial out routing, set the Network field to Dial In & Dial Out.

Hardwired: It's also possible to connect a user directly to the external serial port (Port 1, on the NETServer/2, Port 0 on all other NETServers) via a serial cable. In this case, you might set the port to network hardwired. Since this port is the only serial port that can be directly attached to a serial cable, it is the only port for which this setting is valid.

If you configure the external serial port as a hardwired port, set the following parameters and go to Step 5 (For an explanation of these parameters see *Ports Table, Hardwired Port Parameters* in Chapter 10).

- IP Address
- Netmask
- Routing
- Compression
- IPX Network Number
- Protocol
- MTU

Click on the Configure Port button. You will now see the Login parameters window. Note that the appearance of this window varies since it displays only the options for the port type or types you have selected.



Network Dial In Port Parameters

Step 3 - Optional friendly stuff

The following two parameters allow you to customize the port's printed response to dial in users. Note that Hardwired ports do not use these settings:

Login Message

In this box, you can enter a message (banner) that users will see prior to login. the message can be up to 240 characters in length and does not need to be surrounded by quotation marks (if you use quotes, they will be included in the message). Use the carat (^) to designate the start of a new line.

Login Prompt

You can also customize the login prompt for each port. The default prompt for network dial in ports is *login:*. If you use quotation marks, they will be included in the prompt.

Note: Many automated login scripting systems expect a login prompt to end in *login:*. Putting any character after the colon (including quotation marks!) will cause some login scripts to crash.

Step 4 - Dialback users on this Port?

If dialback users will be dialing into this port, it is a good idea for the NETServer to be able to use the same port for dial out. This makes sure that a dial out port will be available to dial the user back. Part of this was done in step 2, when you setup the port as Network Dial In & Dial Out. The other thing that needs to be done for a dial out port is assign the port to a dial group. Enter a number between 0 and 99 in the Dial Group box of the port you wish to configure.

Note: The Dial Group box only appears if you have enabled dial out on the port.

Step 5 - Save your work and reset the port

With the port you just configured selected, save your changes by clicking on the Save button. Then reset the port by clicking on the Reset button.

Note: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes permanently. To save the changes permanently to flash memory from Windows, you must select Save to FLASH from the File menu.

Adding a Network User to the User Table

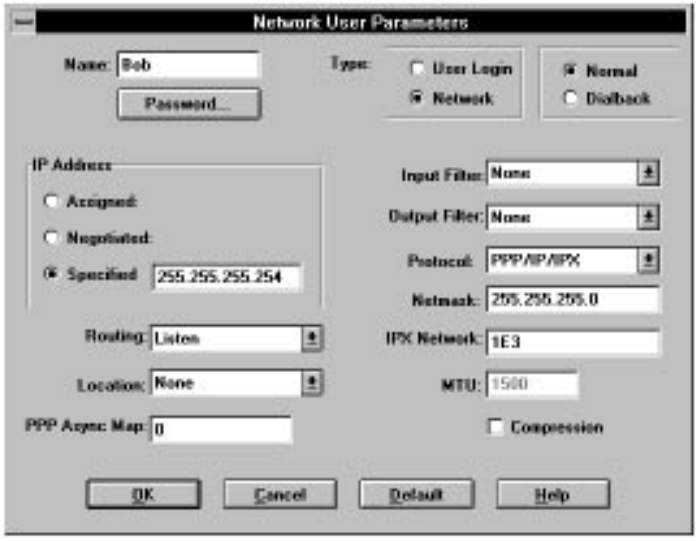
Note that User Table entries do not need to be created for Hardwired ports. Hardwired ports do not use this table.

Step 1 - Create a new user

Select User from the Tables menu. The User Table Configuration window appears. Add the dial in user to the User Table:

a. Click on the New button.

b. The Network User Parameters window appears. This is the default type of user. Type a User Name in the Name field.



Network User Parameters Window

c. Click on the Password button to set the user's password.

The User Password Validation box appears. There are two blank fields to type the password in. Type the password in the first field. Then press the Tab key or click on the second field to advance the cursor. Type the password again . When finished, press the Enter key or click on the OK button.

Step 2 - Normal or dialback user?

Normal users dial in and immediately initiate a session with the network. When a dialback user dials in and types his or her user name and password, the NETServer hangs up the line and calls the user back. This can be useful if you want to reverse charges on the phone bill.

If you are configuring a normal user, go to step three. Dialback user configuration

a. Click on the dialback button in the upper right corner of the Network User window.

b. If you have not already done so, you must create a location table entry that the NETServer will use to dial out to this user. A description of the location table can be found in Chapter 10. A location table walk-through can be found in Chapter 6 under *Adding a Remote Device to the Location Table.*

c. Once you have created the location table entry, return to this user table entry, pull down the location menu, and select the correct location.

d. Since configuration for dial out connections is handled by the location table, no further information needs to be added to a dialback user table entry (you can skip to step 4).

Step 3 - Add configuration information for the user

You must set the following parameters. All other parameters are optional.

IP Address

This is the dial in user's IP address for the duration of the connection. This address can be selected in three different ways.

Assigned	The user is dynamically assigned an address from a pre-defined pool of IP addresses. This requires that an Assigned Address pool be defined (See *Global Configuration* in Chapter 10).
Negotiated	PPP connections only. The NETServer tries to learn the dial in user's IP address using IPCP address negotiation.
Specified	The user has a fixed IP address, which is specified here.

IPX Network

If the dial in user wants to talk IPX, the connection between the NETServer and the dial in user must have an IPX network number assigned to it just like any cabled connection would. Note that this number must be unique (not already used) on the NETServer's LAN and also must be unique to whatever network the dial in user may be connected to.

Protocol

Select the protocol that the dial in user will use for the connection (PPP or SLIP). PPP has three options: PPP / IP, PPP / IPX, PPP / IP / IPX. SLIP is IP only. Select the one that reflects the network protocol that the local and remote systems are using (IP, IPX, or both).

> IPX remote access sessions require the PPP protocol.

MTU

The Maximum Transmission Unit specifies the size of the largest packet that may be sent to the user. IPX connections will discard larger packets. IP connections will fragment larger packets prior to transmission. Normally, this should be set to the largest value that both the user and your local network can handle.

Valid PPP MTUs range from 100 to 1500 (default is 1500). Note that PPP allows a remote user's system to negotiate a smaller MTU if needed. Valid SLIP MTUs range from 100 to 1006 (default is 1006)

> IPX remote access connections require an MTU of 1500. If you have entered an IPX network number, the NETServer will set this to 1500 automatically.

Netmask

Type in the dial in user's IP subnet mask.

Routing

Set the level of RIP messaging that the NETServer will exchange with the dial in user during the connection.

broadcast	Send dynamic routing information to the dial in user (but do not listen)
listen	Listen for dynamic routes received from the dial in user (but do not broadcast)
broadcast & listen	Do both of the above
off	Do not send dynamic routing information. Ignore dynamic routes received

Compression

If using SLIP, enable Van Jacobson IP header compression only if both networks use CSLIP (compressed SLIP).

If compression is enabled for a PPP connection, the NETServer will attempt to negotiate for compression, but will not use it if the remote site does not support compression.

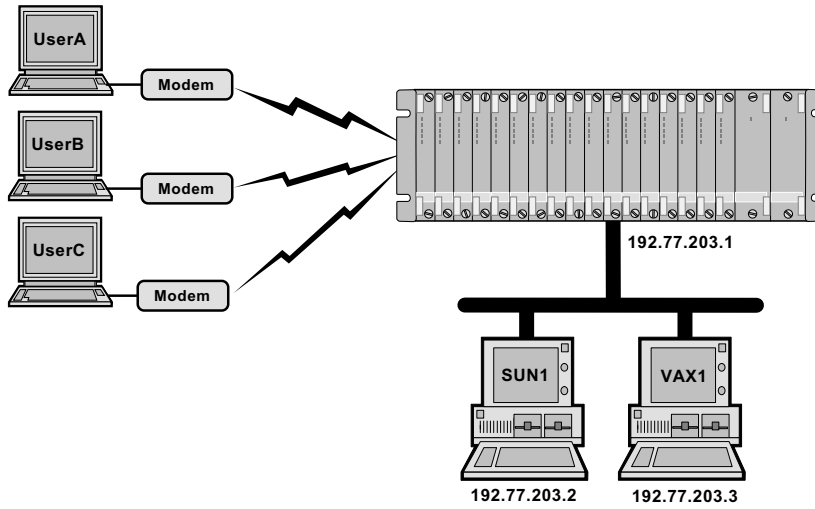
Step 4 - Save your work

When finished, click on the OK button to return to the User Table Configuration window. Save your changes by clicking on the Save button.

Note: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes to flash memory. To save the changes permanently to flash memory from Windows, you must also select Save to FLASH from the File menu.

IP Remote Access Case Study

UserA, UserB and UserC will be dialing to connect with the local network. UserC will be a dialback user.



IP Remote Access Case Study

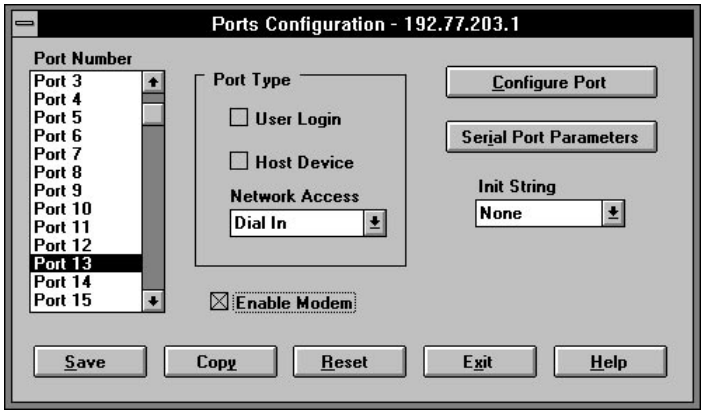
This case study assume the following:

- The configuration will take place from the Windows management software.
- The NETServer has the correct LAN port IP address and subnet mask
- The NETServer is set to the factory defaults on all other settings.

Configure the ports

This example will use Ports 13 and 14 to answer calls from dial in users. The internal modem will also be used to dial out.

a. Select Ports from the Table menu. The Port Configuration Window appears.



Network Dial In Port Setup (Example)

b. Select Port 13 by clicking on it in the Port Number box.

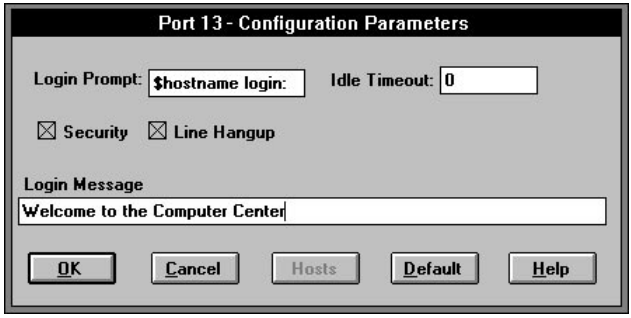
c. If the Enable Modem box appears (NETServer card only), make sure it's checked. This connects Port 13 to the packet bus.

d. Turn User Login and Host Device off.

> **Note:** It is not strictly necessary to disable User Login and Host Device. A port can be configured to serve several purposes. However, our example assumes that you don't want people using the port for anything other than the given application.

e. Set the Network Access field to Dial In.

f. Click on the Configure Port button. The Dial In Port Parameters Window appears:



Configuration for Port 13

When users connect to the port, the NETServer will greet them.

g. In the Login Message box, type Welcome to the Computer Center.

h. Click OK.

i. When the Port Configuration windows reappears, click Save and then Reset.

The dialback port

Since User C will be a dialback user, the NETServer will need to use one of its ports to dial out.

a. Select Port 14 from the list on the left edge of the window.

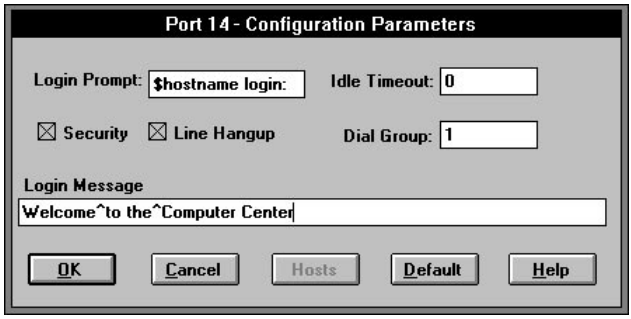
b. Enable the modem.

c. Disable User Login and Host Device.

d. Set Network Access to *Dial In & Dial Out*.

e. Click on Configure Port, the Dial In and Dial Out Port Parameters window appears.

f. Type *Welcome^to the^Computer Center* in the Login Message box. Although the greeting says the same thing as the other port's greeting does, Port 13 will write it all on one line, while Port 14 will split it up over three lines.



Notice that this window contains one parameter more than the Dial In Port Parameters window. A Dial Group of modems must be assigned to each dial out location to tell the NETServer which modems it can use to dial out with. Before you can assign such a group to a location, you must create the group here in the Ports Table.

g. Only Port 14 has been configured for dial out. To assign it to a dial group. Enter a dial group number in the Dial Group box. In this case, let's use the number 1.

h. Click OK.

i. When the Port Configuration window reappears, Click Save and the Reset.

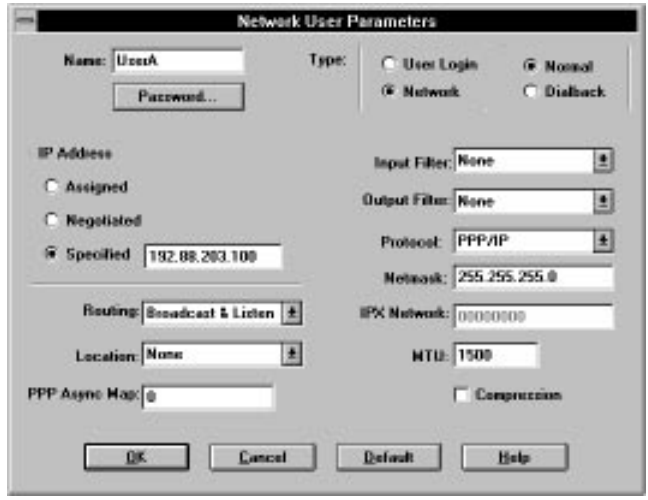
j. Close the Port Configuration Window.

Create User Table entries for the Dial In users

Select User from the Table menu.

User A Configuration

a. Click on New. The Network User Parameters window appears.



User A Setup

b. Click on the Name field. Enter the name *UserA*.

c. Click on the Password button. Enter the password *userApw* twice and then click OK.

d. Under IP Address, select Specified. Click on the IP address field next to *Specified* and enter *192.88.203.100*.

e. Enter *255.255.255.0* in the Netmask box.

f. Select *PPP/IP* in the Protocol box.

g. Enter an MTU of *1500*.

h. Pull down the Routing menu and select *Broadcast & Listen*.

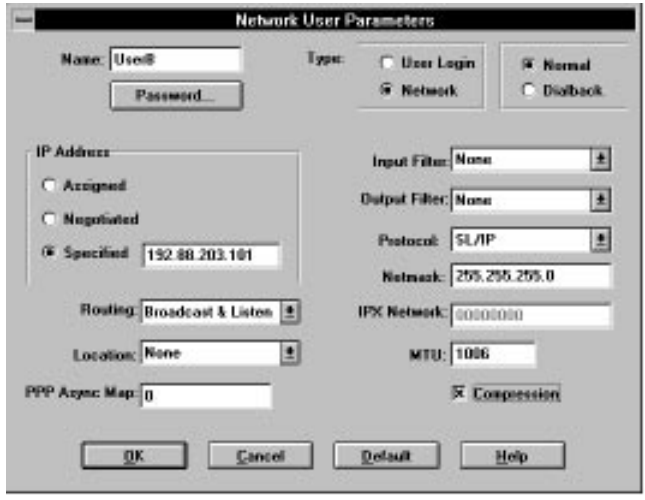
i. Click OK.

User B Configuration

User B will be configured to use CSLIP (Compressed SLIP)

a. Click on New.

b. Click on the Name field. Type the name *UserB*.



c. Click on the Password button. Enter the password *userBpw* twice and then click OK.

d. Under IP Address, select *Specified*. Click on the IP address field next to Specified and enter *192.88.203.101*.

e. Enter *255.255.255.0* in the Netmask box.

f. Select *SLIP* in the Protocol box.

g. Click on the compression box.

h. Enter an MTU of *1006*.

i. Pull down the Routing menu and select *Broadcast & Listen*.

j. Click OK.

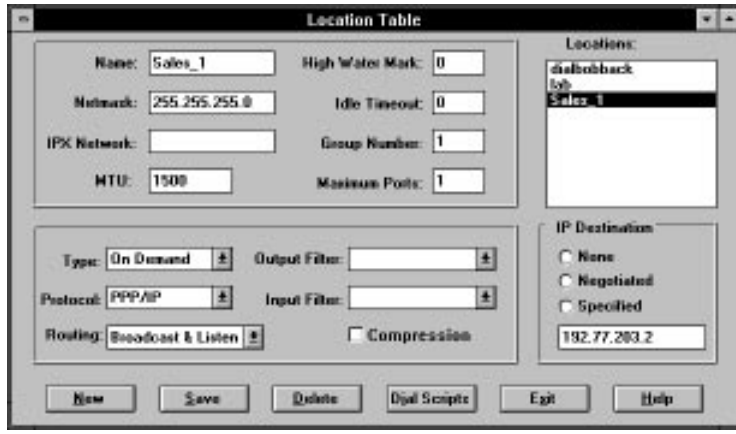
Create a Location Table entry for the Dialback user

The NETServer dials out to a dialback user. Dial out connections are handled by the Location Table. Although the User Table is not consulted for dial out, dialback users still need a (very simple) User Table entry for authentication purposes. However, the location table entry should be created first.

a. Go to the Location Table window by selecting Locations on the Table menu or by clicking on the Locations button in the Toolbar.

b. Click on New.

c. Enter *Sales_1* in the Name field.



Dialback Location Setup

d. Select *On Demand* in the Type field.

e. Select *specified* in the IP Destination box and then enter an address of *192.77.203.102*.

f. Enter *255.255.255.0* in the Netmask field.

g. In the protocol box, select *PPP/IP*.

h. Enter an MTU of *1500*.

i. In the Routing box, select *Broadcast & Listen*.

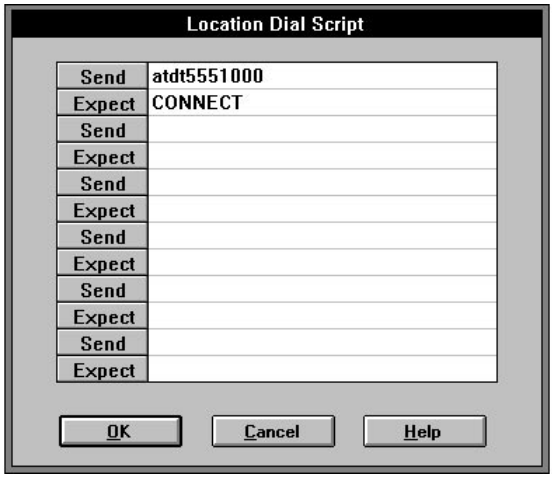
j. Now we need to assign the dial group we created earlier to this location. Enter *1* in the dial group box.

k. Maximum Ports (the maximum number of ports that can be used to dial out to the location) must be set to something other than its default (0). Enter 1 in the Maximum Ports box.

Creating the Dial Script

Now we have to tell the NETServer how to dial out to this location. This is done by creating a dial script.

a. Click on the Dial Scripts button. The Dial Scripts window appears.



Dial Script for UserC

b. In the first Send line, enter *atdt5551000\r*. This tells the modem to dial 555-1000 (The *\r* sends a carriage return to the modem, telling it that the AT command string is finished).

c. In the first Expect line, enter *CONNECT*. This tells the NETServer not to proceed until it receives a CONNECT message.

d. Click OK.

You will now be back in the Location Table window. Click on the Save button. Then click Exit.

For a more in-depth discussion of location table entries, see *Adding a Remote Device to the Location Table* in Chapter 6.

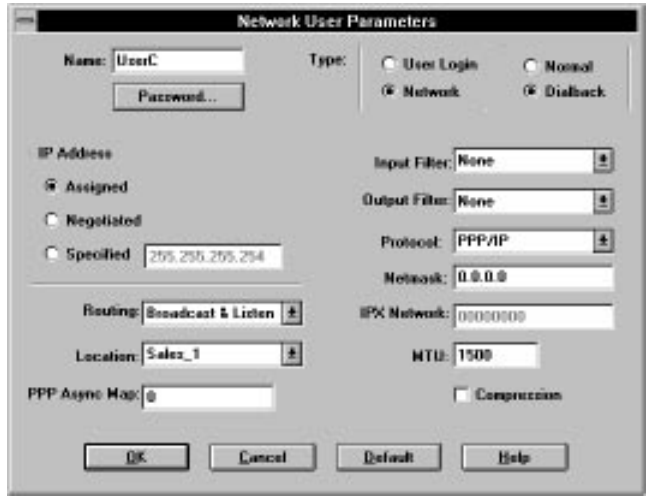
Creating a User Table entry for the Dialback user

Since dialback user table entries are only used for authentication purposes, they are very short.

a. Return to the User Table.

b. Click on new.

c. Type *UserC* in the Name field.



User C Setup

d. Click on the password button and enter the password *callmeback*.

e. Click on the Dialback button in the upper right corner of the window.

f. Pull down the Location menu and select the location we just created (Sales_1).

g. Click on the OK button.

Note that although some of the remaining fields display (default) values, the settings of these fields are irrelevant for a dialback user.

Connecting to the NETServer

The users are now ready to connect to the local network. When they dial in to the NETServer from a communications software package, they will see a login message (banner) and prompt.

If UserA and UserB respond to the User Name and Password prompts correctly, the NETServer connects them to the network.

If userC types in its user name and password at the login prompt, the NETServer sends the message "Dialback Accepted . . ." and disconnects. UserC must set his modem to Auto Answer (usually with ATS0=1). The NETServer dials the user back, using the number entered as part of the location dial script.

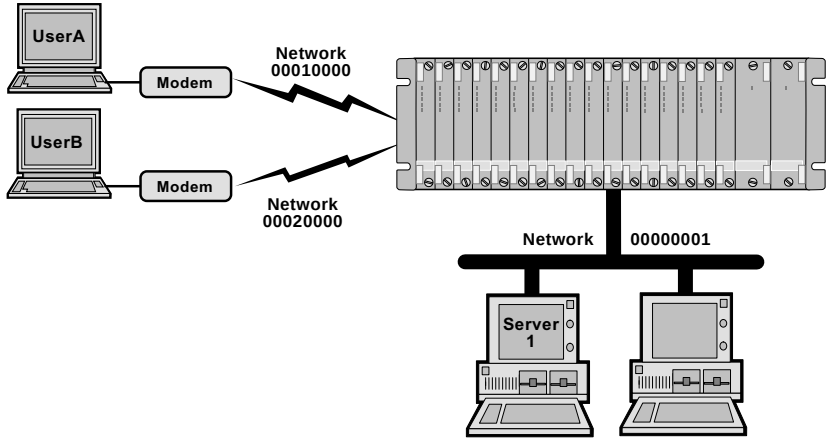
Once connected to the network, users can run TCP/IP software such as Novell's LAN workplace to telnet, ftp, and so on to other hosts on the network.

Note: Users with automated dialing software, such as Chameleon, may not see the login banner or prompt.

IPX Remote Access

This case study assumes the following:

- The configuration will take place from the Command Line software
- The NETServer's LAN interface is configured with the correct IPX network number, IPX Frame Type, and Sysname (its name on the network)
- The NETServer is set to the factory defaults on all other settings
- Two users want access to a Novell server on the NETServer's local network (userA and userB)

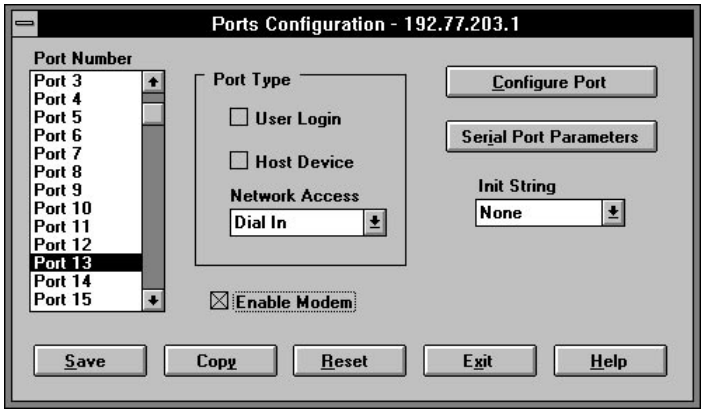


IPX Remote Access Case Study

Configure the ports

This example will use both modems to answer calls from dial in users.

a. Select Port from the Table menu. The Port Configuration Window appears.



Network Dial In Port Setup (Example)

b. Select Port 13 by clicking on it in the Port Number box.

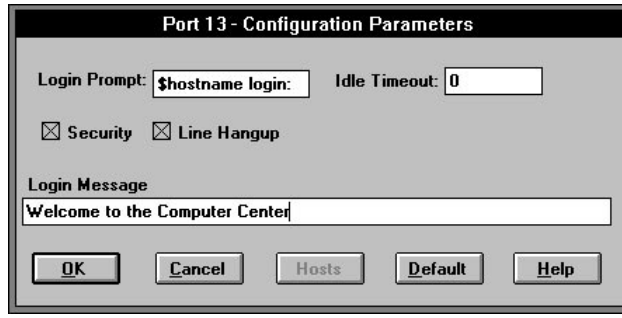
c. If the Enable Modem box appears (NETServer card only), make sure it is checked.

d. Set User Login and Host Device to Disabled.

> **Note:** It is not strictly necessary to disable User Login and Host Device. A port can be configured to serve several purposes. However, our example assumes that you don't want people using the port for anything other than the given application.

e. Set the Network field for both to *Dial In*.

f. Click on the Configure Port button. The Dial In Port Configuration window appears.



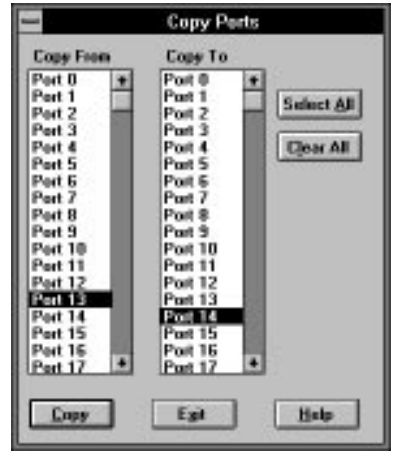
When users connect to the port, the NETServer will greet them.

g. In the Login Message box, Type Welcome to the Computer Center.

h. Click OK.

i. When the Port Configuration window reappears, click Save and then Reset.

j. Click on the Copy button. The Copy Ports window appears.



k. Select Port 13 on the left and Port 14 on the right.

l. Click Copy and then Click Exit.

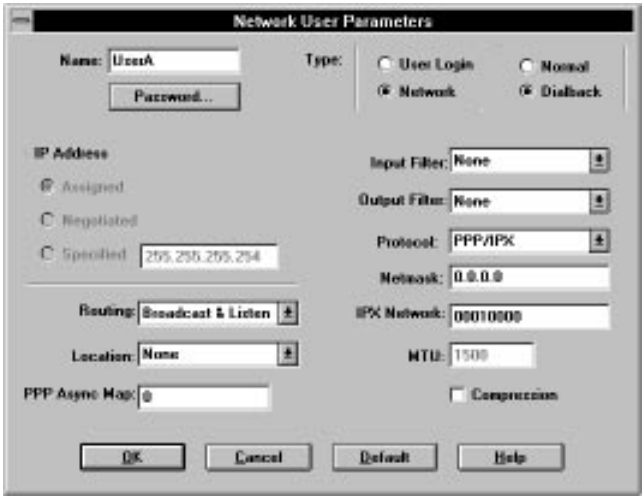
m. When the Port Configuration window reappears, Select Port 14, then click Save and then Reset.

User A Configuration

a. Select User from the Table menu.

b. Click on New. The Network User window appears.

c. Click on the Name field. Enter the name *UserA*



Setup for User A

d. Click on the Password button. Enter the password *userApw* twice and then click OK.

e. In the IPX Network field, enter *00010000.*

f. Select *PPP/IPX* in the Protocol box.

g. Enter an MTU of *1500.*

h. Pull down the Routing menu and select *Broadcast & Listen*.

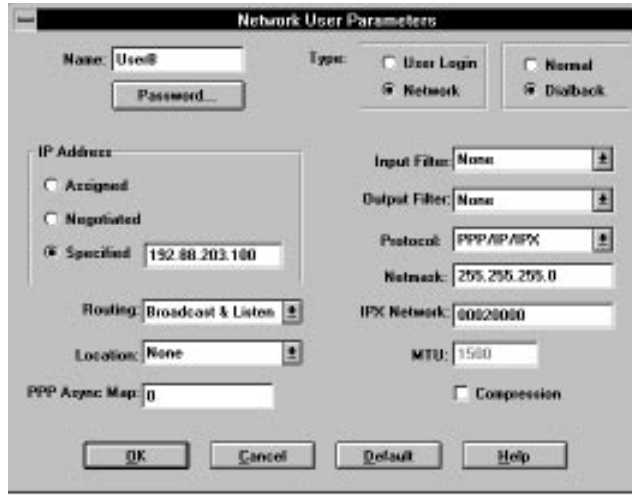
i. Click OK.

User B Configuration

User B has both the IP and the IPX protocol stacks load on his machine. So, we'll tell the NETServer what his IP address is just in case he ever wants to talk IP across the link.

a. Click on New. The Network User Configuration window appears.

b. Click on the Name field. Enter the name *UserB*.



User B Setup

c. Click on the Password button. Enter the password *userBpw* twice and then click OK.

d. Under IP Address, select *Specified*. Click on the IP address field next to Specified and enter *192.88.203.100*.

e. Type 255.255.255.0 in the Netmask box.

f. In the IPX Network box, type *00020000*.

g. Select *PPP/IP/IPX* in the Protocol box.

h. Enter an MTU of *1500*.

i. Pull down the Routing menu and select Broadcast & Listen.

j. Click OK.

Chapter 6
LAN-to-LAN Routing

The NETServer can perform IP or IPX LAN-to-LAN routing with a remote NETServer or third party router. This chapter assumes that the NETServers / routers have been installed and configured correctly.

Setup for NETServer Routing (Overview)

Before you begin, obtain the following information. These items are required for routing connections:

TCP/IP routing

- An IP address to connect to. If the remote device is another NETServer, you may use its Net0 IP address (the address you assigned during the startup procedure).

  Some routing devices have an IP address assigned to each port rather than just one IP address for the whole box. If this is the case with the remote device, use the address of the port you want to connect to.
- The connection protocol (PPP or SLIP) the NETServer will use. If routing IPX, the NETServer will set this for you (as PPP).
- The remote system's netmask
- The Maximum Transmission Unit (MTU, the largest packet that the NETServer will send to the remote device); both local and remote MTUs must match.
- Whether or not the remote device is configured for Van Jacobson compression.

IPX routing

- An IPX network number that will represent the connection between the two devices. This number must not already exist on either network.
- IPX connections must use the PPP protocol and an MTU of 1500. When you assign an IPX network number to the connection, the NETServer will set these values automatically.

Configuration

A. Configure at least one NETServer port for a connection with the remote device. See *Configuring a Port*, later this chapter.

B. If you want to use dynamic routing during the connection, set the Routing (RIP messaging) for the port you intend to use to Broadcast & Listen (On).

   If you do not want to use dynamic routing, shut RIP messaging off. It only clutters the interface, slowing traffic.

C. If the remote device will be dialing in to this NETServer, you must create a User Table entry (Network User) for it. See *Adding the Remote Device to the User Table*, later in this chapter.

D. If this NETServer will be dialing out to the location, you must create a Location Table entry for the remote device. See *Adding a Remote Device to the Location Table*, later in this chapter.

E. If you are using PPP, you can also use CHAP authentication. This requires some special configuration:

   - Regardless of whether the NETServer is dialing out to a remote device or authenticating a dial in device, it must have a (network user) user table entry for the User ID that the remote device will send. (If the remote device is another NETServer, it will send its Sysname).
   - The Password in this user table entry must be the CHAP shared secret.
   - The remote device must be configured to look up this same password when it receives the User ID (Sysname) that the NETServer will send.

   See Chapter 6 of the NETServer *Command Reference* for more information on CHAP authentication.

F. Test the connection from both sites. See *Testing the Connection* in Chapter 6 of the NETServer *Command Reference* for details.

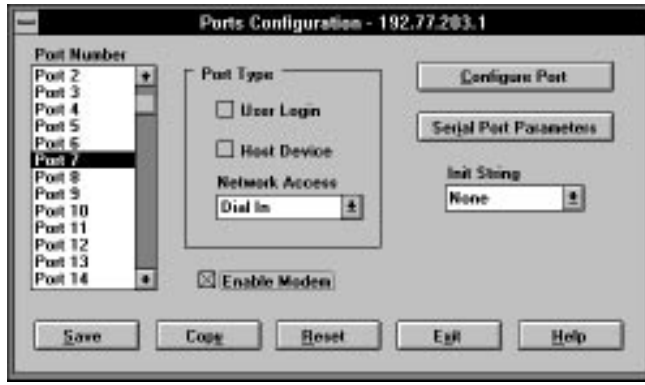
Detailed Setup

The following section gives details on configuring routing from the Windows Management Software. For this application, you must do the following:

- Configure at least one port
- Add location table entries for dial out connections
- Add users for dial in connections

Configuring the Ports

A port used for LAN-to-LAN routing should be configured as a Network Port. Select Ports from the Tables menu. The Port configuration window will appear.



Step 1 - Enable the modem (NETServer card only)

Packet bus quad modems in the Total Control Chassis must be enabled before they can be used. To do this, click on the Enable Modem box. This option will not appear on non-packet bus ports.

Step 2 - Port Type

If the port will initiate dial-up routing connections, set the Network field to Dial Out. If it will receive dial-up routing connections, set the Network field to Dial In. Select Dial In & Dial Out if you want the port to do both.

Note that the User Login and Host Device settings are completely independent of the routing engine. They do not affect routing. However, setting the port up for additional applications may affect the availability of the port.

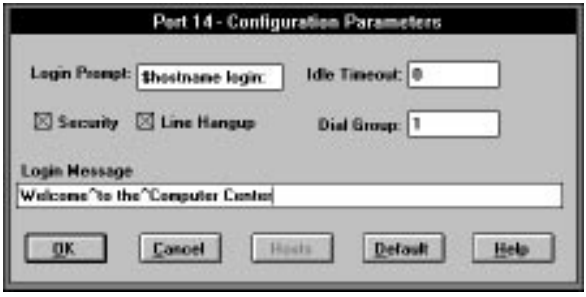
Hardwired: It's also possible to form a network connection through the external serial port (Port 1 on the NETServer/2. Port 0 on all other NETServers). In this case, you might set the port to network hardwired. Since the external serial port is the only port that can be directly attached to a serial cable, it is the only port for which this setting is valid.

If you configure the external serial port as a hardwired port, set the following parameters and go to Step 3 (For an explanation of these parameters see *Ports Table, Hardwired Port Parameters* in Chapter 10).

- IP Address
- IPX Network Number
- Netmask
- Protocol
- Routing
- MTU
- Compression

Step 3 - Create a Dial Group for dial out ports

Click on the Configure Port button. You will now see the Port Parameters window. Note that the appearance of this window varies since it displays only the options for the port type or types you have selected.



Parameters for a Dial In & Dial Out Port

If the NETServer will dial out to the remote location, you must create a group of modems that can be assigned to the location for dial out use. You must do this even if only one modem will be used for that particular location.

Assign the port to a dial group by entering the number of the group you wish to assign it to. Valid group numbers range from 0 to 99.

Note: The Dial Group box only appears if you have enabled dial out on the port.

When you are finished, click OK to exit the port parameters window.

Step 4 - Save your changes

With the port you just configured selected, click on the Save button. Then, Reset the port (click Reset) so your changes take effect.

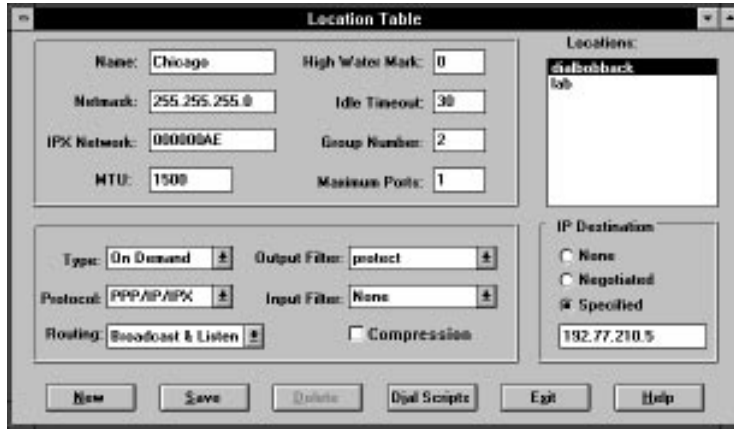
Note: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes permanently. To save the changes permanently to flash memory from Windows, you must select Save to FLASH from the File menu.

Adding a Remote Device to the Location Table

This is required only if the NETServer will dial out. If the NETServer will not be initiating connections to the remote location (the remote device will always do the dialing), you may skip to the section titled *Adding a Remote Device to the User Table.*

Step 1 - Create a new location table entry

Select Location from the Table menu. The Location Table appears:



Location Table Window

a. Click on the New button.

b. Type the name of the location in the Name field.

Step 2 - Set the required location parameters

The parameters listed below must be set:

Type

This value determines when the NETServer will dial out to a remote location. Set the type of connection to On Demand or Continuous. Note that you cannot set the type to Manual as you can from the NETServer's Command Line.

On Demand The NETServer dials out to the remote device when it has packets queued for that location. It then maintains the connection only as long as there is traffic on the line. Note that dynamic routing information is updated while there is a connection between the two devices, but not before the NETServer dials or after it hangs up. When an on-demand connection is terminated, the NETServer retains current RIP and SAP information in memory (does not delete old dynamic routes). It then uses these last known values to "spoof" (fake) RIP and SAP broadcasts to active LAN and WAN connections. When an on-demand connection is first created, the NETServer will immediately attempt to dial the remote location to obtain some initial RIP and SAP values.

Continuous The NETServer will attempt to maintain the connection at all times. If the connection is broken, it will dial again.

IP Destination

This is the IP address of the remote device. If set to Specified, type in the IP address. If set to *Negotiated* (PPP connections only), the NETServer tries to learn the other device's IP address using IPCP address negotiation. Note that negotiated addresses cannot be used with on-demand locations since the NETServer needs the IP address to know when to dial an on-demand location.

IPX Network

If IPX packets will be routed across the connection, you must assign an IPX network number. This network number refers to the dial up connection itself. It does not designate a physical network cable on either side of the connection. Note that the IPX network number must not already exist in either the remote or the local network.

Compression

If using SLIP, enable Van Jacobson IP header compression only if both networks use CSLIP (compressed SLIP).

If compression is enabled for a PPP connection, the NETServer will attempt to negotiate for compression, but will not use it if the remote site does not support compression.

MTU

The Maximum Transmission Unit specifies the size of the largest packet that may be exchanged with this location. IPX connections will discard larger packets. IP connections will fragment larger packets prior to transmission. Normally, this should be set to the largest value that the remote network can handle. However, an IP connection using multi-line load balancing may benefit from a smaller MTU. (see Step 3, below).

Valid PPP MTUs range from 100 to 500 (default is 1500). Note that PPP allows a system to negotiate a smaller MTU if needed. Valid SLIP MTUs range from 100 to 1006 (default is 1006).

> IPX LAN-to-LAN routing requires an MTU of 1500. If you have assigned an IPX Network Number, the NETServer enters this value automatically.

Netmask

Type in the remote network's IP subnet mask.

Protocol

Select the protocol that will be used for the connection (PPP or SLIP). PPP has three options: PPP / IP, PPP / IPX, PPP / IP / IPX. SLIP can be used only on TCP / IP connections.

Routing

Set the level of RIP messaging that the two devices will exchange during the connection.

Broadcast	Send dynamic routing information to the remote device. (but do not listen)
Listen	Listen for dynamic routes received from the remote device. (but do not broadcast)
Broadcast & Listen	Do both of the above.
Off	Do not send dynamic routing information. Ignore dynamic routes received.

Dial Group Number

Specifies which pool of modems will dial out. Only ports that have been assigned this Group Number can dial out to the location. Range is 0 to 99.

Idle Time-out

How many minutes an on-demand session can remain idle (no packets being sent or received) before the NETServer closes the connection. Continuous locations do not time out. Default is 0 (disable time-out).

> You *must* set the Idle Time-out field to something other than its default (disabled) for on-demand locations. If you don't do this, the initial connection will stay up permanently.

Step 3 - Setup to use multiple lines for a single connection

When talking to other NETServers, the NETServer can spread a single TCP / IP connection over multiple lines (increasing throughput).

Individual IPX clients / socket connections will show little (if any) benefit from this technique. However, because load balancing is employed, this technique may allow you to pipe more IPX clients or socket connections through the same bandwidth.

There are two parameters used to set this up: High Water Mark and Maximum Ports. Furthermore, there is some additional setup needed to allow the dialing NETServer to dial multiple numbers from a single location table entry.

High Water Mark

Determines when the NETServer should add another line to the connection. The NETServer will use an additional port if all three of the following are true:

- The number of bytes queued for the remote location exceeds the High Water Mark.
- Maxports is greater than the number of ports currently used for the connection.
- There are available ports in the location's dial group.

The default is 0 (always open all unused ports in Dial Group until Maxports is reached).

Maximum Ports

Sets the maximum number of ports the NETServer can use for a single connection to the remote location. Possible settings:

0 (Default) The NETServer may not use any ports to dial out to the location (dial out is disabled).

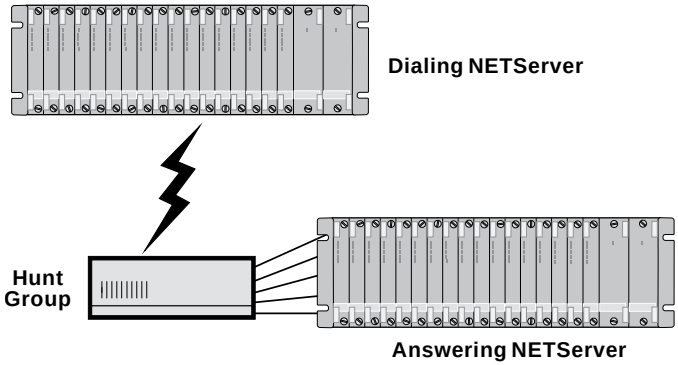
1 The NETServer may only use one modem for a connection to the remote location. This is the required setting if the remote device is not another NETServer.

2+ The NETServer may use up to this many modems for a single connection to the remote location. Additional lines will be opened based on the high water mark setting. This setting is only valid when the remote device is another NETServer.

Additional setup for multiple line connections

The NETServer on the answering end of the connection must receive each incoming call on a different line even though the other NETServer is dialing the same number every time (there is only one dial script per location). There are two ways to accomplish this:

The first is to have a single phone number set up on a hunt group. A hunt group routes calls through a single phone number out to the first available line.

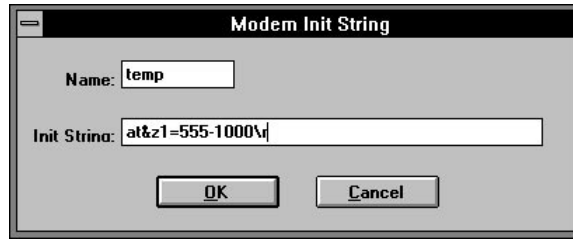


The second method consists of storing a different number in the NVRAM of each modem and then using the dial script to tell the modem to dial the number it has stored. This forces each modem to dial a different number.

Although there are easier ways to send AT commands to the NETServer's modems, they vary from NETServer to NETServer. The following method will work for all NETServers with version 3.1 or later of the NETServer firmware:

a. Select Init Strings from the Table menu.

b. When the Modem Init String window appears, click on New. The window shown below appears:



c. Enter a name for the script.

d. The initialization string will store the phone number of one of the answering modems in the calling modem's memory. Type the following in the Init String box:

AT&Z<slot #>**=**<phone number>**\r\n**

<slot #> is the number of modem NVRAM slot that you wish to configure.

e. Click OK.

f. Click Save.

g. Select Ports from the Table menu. When the Port Configuration window appears, Assign the Init String you just created to the first port in your dial group.

h. Click Save and then Reset.

i. Restore the modem's original init script.

j. Repeat steps D through I for each modem in the dial group, inserting a different phone number each time. Note that the slot number parameter must be the same for all modems in the dial group.

Step 4 - Create a dial script

Click on the Dial Script button. The Dial Script window appears. When you are finished, click on the OK button.

Location Table Dial Script Window

When creating a dial script, you must specify what the NETServer will send (for example, the AT command string the modem dials with) . You also specify what replies the NETServer will wait for (expect) before proceeding (result codes such as *CONNECT*, a *login:* prompt, etc.).

Note that send strings should have a *\r* at the end of the line. Expect strings are case sensitive.

If you have configured this location to use multiple lines without a hunt group (see Step 3), you would configure the NETServer to tell the modem to dial whichever number it has stored, rather than giving it the number explicitly. Since each modem has a different number stored, each will dial a different number. To do this, your dial script should contain the following line:

ATDS<slot #>**\r**

<slot #> is the number of the modem NVRAM storage slot used to store the number to be dialed. Note that for the same storage slot must have been used on all modems in the dial group for this technique to work.

For further information on dial scripts, see *Location Table, Dial Scripts* in Chapter 10. See your modem reference for more information on AT commands supported.

Step 5 - Save your changes

Click on the Save button.

Note: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes to flash memory. To save the changes permanently to flash memory from Windows, you must also select Save to FLASH from the File menu.

Adding the Remote Device to the User Table

Adding a user table entry is required if the remote device will be dialing into the NETServer.

It is only required for dial out connections if you want to use CHAP authentication on a PPP connection.

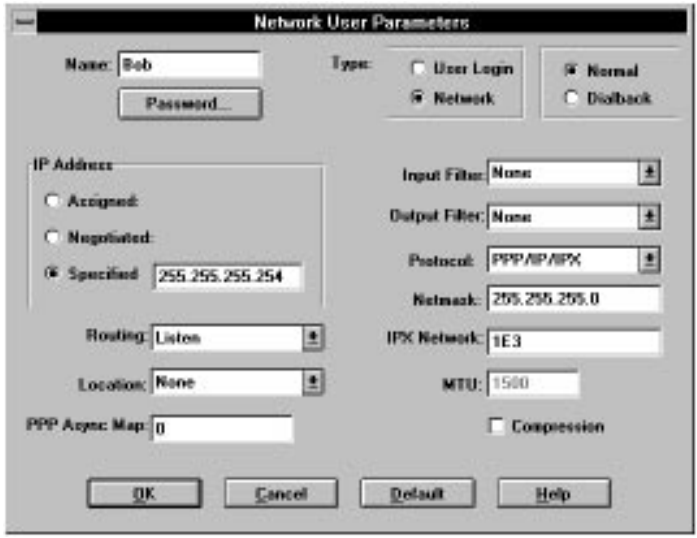
Step 1 - Create a new user table entry

S Select User from the Tables menu. The User Parameters window appears:

a. Click on the New button.

b. The Network User Parameters window appears. Type in a user name in the User Name field.

> **Note:** If you plan to use CHAP authentication, the User Name *must* be the system ID that the remote device will send during a CHAP challenge (other NETServers will send their Sysname).



Network User Parameters window

c. Click on the Password button to set the user's password.

The User Password Validation box appears. There are two blank fields to type the password in. Type the password in the first field. Then press the Tab key or click on the second field to advance the cursor. Type the password again . When finished, press the Enter key or click on the OK button.

Note: If you are planning to use CHAP authentication , the password defined here will be used as the CHAP shared secret. The shared secret *must* be the same on both devices.

Step 2 - Tell the NETServer about the remote device

You must set the following parameters:

IP Address

This is the IP address that the remote device uses for the duration of the connection.

You must assign a Specified IP address—the remote device uses this address when connecting to the local NETServer.

IPX Network

Type in an IPX network number that will be assigned to the link between the two devices during the routing session. This network number must be unique to *both* networks.

Protocol

Select the protocol that the local and remote NETServer will use for the connection (PPP or SLIP). PPP has three options: PPP / IP, PPP / IPX, or PPP / IP / IPX. SLIP can only be used on IP connections.

MTU

The Maximum Transmission Unit specifies the size of the largest packet that may be exchanged with the remote location. IPX connections will discard larger packet. IP connections will fragment larger packets. Normally, this should be set to the largest value possible. However, an IP connection using multi-line load balancing may benefit from a smaller MTU (see Step 3 of Location setup, earlier in this chapter).

Valid PPP MTUs range from 100 to 1500 (default is 1500). Note that PPP allows remote systems to negotiate a smaller MTU if needed. Valid SLIP MTUs range from 100 to 1006 (default is 1006).

> IPX LAN-to-LAN routing requires an MTU of 1500. If you have entered an IPX Network number the NETServer will automatically set this to 1500.

Netmask

Type in the remote network's IP subnet mask.

Routing

Set the level of RIP messaging that the two devices will exchange during the connection.

Broadcast	Send dynamic routing information to the remote device. (but do not listen)
Listen	Listen for dynamic routes received from the remote device. (but do not broadcast)
Broadcast & Listen	Do both of the above.
Off	Do not send dynamic routing information. Ignore dynamic routes received.

Compression

Van Jacobson TCP/IP header compression should be enabled for a SLIP connection only if both the local NETServer and the remote device are configured to use compressed SLIP (CSLIP). Both sides must agree on whether to use compression or the connection will fail.

Enabling compression on a PPP connection will cause the NETServer to negotiate for compression. Compression will be used only if the remote device supports it.

Step 3 - Save your changes

When finished, click on the OK button to return to the User Table Configuration window. Save your changes by clicking on the Save button.

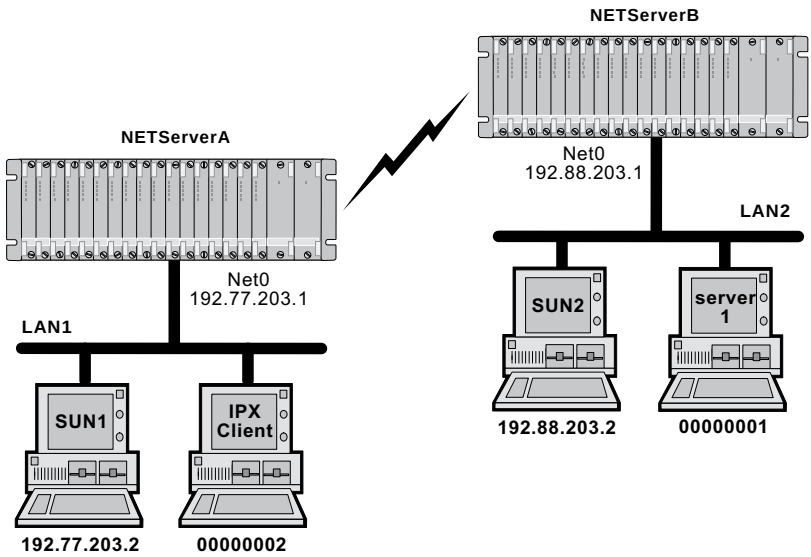
Note: Clicking on the Save button saves your changes to the NETServer's RAM only. It does not save those changes to memory. To save the changes permanently to flash memory from Windows, you must also select Save to FLASH from the File menu.

LAN-to-LAN Routing Case Study

The following example shows routing between two NETServers in order to demonstrate how each end of the connection would be configured.

This case study assumes the following:

- both NETServers (NETServerA and NETServerB) are configured with the correct IP address, Netmask, IPX network number and IPX Frame Type.
- NETServerA's Sysname is *nsa.* NETServerB's Sysname is *nsb.*
- both NETServers are set to the factory defaults on all other settings
- NETServer A is on LAN1, the main data center of a company, and NETServer B is on LAN2, a branch office.
- if traffic on the connection becomes too great, NETServerB will open a second line
- if there is no traffic on the connection for 30 minutes, NETServer B disconnects



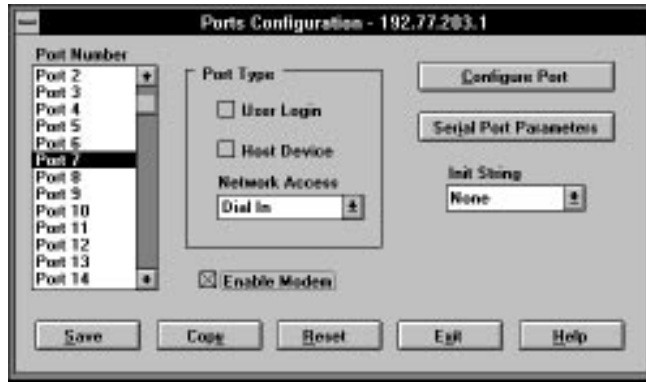
Case Study—LAN to LAN Routing Between Two NETServers

This example sets up two NETServers for LAN to LAN routing. NETServer B will be configured to dial NETServer A on demand. When packets are waiting to be transferred, NETServer B will form a virtual connection to NETServer A. When the connection is no longer needed, it is terminated.

Setting Up NETServer A

NETServer A will use modems 7 and 8 to answer dial in routing connections from NETServer B.

1. Login to NETServer A and select Ports from the Tables menu. The Port Configuration Window appears:



NETServer A Port Setup

2. Select Port 7 in the Port Number box.
3. If the Enable Modem box appears (NETServer card only), make sure it is checked. This activates the packet bus connection to Port 7.
4. Set the Network Access field to Dial In.
5. Turn User Login and Host Device off.

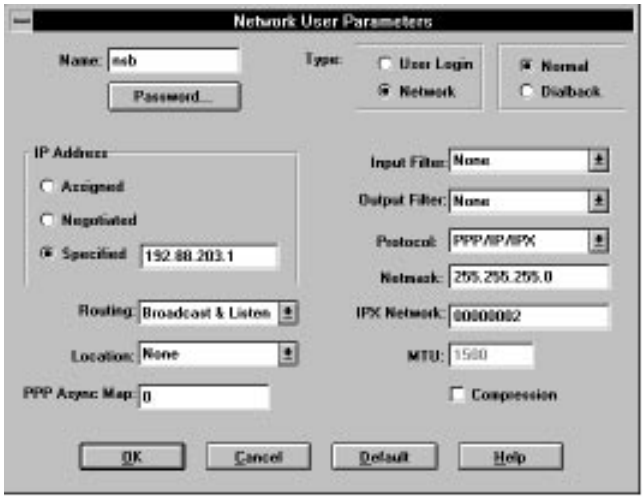
> **Note:** It is not technically necessary to disable User Login and Host Device. However, this example assumes that you will be using these ports only for the given application.

6. Click on Save and then Reset.

7. Click on the Copy button. Copy the configuration from Port 7 to Port 8.
8. When you return to the Port Configuration window, select Port 8. Then click on Save and then Reset.
9. Click on the Exit button.

Since NETServer B will be dialing in to form a network connection, NETServerA is a network user. It will need an entry in the Users Table.

10. Open the Users Table Configuration window by selecting Users from the Tables menu.
11. Click on New. The Network User Parameters window appears:



NETServer B's user table entry on NETServer A

12. Click on the Name field. Enter the name *nsb*.
    Note: For CHAP, this is NETServer B's Sysname.
13. Click on the Password button. Enter the password *xyzabc* twice and then click OK.
14. Under IP Address, select Specified and enter 192.88.203.1.
15. Select PPP / IP / IPX in the Protocol box.
16. Enter 255.255.255.0 in the Netmask field.

17. Enter 2 in the IPX Network box.

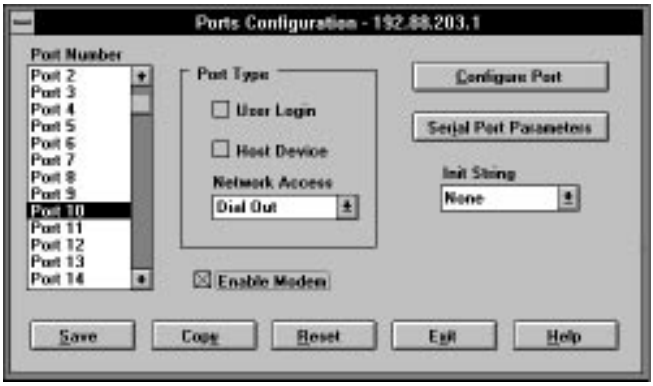
The NETServers should exchange dynamic routing information (RIP packets) with each other.

18. In the Routing field, select Broadcast & Listen.
19. Click OK to save your work.

Setting Up NETServer B

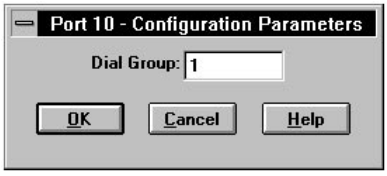
NETServer B will use ports 10 and 11 to dial out to NETServer A.

1. Log into NETServer B and select Ports from the Table menu. The Port Configuration window appears:



NETServer B Port Configuration

2. Select (click on) Port 10 in the Port Number box.
3. Enable the Modem (NETServer card only).
4. Disable User Login and Host Device.
5. Set the Network field to Dial Out.
6. Click on the Configure Port button. The Port Parameters window appears:



Configuring a Dial Group

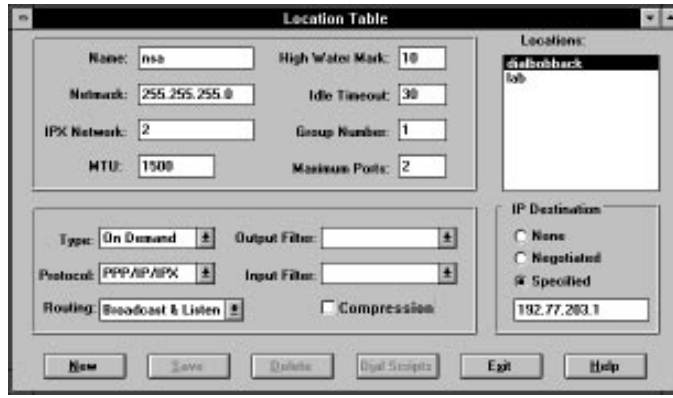
7. Enter 1 in the Dial Group box (assign this modem to dial group 1).
8. Click OK.

9. When the Port Configuration window reappears, click on Save and then Reset.
10. Click on the Copy button. Copy Port 10 to Port 11.
11. When the Port Configuration window reappears, select Port 11 in the Port Number box.
12. Click on Save and then Reset.

The Dial Out Location

Instead of user entries, dial out ports have entries in the location table. In this case, a location entry for NETServer A.

1. Go to the Location Table window by selecting Locations on the Tables menu or by clicking on the Locations button in the Toolbar.
2. Click on New.
3. Enter *nsa* in the Name field. Note that because we are using CHAP, this field must contain NETServer A's Sysname.



NETServer A's location table entry on NETServer B

4. Type *255.255.255.0* In the Netmask field.
5. Type *2* in the IPX Network box.
6. Set the MTU value to *1500*.
7. In the IP destination box, click on Specified and enter *192.77.203.1*.
8. In the Protocol field, select *PPP/IP/IPX*.

9. In the Type box, select *On Demand*.
10. In the Routing box, select *Broadcast & Listen*.

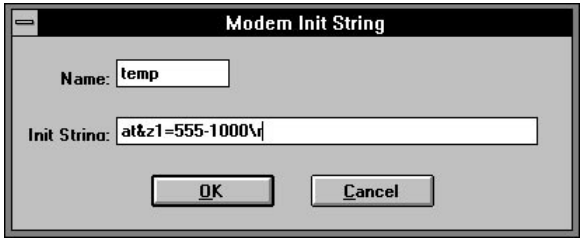
Now, we need to tell NETServer B which modems it can use to dial out to NETServer A. In this case, the group of modems we just created.

11. Enter a Group Number of 1.

Multiple line setup

Steps 12 to 15 configure NETServer B to dial out with a second line if the first line is backed up.

12. In the High Water Mark field, type 10. This instructs the NETServer to dial out with a second modem when the queue is backed up by more than 10 bytes (in other words, the High Water Mark is exceeded).
13. Set Maximum Ports to 2. This tells the NETServer that it can use both modems in the dial group for the connection.
14. Set an Idle Time-out of 30. Since this will be an on-demand connection, each modem should hang up if there has been no traffic on the line for the last 30 minutes.
15. Click on Save and then exit the Location Table.
16. Since this example, uses multiple ports for a single connection, the modems should be set up to dial different numbers. Select Init Strings from the Table menu.
17. When the Modem Init String window appears, click on New. The window shown below appears:



18. Type *temp* in the Name box.

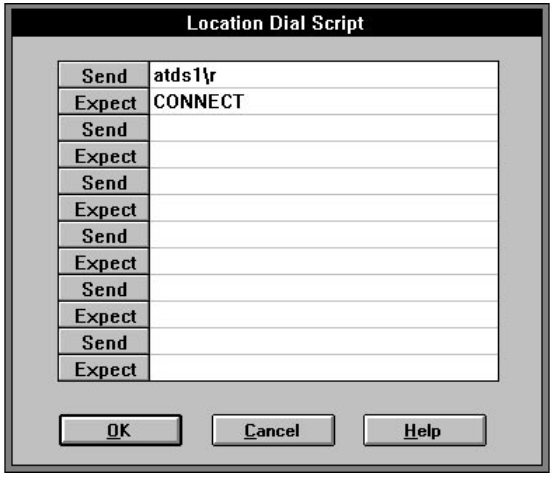
19. The initialization string will store the phone number of one of the answering modems in NVRAM slot 1 of Port 10, one of the calling modems. Type the following in the Init String box:

    AT&Z1=555-1000\r

20. Click OK
21. Click Save and close the Init String window.
22. Select Ports from the Table menu.
23. When the Port Configuration window appears, select Port 10 from the Port Number box.
24. select temp in the Init String box
25. Click Save and then Reset.
26. You should now return the Init String box to what it was before and then click on Save again.
27. Close the Port Configuration window and return to the Init String window.
28. Delete temp and create a new init string, this time using the number 555-1001.
29. Assign this script to Port 11 and then reset the port.
30. Restore the Port 11's original init string. Delete the second temporary init string.

The Dial Script

16. Return to the Location table, and select the *nsa* entry.
17. Click on the Dial Scripts button. The Location Dial Scripts window appears:



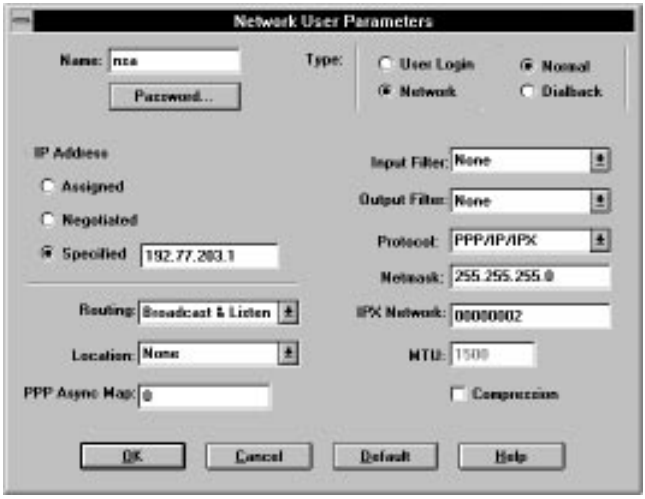
NETServer A's Dial Script

18. In the Send field for Script 1, type *atds1\r*. This tells the modems to dial the number stored in NVRAM slot 1. For connections using only a single line, you would simply put the number dialed here, such as *atdt555-1000\r* In either case, the *\r* switch indicates a carriage return.
19. In the Expect field, type CONNECT. This tells the NETServer to wait for a *CONNECT* message from the modem before proceeding. Note that the values entered as expected result messages are case-sensitive.
20. Click on OK.
21. When the Location Table reappears, click Save and then exit the location table.

The user table entry

When NETServer A receives a call from NETServer B, it will respond with a user name prompt, just like it would for any other network user. But instead of just logging in like a user, NETServer B is going to initiate CHAP authentication. By this process, the NETServers authenticate each other as valid users. Needless to say, this means that NETServer A must be in NETServer B's user table. Let's add a user entry.

1. Open the User Table Configuration window.
2. Click on New.



NETServer A's user table entry on NETServer B

3. In the Name field, type *nsa.*
4. Click on the Password button. Type ***xyzabc,*** then type it again to verify it.

> **Note:** The passwords of both NETServerA and NETServerB must be the same for CHAP authentication. This is called a "shared secret."

5. In the Type box, verify that Network is selected.
6. In the IP Address box, click on Specified, and then enter this address in the field: 192.77.203.1.

7. In the Routing field, select *Broadcast & Listen*.
8. In the Protocol field, select *PPP/IP/IPX*.

Chapter 7
Talking to the Modems

This chapter discusses use of the NETServer's modems. The following topics will be covered:

- Modem Sharing - basic setup
- Implementing security on a shared modem port
- Configuring modems as UNIX pseudo TTYs
- Initialization scripts

Modem Sharing - basic setup

TCP/IP modem sharing on a NETServer requires that you configure some "host device" ports. This allows you to assign a TCP port number to a modem or a pool of modems so that users on the local network can get to the modem's command line using a login service. Setup looks like this:

Step 1 - Configure the port as a host device

a. Select Ports from the Table menu. The Port Configuration window appears.

b. Select (click on) the port you want to configure from the list in the Port Number box.

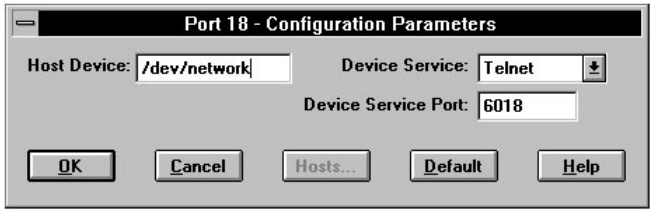
c. For the port that you want to configure, check the Host Device field. Note that you will not be allowed to do this if Network Access is set to Hardwired.

Step 2 - Enable the modem (NETServer card only)

Packet bus quad modems in the Total Control Chassis must be enabled before they can be used. To do this, click on the Enable Modem box. This option will not appear on non-packet bus ports.

Step 3 - Assign a Host Device Name

Click on the Configure Port button. The Port Parameters window appears. Note that the appearance of this window varies since it displays only the options for the port type or types you have selected.



Set the Host Device field to the following:

/dev/network

> **Note:** If you are using one of the pseudo TTY drivers described later, the Device field is configured differently. See *Configuring modems as UNIX pseudo TTYs*, later in this chapter.

Step 4 - Choose a device service

You will now need to choose the login service that will be used to connect to the modem's command line (If Telnet will be used to talk to the modem, choose Telnet, etc.) The device service field has the following options:

Telnet Supported by most TCP/IP computers. You must choose Telnet if you want to implement security on a host device port.

Rlogin Although Rlogin was originally a (BSD) UNIX only protocol, it is now supported by some non-UNIX machines as well.

PortMux PortMux is used only for pseudo TTY host device configuration. See Configuring modems as UNIX pseudo TTYs, later in this chapter.

Netdata (Default) Selecting Netdata as the login service allows an application program to for a "Clear TCP" connection with a modem. In other words, data exchanged with the modem will not be filtered in any way.

Netdata's clear TCP connection can be used by applications that require a socket interface. The NETTTY pseudo TTY device driver, described later in this chapter is an example of such application.

Step 5 - Choose a TCP port number

Assign the modem a TCP port number. To do this, type the port number in the Device Service Port field. If you do not want to implement security for dial out users, we suggest 6000 plus the S-Port number. If you do want to implement security for these users, you must select a port number between 10000 and 10100.

Assigning the same TCP port number to multiple ports will create a pool of modems. The user will be connected to the first available modem in the pool.

Step 6 - Save your work and reset the port

Click OK. When the Port Configuration window reappears, click on Save and then Reset.

Implementing Security on a Host Device Port

To authenticate a host device dial out user, configure a host device port with a device service of Telnet and a TCP port number between 10,000 and 10,100. These ports can only be connected to by the NETServer itself, forcing the user to Telnet to port 23, the default Telnet port. When the user connects to port 23, he or she will be prompted for a user name and password just like any other login user. Once authenticated, the NETServer can forward valid users to the correct port.

User table entries

Since a dial out user for a host device port with security will be authenticated, he or she will require a user table entry.

1. Select User from the Table menu.
2. Click on New
3. When the User Parameters window appears, select User Login in the Type box.
4. Enter a name and a password for the user.
5. In the Host box, select Specified and Enter the NETServer's own IP address.
6. Select a login service of Telnet
7. In the Access Port field, enter the TCP port number assigned to the modem or pool of modems the user will access.

To use a modem, the user telnets to the NETServer

telnet <NETServer IP address>

The user will then be prompted for a user name and password. If he or she responds correctly, the user will be connected directly to the modem's command line.

Note: RADIUS servers have a user type called Outbound User which is defined as a dial out user on the local network. However, because the NETServer defines these users as login users whose host is the NETServer itself, in RADIUS you would configure these users with the user type Login-User.

Configuring modems as UNIX pseudo TTYs

A pseudo TTY device acts like a serial device, but is actually something else entirely. In this case, we would like one of the NETServer's modems to act as if it is connected to one of the serial ports of a UNIX host, even though it's really attached to the NETServer.

There are two different UNIX pseudo TTY device drivers that work with the NETServer. Both are available on the U.S. Robotics Web site.

nettty This daemon is used for pseudo TTY access to Host Device ports configured to use the Netdata device service.

in.pmd This PortMux login service daemon will also provide pseudo TTY functionality. Host Device ports should be configured to use the PortMux device service.

Once obtained, such a daemon must be installed on each UNIX host that will be using the modems.

Port Setup

You must then set up some host device ports on the NETServer. This is a special case of the host device port setup described earlier in this chapter. When configuring pseudo TTYs, the Device Service must be set to Netdata or PortMux, depending on which pseudo TTY driver you have loaded on your hosts.

All ports in a single dial out pool must use the same TCP port number.

Host Device Name

The Host Device field must identify the UNIX pseudo-tty device in the host's /dev directory. The default is none. This same value must be entered at the host's command line when you run the nettty daemon. Some standard entries are:

/dev/ttyp0 *through* **/dev/ttypf**

/dev/ttyq0 *through* **/dev/ttyqf**

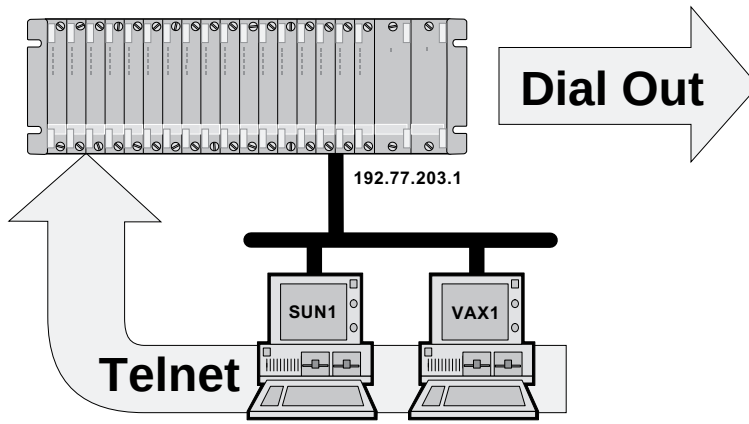
/dev/ttyr0 *through* **/dev/ttyrf**

Keep in mind that other programs on the host may use these pseudo-tty devices, but usually select the pseudo-tty drivers from the beginning of the list (for example, /dev/ttyp0, /dev/try, and so on). We recommend you select the pseudo-tty device drivers from the end of the list (for example, /dev/ttypf or /dev/ttyqe).

Host Device Case Study

SUN1 and VAX1 are IP users on the local network who want to dial out using the NETServer's modems. The setup will follow the guidelines below:

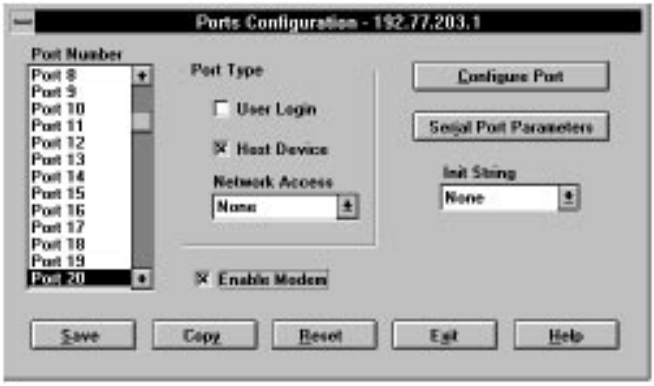
- Password security will be implemented in order to limit the modems to authorized users only.
- A pool of modems will be created using ports 20 and 21. When SUN1 and VAX1 logs into the NETServer, they will be connected to the first available modem in the group.



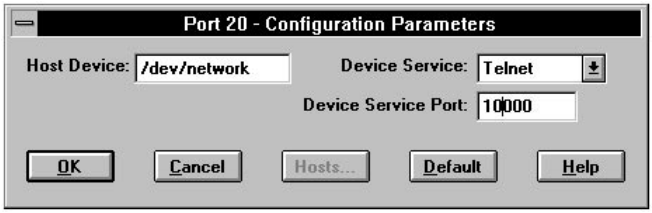
Host Device Case Study

Port Configuration

1. Select Ports from the Table menu. The Port Configuration window appears:



2. Click on Port 20 in the Port Number window.
3. If the Enable Modem box appears (NETServer card only), make sure it's checked. This activates the packet bus connection between the NETServer and the modem.
4. In the Port Type box, select Host Device, turn off User Login, and set Network Access to *None*.
5. Click on the Configure Port button The Port Parameters window appears:

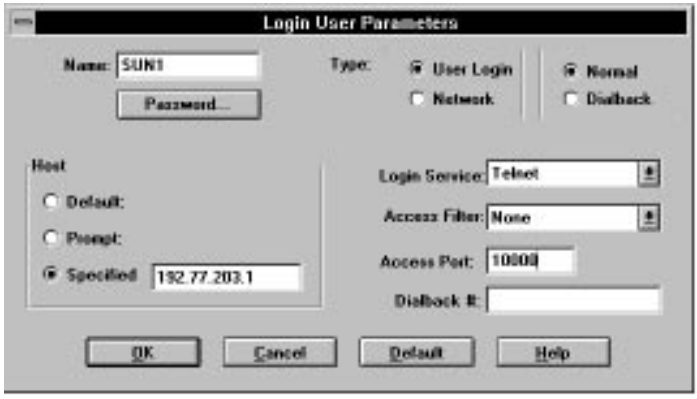


6. Type */dev/network* in the Host Device box.
7. Pull down the Device Service box and select Telnet.
8. Type 10000 in the Device Service Port box.
9. Click OK.

10. When the Port Configuration window reappears, click Save and then Reset.
11. Click on the Copy button.
12. Copy Port 20 to Port 21. Note that both ports now use the same TCP port number (100000), making them a pool of modems.
13. When the Port Configuration window reappears, click Save and then Reset.

User Configuration

1. Select User from the Table menu.
2. When the User Configuration window appears, click on the New button.
3. The Network User Parameters window appears. Click on User Login in the Type box. The window changes to Login User Parameters.



4. Type *SUN1* in the Name box.
5. Click on the Password box. The User Password Validation window appears:

6. Enter the password *Dialout* twice and click OK.
7. In the Host box, select Specified and enter the NETServer's IP address (192.77.203.1).
8. Pull down the Login Service box and select Telnet.
9. In the Access Port box, type the TCP port number assigned to the modems (10000).
10. Click OK.
11. Click on New again and create a user table entry for VAX1.

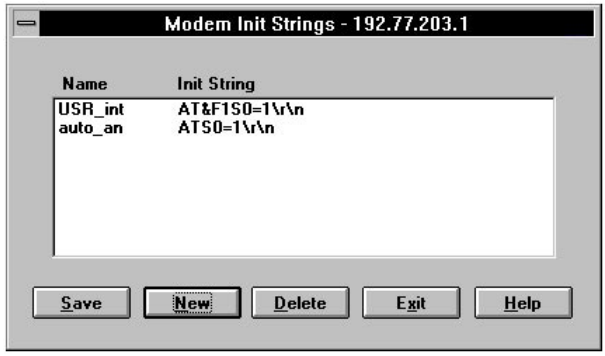
Modem Initialization Scripts

An initialization string may be sent to any one of the NETServer's S-Ports each time the port is reset (a modem resets itself each time it disconnects). An initialization string can contain any text that needs to be sent to a port at start up. For a modem, the initialization string will usually contain AT commands.

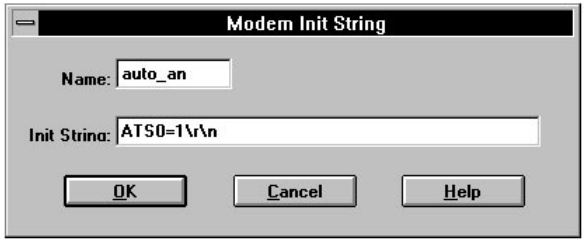
There is no standard list of what commands a modem initialization string should execute. Every system administrator will have different needs for each modem. For example, an administrator with a number of remote dial in users who have a wide range of modems of varying reliability may choose to force a NETServer modem to a safe modulation like V.32 *bis* rather than allow higher speed modulations. A separate initialization string may be assigned to each port.

Creating initialization strings

1. Select Init Strings from the Table menu. The Modem Init String window appears:



2. Click on the New button.



3. Type a name for the initialization string in the Name box.
4. The init string itself is the text that is sent to the port when the script is executed. When composing this string, be sure to follow the syntax rules (case sensitivity and so on) of the device attached to the port. The string can be no longer than 56 characters.

> **Caution:** Avoid using commands that write to the modem's NVRAM (such as &W) in an initialization script that you plan to use indefinitely. Rewriting the NVRAM every time the port is reset may eventually wear the NVRAM out. Use such commands only on a short term basis.

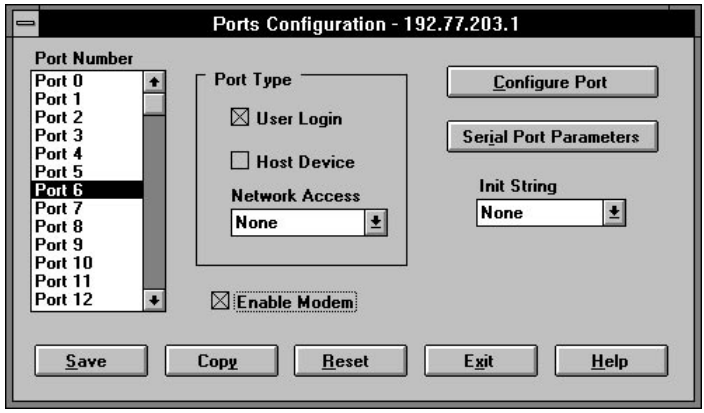
The following special characters are allowed. *\r* should *always* be present at the end of a modem initialization string:

\r	carriage return
\n	line feed
*\o*xx	octal digit xx
\ \	single backslash

5. When you are done entering the initialization string, click OK and then click Save.

Using initialization strings

Once you have created an initialization string, it must be assigned to the appropriate ports. This is done in the Port Configuration window.



1. Select the port you want to configure from the Port Number box.
2. Pull down the Init String list and select the name of the string you want to use.
3. Click Save.

The default initialization string

NETServer/2, NETServer/8 and NETServer/16 all have a predefined initialization script assigned to all their internal modems. This script is called *USR_int* and looks like this:

```
AT&FS0=1\r\n
```

This string sets a U.S. Robotics modem for hardware flow control and auto answer.

There is no such default init string defined for the NETServer card.

Chapter 8
Packet Filters

This chapter covers setting up packet filters for the NETServer. The following topics are included:

- Filter overview
- Creating new packet filters
- Filter rule format
- TCP/IP packet filtering
- IPX packet filtering
- Editing Packet filters

Overview

Packet filters are primarily used in networks that cross organizational or corporate boundaries. They control inter-network data transmission by permitting or denying the passage of specific packets through network interfaces.

When data packets are received by a network interface such as a modem, the packet filter analyzes their header information. After evaluating the data packet against its set of rules, the filter permits it to pass through or discards it. If an IP packet is discarded, the NETServer sends an ICMP "Host Unreachable" message back to the originator.

Types of Filters

The NETServer supports the following types of packet filters:

- Input and output filters; packet filters can be created to control either inbound or outbound data packets

- Source and destination address filtering; a packet filter can permit or deny access based on the IP address of the source and / or destination
- Protocol filtering; inbound or outbound network traffic can be evaluated based on the protocol
- Source and destination port filtering; a packet filter can control what services local or remote users can access
- Established session filtering; a packet filter can permit users to connect with a remote network without letting remote users have access to the local network (or vice versa)

Packet Filters and the NETServer

Once created, a packet filter can be designated for use in any of the following applications:

- Filter packets exchanged with the local network (Input Filter and Output Filter fields of LAN Port Configuration)
- Control which hosts all login users can access (Input Filter field of Port Parameters window for user login ports);
- Control which hosts a specific login user can access (Access Filter field of the Login User Parameters window)
- Filter packets passing through a hardwired connection (Input Filter and Output Filter fields of the Port Parameters window for hardwired ports)
- Filter packets exchanged with a specific network user (Input and Output Filter fields of Network User Configuration)
- Filter packets exchanged with a specific location (Input Filter and Output Filter fields of the Location Table)

Information Sources

Internet packet filtering and security are complex issues which this chapter can barely scratch the surface of. The following sources provide additional information:

Cheswick and Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison Wesley, 1994, ISBN 0-201-63357-4

Siyan and Hare, *Internet Firewalls and Network Security*, New Riders Publishing, 1995, ISBN 1-56205-437-6

Input filters vs. Output filters

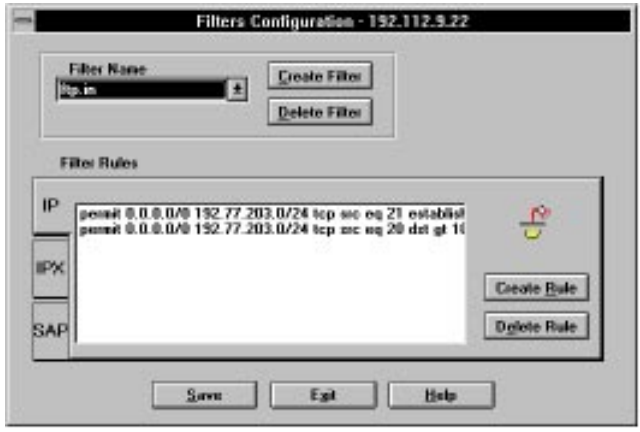
You can assign two packet filters to each interface: an input filter and an output filter. Input filters control which packets are allowed *into* the NETServer through the interface. Output filters control what packets are allowed *out* of the NETServer.

When possible, use the input filter to filter out an incoming packet rather than waiting to catch a packet on its way out of the NETServer. There are several good reasons for this.

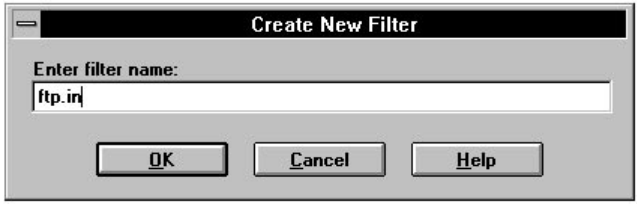
- Preventing a packet from entering the NETServer can keep potential intruders from attacking the NETServer itself.
- The NETServer's routing engine does not waste time processing a packet that is going to be discarded anyway.
- Most importantly, the NETServer does not know which interface an outgoing packet came in through. If a potential intruder forges a packet with a false source address (in order to appear as a trusted host or network), there is no way for an output filter to tell if that packet came in through the wrong interface. An input filter, on the other hand, can filter out packets purporting to be from networks that are actually connected to a different interface.

Adding Packet Filters

1. Select Filters from the Table menu. The Filter Configuration window appears:



2. Click on the Create Filter button. The Create New Filter window appears:

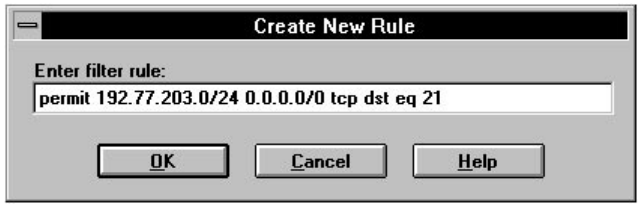


3. Type in the name of the packet filter and click OK.

   The filter name can be up to 15 characters long. You can also add an extension to a given filter. For example, we recommend that you add *.in* to an input filter name (such as *sales.in*) and .out to the corresponding output filter (such as *sales.out*) . Filters used in conjunction with RADIUS Framed Users are *required* to follow this naming convention.

   The new packet filter appears in the Filter Names list.

4. Select what type of rule you want to create: IP, IPX, or SAP. Click on the “tab” designating that filter type.
5. To add a filter rule of the specified type, click on the Create Rule button. A dialog box appears, asking you to type in the packet filter rule. See *Filter Rule Format*, later in this chapter for more information on filter rules.



Note: The NETServer evaluates rules in order, so you should put the most frequently matched rules first.

6. Click OK.
7. Repeat steps 4 through 6 for all required rules. Note that although the number of packet filter rules in the NETServer itself is limited only by available memory and storage space, NETServer manager limits you to a maximum of 100 rules of each type.
8. When you are finished, click on the Save button.

Note: You are saving changes to the NETServer RAM, not flash memory. To save the changes permanently to flash memory, you must select Save to FLASH from the File menu.

Filter Rule Format

There are three types of packet filter rules: IPX rules, IP rules, and SAP rules. A packet filter can contain all three types.

In the Windows software, you must use the following format, regardless of the filter rule type (IP, IPX, or SAP):

<*permit* | *deny* > <IP, IPX, or SAP options>

Permit or Deny

This is a required parameter which indicates whether packets meeting the specified criteria should be forwarded (permit) or discarded (deny).

If a packet does not meet any of a filter's rules, the NETServer denies the packet. The NETServer takes this "if in doubt, discard" approach to packet filtering because in many cases it's impossible to explicitly deny every possible intrusion into your network. Even if you managed to create such a filter, it would be out of date tomorrow. The accepted method of filter creation is to:

1. Explicitly permit the services which are absolutely necessary. Limit the permission in every way you can.
2. Allow everything else to be denied.
3. See who yelps. Go to step 1.

However, if you want to create a filter that permits everything not specifically denied, the last rule of all three types should be simply *permit*.

Options

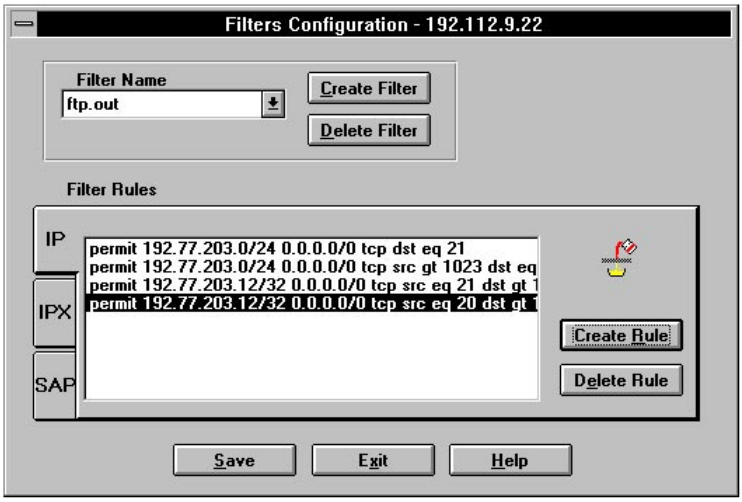
See TCP/IP packet filtering and IPX packet filtering, below.

TCP/IP packet filtering

After *permit* or *deny*, IP rules start with the following parameters:

<source_address/mask> <dest_addr/mask> <*tcp* | *udp* | *icmp*>

Depending on the protocol, there can be more options following these parameters. See *TCP and UDP parameters* and *Filtering ICMP packets* for more information.



Source_Address

The address given here is compared to the source address of the packet. Note that only the part of the address specified by the *mask* field is used in the comparison.

The following rule example permits source addresses that match the first 16 bits of the given IP address (that is, addresses beginning with 192.77):

permit 192.77.200.203/16

Note: The source address and destination address fields generally are used to limit permitted access to trusted hosts and networks only, to explicitly deny access to hosts and networks that are not trusted, or to limit external access to a given host (for example, a web server or a firewall). The following rule permits E-mail packets only if they are from host 192.77.203.24.

permit 192.77.203.24/32 0.0.0.0/0 tcp dst eq 25

Dest_Address

The address given here is compared to the destination address of the packet. Note that only the part of the address specified by the *mask* field is used in the comparison.

The following rule example denies destination addresses that match the first 8 bits of the given IP address (that is, addresses beginning with 192).

deny 0.0.0.0/0 192.77.200.203/8

Masks

These fields specify the number of bits to be used in the *source_address* and *dest_address* comparisons. Valid masks range from 0 to 32. Common bit counts are:

0 Match packets with any IP address. The contents of the source_address or dest_addr field are not important.

8 Compare the first byte (octet) in the IP addresses.

16 Compare only the first two bytes of the IP addresses

24 Compare only the first three bytes of the IP Addresses

32 Match the entire IP address

The masks are separated from source_address and dest_addr by forward slashes (/).

TCP and UDP parameters

TCP and UDP packets can be filtered by source and destination socket numbers. This allows you permit or deny specific services.

<tcp |udp> ***src*** *<lt | gt | eq>* <TCP/UDP port #>

Compare the source port number in a TCP or UDP packet to a specific value.

lt or *lessthan*	less than
eq or *equal*	equal to
gt or *greaterthan*	greater than

A sample rule might look something like this:

```
permit tcp src gt 23
```

<tcp |udp> ***dst*** *<lt | gt | eq>* <TCP/UDP port #>

Compare the destination port number in a UDP packet to a specific value. Example:

```
deny udp dst eq 40
```

established

Evaluates whether the packet is for an established connection. Note that since UDP is not a connection-oriented protocol, this parameter can only be used in TCP rules. Example

```
permit tcp dest eq 192 established
```

Established is used to restrict a normally two-way connection to only one way. One example would be allowing internal users to establish FTP sessions with external hosts, while denying external users FTP access to local hosts. Since a single FTP session sends packets in both directions, filtering out FTP packets headed in either direction will kill FTPs in both directions. See the discussion of FTP below for more information.

Standard Port Numbers

The table below contains information on standard port numbers for some common services. For a complete list, see the most recent "Assigned Numbers" RFC (currently RFC 1700).

TCP	*UDP*	*Description*
20	-	File Transfer Protocol (data)
21	-	File Transfer Protocol (control)
23	-	Telnet
25	-	Simple Mail Transfer Protocol
43	43	Who Is
53	53	Domain Name Service
-	69	Trivial File Transfer Protocol
70	70	Gopher
79	79	Finger
80	-	World Wide Web HTTP
88	88	Kerberos
110	-	Post Office Protocol - Version 3
111	111	Sun Remote Procedure Call
113	113	Authentication Service
119	-	Network News Transfer Protocol
123	123	Network Time Protocol
161	161	SNMP (Total Control Manager)
162	162	SNMP trap
220	220	Interactive Mail Access Protocol v3
512	-	remote process execution
513	-	remote login (rlogin)
-	513	who
514	-	cmd
-	514	Syslog
515	-	lpd spooler
517	517	talk
518	518	ntalk

TCP	*UDP*	*Description*
-	520	RIP
540	540	uucp
540	540	uucp-rlogin
543	543	klogin
1642	-	PortMux daemon
-	1645	RADIUS security
-	1646	RADIUS accounting

Filtering RIP messages

If the NETServer is listening for or broadcasting RIP messages, you should permit them (UDP dst eq 520) to pass in the appropriate direction(s).

Note that spurious RIP messages can disrupt your routing tables. If you are listening for RIP messages on a given interface, you may wish to consider filtering out RIP updates from untrusted networks.

FTP Packet Filtering

FTP is one of the most difficult protocols to permit while still protecting your network. The input and output filters must permit two separate bi-directional connections, one initiated by the client and one initiated by the host. However, they should still be able to provide as much protection from outside attackers as possible. To write such a filter, we'll go through the FTP process and write the appropriate lines as we go.

In the example below, we will permit all users on the local class C network, *192.77.203.0*, to initiate an FTP connection to any other host on the Internet. However, incoming FTPs will be denied.

Step 1 - Create two filters

Since we will be filtering both incoming and outgoing packets, we must create two filters.

a. Select Filter from the Table menu.

b. When the Filter Configuration window appears, click on Create Filter. The Create New Filter window appears:

c. Type *ftp.in* and then click OK.

d. Create a second filter. This time enter the name *ftp.out*.

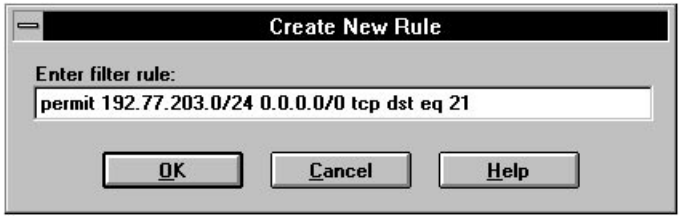
Step 2 - The client opens a control channel

To initiate an FTP session, the client opens a control channel on the well-known FTP port 21. This means any client on mynet.com must be able to send packets to TCP port 21 on any external host. This requires adding a rule to the filter *ftp.out*.

a. Pull down the Filter Names menu and select *ftp.out*.

b. Click on the IP tab.

c. Click Create New Rule.



d. Type the following and click OK:

permit 192.77.203.0/24 0.0.0.0/0 tcp dst eq 21

Step 3 - The host must reply

Allow packets coming from port 21 on any external host. To prevent intruders from using this opening, restrict the access to connections "established" by outgoing clients. Add the following rule to *ftp.in*:

```
permit 0.0.0.0/0 192.77.203.0/24 tcp src eq 21 established
```

Step 4 - The host opens a data transfer channel

Once a file transfer has been set up on the control channel, the host initiates a data transfer connection from port 20. However, we don't know what the destination port will be beforehand. To permit this connection, we would have to permit any external host initiating a connection from port 20 to connect to any port on any host on the internal network. Unfortunately, this also leaves the network open to any intruder initiating a connection on port 20. Since most standard services that are vulnerable to attack are below port 1023. We can block most of these attacks by forcing the host to connect to a port above 1023. Add the following rule to *ftp.in*:

```
permit 0.0.0.0/0 192.77.203.0/24 tcp src eq 20 dst gt 1023
```

Note: Since the ports above 1023 are still vulnerable, you should add additional rules that deny packets to any services you want to protect. These rules should be placed before the rule given.

Step 5 - The client must reply

The client must use the data transfer channel to send acknowledgment packets back to the FTP host. Add the following rule to *ftp.out*:

```
permit 192.77.203.0/24 0.0.0.0/0 tcp src gt 1023 dst eq 20
    established
```

FTP Example 2

If you also wanted to allow external clients access to a specific FTP server on your network, you could add a few more rules. In this example, our FTP server is 192.77.203.12. Add the following two rules to *ftp.in:*

```
permit 0.0.0.0/0 192.77.203.12/32 tcp dst eq 21

permit 0.0.0.0/0 192.77.203.12 tcp src gt 1023 dst eq 20
    established
```

Add the following two rules to *ftp.out*:

```
permit 192.77.203.12/32 0.0.0.0/0 tcp src eq ftp dst gt 1023
    established

permit 192.77.203.12/32 0.0.0.0/0 tcp src eq ftp-data  dst gt
    1023
```

Filtering ICMP packets

ICMP packets can only be filtered by type. So the only option is:

type <icmp message type>

For example, using the following rule in an input filter helps prevent potential vandals from changing your routing tables by sending ICMP redirects:

deny icmp type 5

The ICMP message types are listed below. Note that most of them are error messages necessary for the correct operation of TCP / IP:

Type	*Description*
0	Echo Reply (Ping)
3	Destination Unreachable
4	Source Quench
5	Redirect (change route)
8	Echo Request (Ping)
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

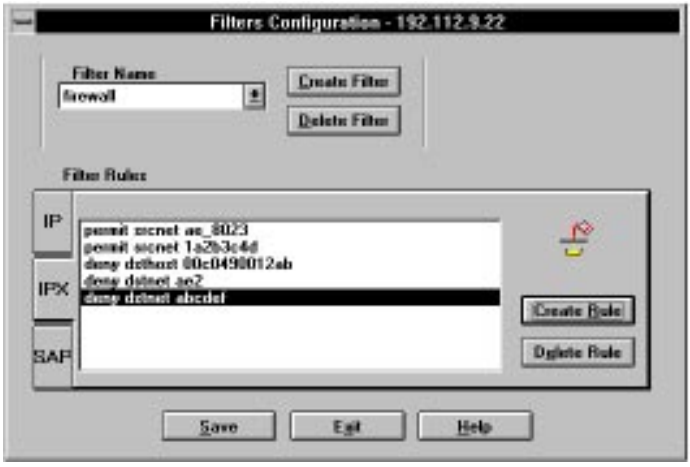
If you are concerned about security, filter out incoming type 5 messages. Sending ICMP redirects is an easy way for a vandal to change your routing tables.

Although PING is useful for troubleshooting, it allows a potential intruder to obtain a map of your network by systematically pinging every possible address. If you think this is a security risk, then filter out incoming type 8 packets or outgoing echo replies (type 0).

IPX packet filtering

IPX packets can be filtered by source and destination host, network or socket. Additionally, SAP packets can be specifically permitted or denied. Note that IPX network numbers must be specified as 8-digit hex values. Node addresses must consist of the 8-digit network number, followed by a colon and then the 12-digit MAC address.

IPX Rules



The IPX rule format is as follows:

<*permit* | *deny*> <keyword> <value>

<keyword> may be srcnet, dstnet, srchost, dsthost, srcsocket, or dstsocket.

srcnet

Compare the source IPX network number contained in the packet to the network number given. The network number must be in hexadecimal format.

<*permit* | *deny*> **srcnet** <IPX network number>

dstnet

Compare the destination IPX network number contained in the packet to the address given. The network number must be in hexadecimal format.

<*permit* | *deny*> **dstnet** <IPX network number>

srchost

Compare the source IPX node address contained in the packet to the address given. The IPX address should be in hexadecimal format.

<*permit* | *deny*> **srchost** <IPX node address>

dsthost

Compare the destination IPX node address contained in the packet to the address given. The IPX address should be in hexadecimal format.

<*permit* | *deny*> **dsthost** <IPX node address>

srcsocket

Compare the source IPX socket number contained in the packet to the socket number given. Valid comparisons are: less than (lt), equal (eq), or greater than (gt).

<*permit* | *deny*> **srcsocket** <*lt* | *gt* | *eq*> <socket number>

dstsocket

Compare the destination IPX socket number contained in the packet to the socket number given. Valid comparisons are: less than (lt), equal (eq), or greater than (gt). Example:

deny dstnet 000342BF dstsocket lt 32

If the destination at address 000342BF has a socket value of less than 32, the packet is discarded.

SAP Rule Options

SAP rules are only used in output filters. The rule format is as follows:

<*permit* | *deny*> <keyword> <value>

Possible keywords are server, network, host, and socket.

server

Compare the name of the advertising server to the specified server name.

<*permit* | *deny*> **server** <server name>

network

Compare the IPX network number of the advertised service to the specified network number. The IPX network number must be in hexadecimal format.

<*permit* | *deny*> **network** <IPX network number>

host

The IPX node address of the host advertising the service is compared to the node address specified. The IPX address must be in hexadecimal format.

<*permit* | *deny*> **host** <IPX node address>

socket

Compare the socket number of the advertised service to the number specified. Valid comparisons are: less than (lt), equal (eq), or greater than (gt). The following is an example:

permit server sales_1 socket lt 32

If the server name of the advertised service is sales_1 and its socket number is less than 32, the packet is permitted to pass.

Editing Packet Filters

See *Filter Rule Format*, earlier in the chapter for information on adding rules. For information on filter rule options, see the section specific to the type of packet filter you are editing.

How to . . .

Delete a Packet Filter Rule

1. Select Filters from the Table menu.
2. The Filter Configuration window appears. From the Filter Names list, select the packet filter you want to delete the rule from.
3. Select what type of rule you want to delete: IP, IPX, or SAP. Click on the tab designating that filter type.
4. Highlight the rule you want to delete.
5. Click on the Delete Rule button or press ALT-E.
6. A dialog box appears, asking you to confirm the deletion. Click on the OK button.
7. Another dialog box appears, telling you whether or not the rule was successfully deleted. Click on the OK button.
8. When you are finished, click on the Save button.

Delete a Packet Filter

1. Select Filters from the Table menu.
2. The Filter Configuration window appears. Select the packet filter you want to delete from the Filter Names list.
3. Click on the Delete Filter button or press ALT-D.
4. A dialog box appears, asking you to confirm your choice. Click on the OK button.
5. Another dialog box appears, telling you if the deletion was successful. Click on the OK button.
6. When you are finished, click on the Save button.

Insert a new rule in the middle of a packet filter

1. Select Filters from the Table menu.
2. The Filter Configuration window appears. Select the filter you want to create the rule for from the Filter Names list.
3. Click on the tab designating the type of rule you want to edit, delete, or create: IP, IPX, or SAP.
4. Click on the Create Rule button. Type the new rule and click OK.
5. Move the mouse pointer to the new rule in the Filter Rules box. You can now “Drag and Drop” the rule anywhere in the filter.
6. When you are finished, click on the Save button.

Save a Filter

When you are finished making changes to the filter, click on the Save button, or type ALT-S, to save the changes.

> **Note**: You are saving changes to the NETServer RAM, not to flash memory. To save the changes permanently to flash memory, you must select Save to FLASH from the File menu.

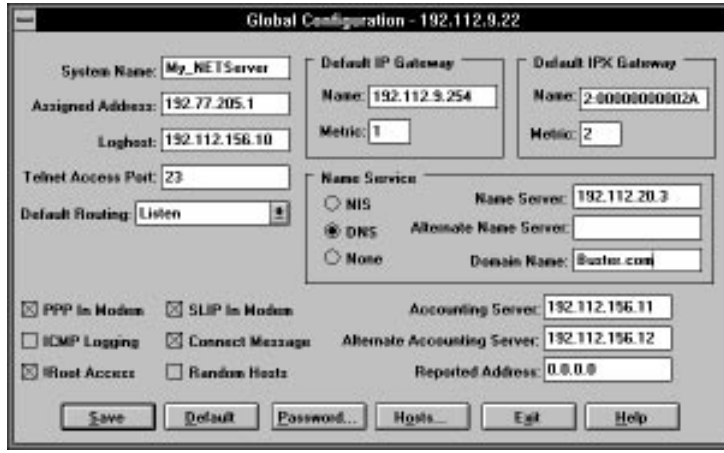
Chapter 9
Administrative Tools

This chapter covers the purely administrative functions of NETServer manager:

- Configuring the !root account
- Viewing administrative data

Configuring the !root account

This section covers settings in the Global Configuration window that control access to the supervisor account (!root).



!Root Access

Turning this off disables !root login through all S-ports except the console port (Port 1 on the NETServer/2. Port 0 on all other NETServers).

> **Note:** This command does not disable !root login via Telnet sessions. For information on disabling *Telnet access, see Telnet Access Port* below.

Telnet Access Port

You can reach the NETServer's command line by initiating a Telnet session and logging into the NETServer as !root. The Telnet Access Port identifies the specific TCP port number that the NETServer should listen to for incoming Telnet sessions. The default is 23, Telnet's well-known port number.

The Telnet Access port number can range from 1 to 65536. Note that 10000 through 10100 are reserved for an internal filter used for host device port security.

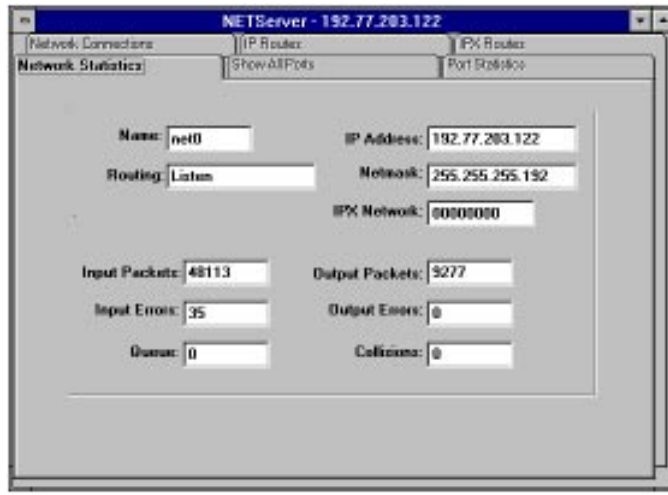
> **Security Note:** Some administrators consider using Telnet's well-known port (23) for remote administration a security risk since anybody can get a login prompt simply by telneting to the NETServer. This allows a potential vandal to attempt to guess your !root password, possibly seizing control of the NETServer.
>
> Changing to a non-standard port adds additional protection by making a potential vandal guess which port the NETServer is listening to.
>
> Alternatively, you may disable Telnet administration altogether by setting this parameter to 0.

NETServer Status Tabs

When you log into a NETServer, the first thing you see is a status window that lets you switch between informational displays by clicking on tabs. The tabs are *Network Statistics, Show all Ports, Port Statistics, Network Connections, IP Routes* and *IPX Routes.*

Network Statistics

This tab shows the status of the LAN (Net0) interface.



Name

Displays the name of the LAN port (Net0)

Routing

How the NETServer is handling RIP messaging on the LAN interface. Possible settings are:

Broadcast	The NETServer is broadcasting RIP to the LAN
Listen	The NETServer is listening for RIP messages coming from the LAN
Broadcast & Listen	The NETServer is doing both of the above.
Off	The NETServer is not exchanging RIP with the LAN.

IP Address

The IP address of the NETServer's LAN port

Netmask

The IP subnet mask of the LAN port

IPX Network

The network number of the cable attached to the LAN port.

Input Packets

How many packets the LAN port has received.

Output Packets

How many packets the LAN port has sent.

Input Errors

How many damaged packets the LAN port has received.

Ouput Errors

How many of the packets that were output through the LAN port caused an error condition.

Queue

How many packets are in the LAN port queue, waiting to be sent. This should normally be zero.

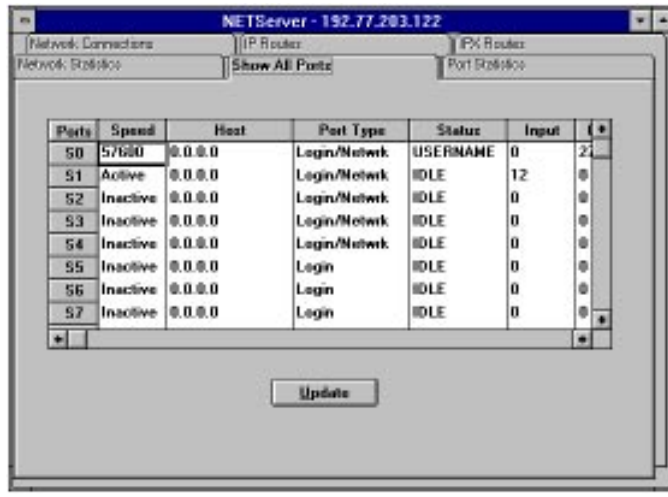
Collisions

How many collisions were detected on the LAN interface.

Note: Unlike the *show netstat* command available at the NETServer's command line, the Network Statistics tab does not show the status of point-to-point links.

Show all ports

This tab shows the status of all the S-Ports:



Speed

For the NETServer/2, NETServer/8, and NETServer/16, this column contains the baud rate of each S-port.

For the NETServer card, the baud rate is only displayed for S0. For S1 to S60, the field displays the status of the packet bus connection (Active/Inactive).

Host

If a login user is connected to a default host, the name or address of the host connected to is displayed. If a network user is connected to the port, the NETServer writes *ptp* is this field.

Port Type

The port type as configured in the Port Configuration window.

Login	User login port
Device	Host device port
2Way	Both user login and host device port
Network	Network dial in or dial out port

Status

Possible entries are:

COMMAND	!root account session
CONNECTING	Setting up connection
DISCONNECT	Disconnecting
ESTABLISHED	Connection is active
IDLE	The port is idle
USERNAME	Waiting for a user name

Input

The number of bytes that have been received from the port

Output

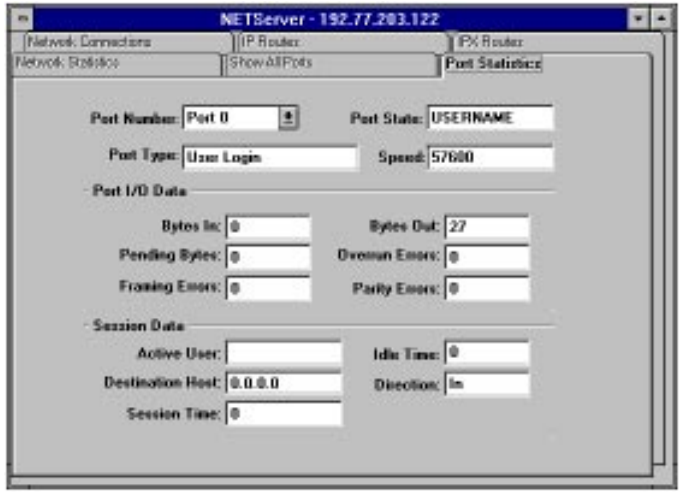
The number of bytes that have been sent out through the port

Pend

The number of bytes waiting in the output buffer

Port Statistics

This tab contains a more detailed status display of an individual S-port. Pull down the Port Number menu to select the port you want to view:



Port Type

The port type as configured in the Port Configuration window.

Login	User login port
Device	Host device port
2Way	Both user login and host device port
Network	Network dial in or dial out port

Port State

This indicates the port's state or whether or not the port is being used for a connection. Possible values include the following:

Idle	port is not in use
Established	connection is active
Command	Supervisor account session
User Name	port is waiting for user name
Connecting	port is trying to make a connection
Disconnect	port is disconnecting

Speed

For the NETServer/2, NETServer/8, and NETServer/16, this column contains the baud rate of each S-port.

For the NETServer card, the baud rate is only displayed for S0. For S1 to S60, the field displays the status of the packet bus connection (Active/Inactive).

Bytes In

This field indicates how many bytes of data have been input through the port.

Pending Bytes

This field indicates how many bytes are queued in the port's buffer, waiting to be output by the port.

Framing Errors

This field indicates how many misaligned bytes the port has encountered.

Bytes Out

This field indicates how many bytes of data the port has output.

Overrun Errors

This field indicates if the port's receive buffer has overflowed.

Parity Errors

This field indicates how many bytes with bit errors the port has received. A lot of parity errors can also mean that the modem or other data communications device (such as another NETServer) is set to a parity setting different from the NETServer.

Active User

This field indicates what user, local or remote, is currently connected to the port. Note that the user must be entered in the NETServer's User Table or a user name will not appear in this field.

Destination Host

This field gives the IP address of the host or network that the user is connected to. Note that this could be a local host or network that a remote user is connected to, or a remote host or network that a local user is connected to.

IPX destinations will show up as 0.0.0.0.

Session Time

This field indicates how long the user has been connected to the host, in hours and minutes.

Idle Time

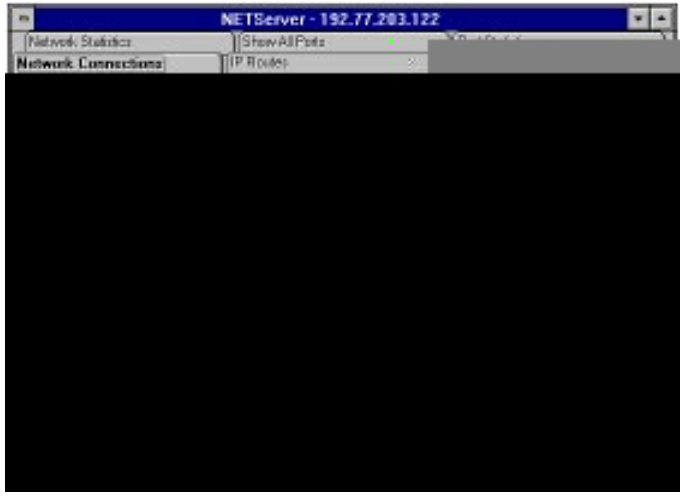
This field indicates the Idle Time-out setting for the current connection, if any. This determines how long, in minutes, the connection may remain idle before the NETServer breaks the connection.

Direction

This field indicates whether the current connection is inbound (remote user dialing in to a local host or the network) or out-bound (local user dialing out to remote host or network).

Network Connections

This summarizes all active connections to the NETServer, providing information on network use, IP socket allocation, and so on.



ID

This is the connection handle. The number can be used to reset the connection from the NETServer's command line.

Port

This indicates the port the connection is on.

Receive-Q

The number of packets in the connection's receive queue.

Send-Q

The number of packets in the connection's send queue

Local address

The address of the local port used for the connection

Foreign Address

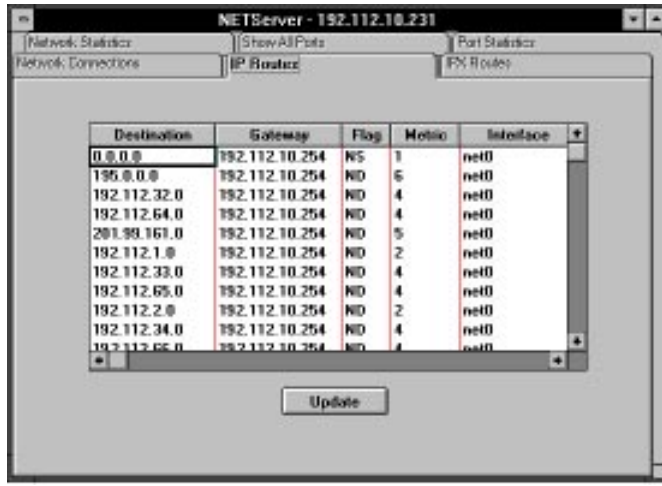
The address of the remote port used for the connection. IPX port addresses appear as 0000000.0

(State)

The status of the connection. Possible values include SPX LISTEN, UDP and LISTEN.

IP Routes

This displays the NETServer's IP routes table. It's format is similar to the IP Static Route Configuration window. However, this window displays both static and dynamic routes.



Destination

This is the IP address or name of the host or network to which the NETServer needs to send packets.

Gateway

This is the IP address of the host through which packets should be forwarded to reach the above destination.

Flag

This reflects a route's status and can be up to four letters long.

H or *N*	Host Route Network Route
S, *L* or *D*	Static Route Local (direct) Route Dynamic Route
C	The route has Changed
O	The route is Old and marked for deletion

Metric

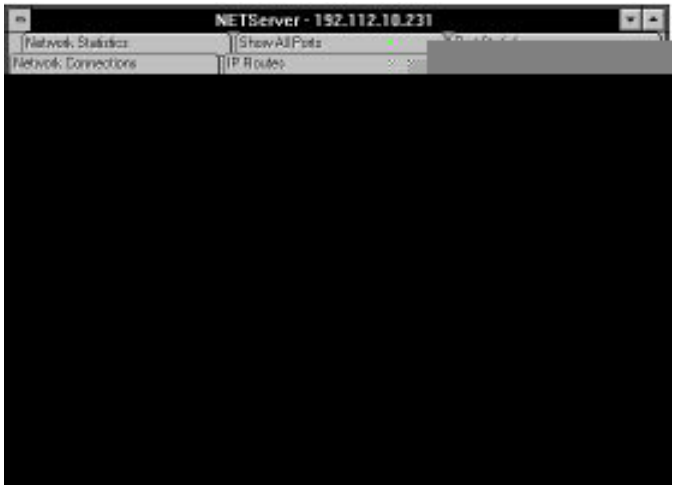
This is the number of hops to the destination.

Interface

This is the port through which packets be sent in order to reach the destination.

IPX Routes

This displays the NETServer's IPX routes table. It's format is similar to the IPX Static Route Configuration window. However, this window displays both static and dynamic routes.



Network

This is the IPX network number of the network to which the NETServer needs to send packets.

Gateway

This is the network node address of the gateway, bridge or router the packets will be forwarded through in order to reach the destination.

Flag

This reflects a route's status and can be up to four letters long.

H or *N*	Host Route Network Route
S, *L* or *D*	Static Route Local (direct) Route Dynamic Route
C	The route has Changed
O	The route is Old and marked for deletion

Metric

This is the number of hops required to reach the destination.

Ticks

This is how many clock ticks it will take to send a packet via a particular route. According to Novell, a tick is approximately 1/18th of a second (there are 18.21 ticks in a second).

Interface

This is the port through which packets be sent in order to reach the destination.

Chapter 10
Reference

This chapter contains a complete description of the following windows accessible through the Tables menu (in alphabetical order).

- Global Configuration
- The Hosts Table
- The Location Table
- Net0 (LAN port) Configuration
- The Netmasks Table
- The Ports Table (S-Port Configuration)
- RADIUS configuration
- SNMP Setup
- Static Route Configuration
- The User Table

Global Configuration

Global Configuration includes commands that affect every user and every port. Since this is a very large group of functions, we have broken it down into several categories including:

- User parameters
- Routing Parameters
- Name Service parameters
- Accounting Server Configuration

Technically, many of the administrative commands covered last chapter are also part of Global Configuration. However, we will not repeat them here.

How to . . .

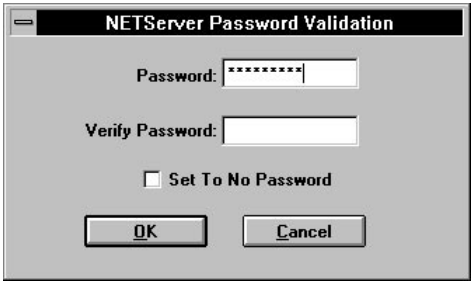
Save Changes

When you are finished making changes to the NETServer, click on the Save button.

> **Note:** You are saving changes to the NETServer RAM, not flash memory. To save the changes permanently to flash memory, you must select Save to FLASH from the File menu.

Set the Password for the Supervisor Account (!root)

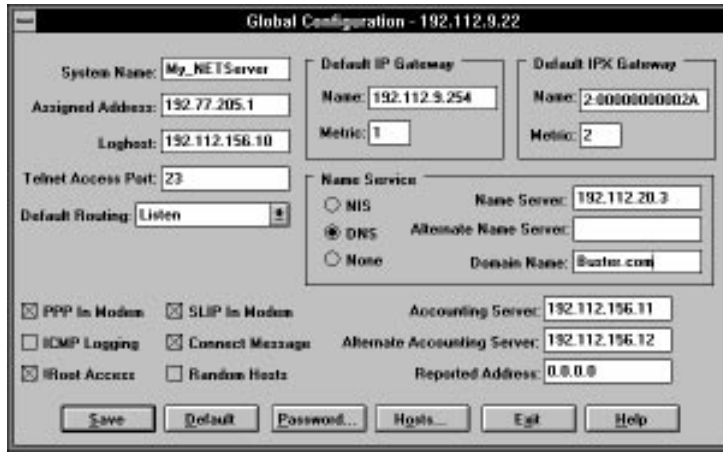
Click on the Password button. The password dialog box appears. Type the password (up to 15 characters) twice. Then, click the OK button.



Set the NETServer to its Default Configuration

Click on the Default button.

Global User Parameters



Assigned Address

The Assigned Address is the first in a block consecutive of IP addresses. Network users whose IP Address field is set to Assigned are given one of these IP addresses when they dial in to the NETServer. The assigned address pool contains as many addresses as there are ports in the NETServer (2 for the NETServer/2, 60 for the NETServer card, etc.)

Connect Message

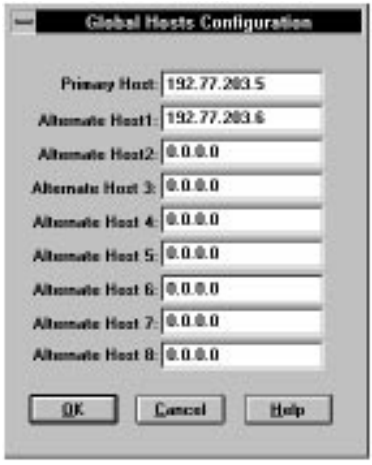
When this parameter is on, the NETServer will issue a “Connected” message to login users after they have successfully connected to a host. This can be useful when the host itself does not give such feedback.

Hosts....

By clicking on the *Hosts...* button, you can define a Global Default host and up to eight Global Alternate hosts. See also *Randomize Hosts*, below. Note that these settings are only used on networks that have Login Users (IPX networks do not).

Default Host

The Primary Host field contains the IP address of the host that a user will log into if there is no host specified in his or her user table entry *and* no host specified for the port he or she is connected to.



Alternate Hosts

If the Global Default Host is unavailable, a user will be directed to one of these alternate hosts.

Randomize Hosts

This command is used to relieve the burden on frequently-used global default, port default and RADIUS user table hosts.

When the Random Hosts function is turned off (default), the NETServer tries to connect the user to a default host first. If the default host is unavailable, he or she will be passed onto the first alternate host that is available.

When the random host command is set on, the user is connected to a random host selected from the default host and all the alternates. A different host is selected each time a connection is made.

Note: The flow of host selection from user table entry to RADIUS user file entry to Port Default Host to Global Default Host is the same regardless of the setting of this parameter. Randomizing hosts only affects the NETServer's choice of a Global Default vs. a Global Alternate Host, a Port Default vs. a Port Alternate Host, and of hosts in the RADIUS user's file

Global routing parameters

These fields configure routing on all ports.

Default IP and IPX Gateways

If the NETServer does not know where to send a packet, it forwards the packet to the default gateway specified here. Default gateways must be on the same subnet as the NETServer.

***Name** (IP)*

This is the IP Address or name of the Default IP Gateway.

***Name** (IPX)*

This is the full IPX node address of the Default IPX Gateway. It is written in hexadecimal format as shown below.

8 digit network number**:**12 digit node MAC address

Metric

You must also enter a metric (hop count) for each type of default gateway. Possible values range from 1 (default) to 15. Note that since the actual metric of a default gateway is only 1 hop, the value entered here is used to control the perceived cost of the gateway to other routers on your network. For example, a high metric will limit the number of hops that the route is broadcast and may cause other routers to see it as a less preferable route.

If the NETServer is configured to listen for IP default route broadcasts (see *Default Route* below), the IP Default Gateway can be overridden by a default route broadcast with a lower hop count.

Default Route

This field determines whether the NETServer will dynamically update IP default gateway information. The Default is *None.*

Broadcast & Listen	The NETServer will broadcast its default gateway information as part of normal RIP messaging and will also listen for default gateways broadcast by other routing devices.
Broadcast	The NETServer will broadcast its default gateway information as part of normal RIP messaging, but will not listen for default gateways.
Listen	The NETServer will listen for default gateway information coming from other routers. However, it will not broadcast its own default gateway information.
None	The NETServer does not send default gateway information to other routers and it will ignore all default gateway messages it receives.

Note: The NETServer will use a default route broadcast by another router only if Default Route is set to on or listen *and* the metric of the route received is lower than the metric of the IP Default Gateway. In such a case, the broadcast default route will override the Default Gateway setting.

PPP/SLIP in modem

When these fields are enabled, the modems will perform some of the SLIP and PPP packet processing themselves, taking some of the load off the NETServer's CPU. The default is both disabled.

Note that Quad Modems used with the NETServer card must be using 2.0.4 or later of the Quad V.34 modem code.

Reported Address

This field configures the IP address that the NETServer reports to remote networks. This allows more than one NETServer to appear to have a single IP address. The default is 0.0.0.0 (no IP address spoofing).

System Name

This is the NETServer's system name, 15 characters maximum. Required if your network uses a name service, SNMP, or IPX. A system name is also required if you will be using CHAP authentication. No other device on your network can be using this name.

Name Service

These fields configure the name service your network uses. A name service allows you to use host names rather than just IP addresses. The default is *none*.

NIS The network uses the Network Information Service (NIS). NIS is sometimes referred to as YP (Yellow Pages).

DNS The network uses the Domain Name Service (DNS).

None The network does not use a name service.

If you select DNS or NIS, you must also enter the Name Server and Domain Name.

Name Server

This is the IP address of the server providing the name service.

Alternate Name Server

This allows you to specify the IP address of an alternate name server.

Domain Name

This is the name of the domain that the NETServer belongs to. Both the primary and the secondary name servers must belong to the same domain.

Network Accounting

These fields configure the NETServer's use of accounting servers.

Accounting Servers

These fields specify the primary and alternate RADIUS accounting servers. RADIUS is an open protocol for network accounting. This allows the NETServer to send accounting messages to any one of a number of RADIUS implementations, including the network accounting support in U.S. Robotics' Total Control Manager version 3.0 (and above). The default for both the primary and the alternate accounting server is 0.0.0.0 (none).

Loghost

Enter a value in this field only if the NETServer will support UNIX Syslog network accounting. Type in the name or IP address of the server that functions as the Syslog host. The default is 0.0.0.0 (no Syslog host).

ICMP Logging

When this field is enabled, the NETServer logs ICMP errors such as Host Unreachable to the Syslog server. The default is disabled, which means that the NETServer does not forward these messages to Syslog. Note that the NETServer must be configured to use Syslog network accounting (see *Loghost).*

Hosts Table Configuration

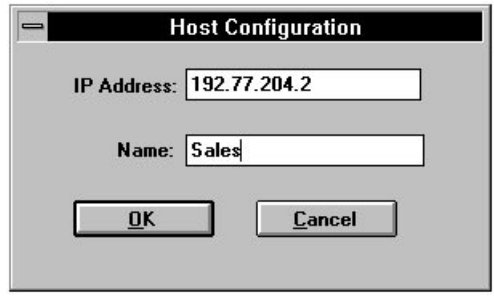
Like a name service, the hosts table translates names to IP addresses and vice versa. However, the hosts table is only used by the NETServer itself , rather than the entire network. If you are not using a name service and you want to use names rather than IP addresses, you must first create host table entries for all the hosts you want to refer to.

Note that when trying to match a name to an IP address, the NETServer will look check the hosts table before it consults a name server.

How to . . .

Add a Host

1. Click on the New button. The Host Configuration window appears.



2. Type in a Name and an IP address for the host.
3. Click on the OK button. The new host appears in the table.

Edit a Host

1. Select the host that you want to edit.
2. Click on the Configure button. The Host Configuration window appears.
3. Make the changes you want. Click on the OK button.

Delete a Host

1. Click on the host that you want to delete.
2. Click on the Delete button.

Save Changes

When you are finished making changes, click on the Save button.

> **Note:** You are saving changes to the NETServer RAM, not flash memory. To save the changes permanently to flash memory, you must select Save to FLASH from the File menu.
>
> If you exit the Hosts table and then return to it without saving to flash memory, you will not be able to see the hosts you configured on your last visit. This is because (unlike other tables) the Windows software reads the hosts table from flash memory rather than RAM. This will not mean that you lost previously configured hosts. You just won't be able to see them until you save them to flash.

Host Table Parameters

IP Address

This is the IP address of the host.

Host Name

This is the name of the host.

Location Table

Use the location table to define sites that the NETServer can dial out to (As opposed to Network Dial In, which requires a User Table entry).

How to . . .

Add a Location

1. Click on the New button.
2. Configure the required fields for the location. See *Location Table Parameters* for details on the fields.
3. Create the location's dial script by clicking on the Dial Script button. When you are finished, click on the OK button. See *Dial Script* for details.
4. Click on the Save button to save the new location.

Delete a Location

1. In locations box, highlight the location you want to delete (by clicking on it).
2. Click on the Delete button.

Edit a Location

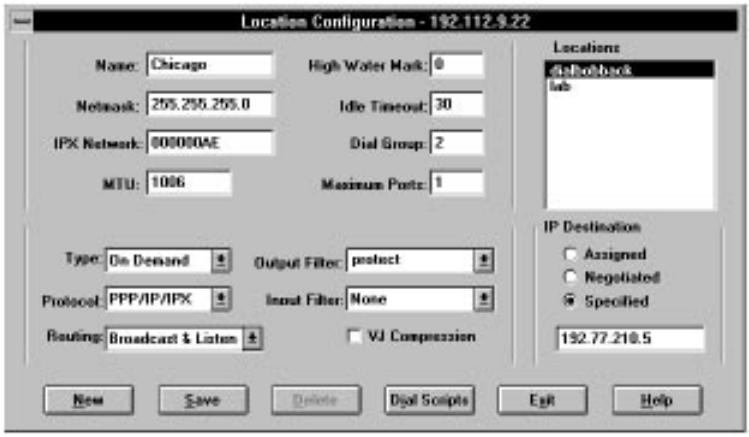
1. In locations box, highlight the location you want to edit by clicking on it. The location's settings will appear.
2. Make the changes. Click on Save when you are finished.

Save Changes to a Location

When you are finished making changes, click on Save.

Note: You are saving changes to the NETServer RAM, not flash memory. To save the changes permanently to flash memory, you must select Save to FLASH from the File menu.

Location Table Parameters



Compression

This field determines whether Van Jacobson TCP/IP header compression is used between the remote site and the NETServer. VJ Compression can improve TCP/IP session performance. The default is no compression.

If VJ compression is to be used on a SLIP connection, both sides of the connection must be configured to use it (CSLIP). If only one side is configured to use compression, the connection will fail.

With PPP connections, however, a NETServer with compression enabled will negotiate for compression, using it only with those locations that can use compression.

Dial Group

This field specifies which dial group (pool of modems) will dial-out to this location. Group numbers can range from 0 to 99.

Creating dial groups allows you reserve modems for dial-up to specific locations, or to ensure that the modems used to make the dial-up connection are compatible with the location.

When you configure a port, you can create a dial group by setting the Group Number field of one or more modem ports to the same number.

High Water Mark

This field determines when the NETServer should dial out with additional lines. This allows the NETServer to dynamically add more bandwidth to an existing connection. Additional lines are closed down when they are idle for the amount of time specified in the location's Idle Time-out field. The NETServer will add additional lines to the connection if all of the following are true:

- The number of bytes queued for the remote location exceeds the High Water Mark.
- There is an available port in the location's dial group.
- The number of ports currently being used for the connection is less than the Max Ports setting.

If you configure a small High Water Mark, the NETServer will use an additional line whenever one is available. A larger High Water Mark will cause the NETServer to use additional lines only when they are really needed, leaving them free for other uses. Keep in mind the kind of traffic you expect across the link. Light traffic, such as a user Telnet session, will usually only queue a few hundred bytes. File transfers, on the other hand, can easily queue several thousand.

The default High Water Mark is 0, which will immediately open the Maximum Ports (if they are available).

Idle Time-out

The field applies to On Demand locations only. This field specifies how many minutes a line can remain idle (no packets sent or received) before the NETServer hangs up. The idle timer ignores RIP, SAP and keepalive packets, allowing ports to time-out even though these protocols are running. The default is 0 (the lines never time- out)

Input Filter

Packets received from the remote location are evaluated against this filter and are discarded or accepted accordingly. Select the name of the filter you want to use.

See Chapter 8 for information on creating packet filters.

IP Destination

This field is the IP address of the location. You can set the IP Destination to *None*, *Negotiated* or, *Specified*. The default is None.

None — No address has been entered (actual value: 0.0.0.0). This disables the location for PPP connections.

Negotiated — The IP Destination is set to 255.255.255.255 which tells NETServer to try to learn the location's IP address using IPCP address negotiation.

This setting is only valid for PPP connections to locations whose *Type* field is set to Continuous. On-Demand locations require a specified IP address.

Specified — The location's IP address is specified in the box below.

IPX Network

While a dial up connection is up, it acts like a virtual network segment to which both and the NETServer and the remote location are attached. This is the IPX network number that will be assigned to that virtual network segment. It is *not* the number of a physical cable on either network

The IPX network number must be unique on both the remote and local networks; that is, no device or service may be using that exact network number.

Locations

The Locations box contains a listing of all available locations. You can switch from location to location by clicking on the name of the one you want to edit next.

Maximum Ports

This sets how many modem ports the NETServer can allocate for a single connection to the dial out location. The default is 0.

Possible Values

0 Users cannot dial-out to the location.

1 The NETServer will allocate only a single line (modem) to a session, regardless of the High Water Mark setting. This is the required setting if the remote device is not another NETServer.

2+ When the High Water Mark is exceeded, the NETServer will allocate additional lines until this number of ports are reached.

If the session is using multiple lines, the NETServer uses load balancing to maximize throughput. Also, when multiple lines are open, the NETServer uses the Idle Time-out setting to determine when to disconnect the additional lines.

For example, a local user connects to a location with a High Water Mark of 100 bytes and a Maximum Ports setting of 2. If the users are transferring large files, the traffic on that session's line would exceed the High Water Mark. The NETServer would allocate another line to handle the file transfer, closing the additional line when the traffic level decreases.

MTU

The Maximum Transmission Unit specifies the size of the largest packet that may be sent to the remote location. IPX connections will discard larger packets. IP connections will fragment larger packets. Normally, you should set the largest MTU possible. However, an IP connection using multi-line load balancing (see *High Water Mark*) may benefit from a smaller MTU.

Valid PPP MTUs range from 100 to 1500 (default is 1500). Note that PPP allows remote systems to negotiate a smaller MTU if needed. Valid SLIP MTUs ranger 100 to 1006 (default is 1006).

> If the connection will support IPX, MTU must be set to 1500.

Name

This is the name of the location, up to 15 characters maximum. The Name should be the name for the remote site in the remote network's SNMP server, domain server, or Novell bindery.

Netmask

This is the remote location's IP subnet mask. The default is 255.255.255.0, which would be appropriate for a Class C network with no subnetting or for Class C size subnets of larger networks. You must change this value if the remote location is using a different subnet mask.

Output Filter

Packets being sent to the remote location are evaluated against this filter and are discarded or accepted accordingly. Select the name of the filter you want to use.

See Chapter 8 for information on creating packet filters.

Protocol

This field indicates what protocol the NETServer should use to encapsulate packets bound for the remote location. The default is SLIP.

Your options are PPP / IP, PPP / IP / IPX, PPP / IPX, and SLIP.

Use the option that corresponds to how you have configured your NETServer and how the remote site is configured.

Routing

This is the level of RIP messaging between the NETServer and the remote site. The default is Broadcast & Listen.

None The NETServer does not exchange dynamic routing information with the location.

Broadcast The NETServer sends dynamic routing information to the location (but does not listen).

Listen The NETServer listens for dynamic routes received from the remote location (but does not broadcast).

Broadcast & Listen The NETServer sends route information to the location *and* accepts route information from the location.

Type

This field determines when the NETServer will dial out to the remote location. The default is On Demand.

Continuous The NETServer keeps the connection to the remote site active at all times. If the connection is broken for any reason, the NETServer automatically tries to reconnect.

On Demand The NETServer dials out to the remote device when it has packets queued for that location. It then maintains the connection only as long as there is traffic on the line. Note that dynamic routing information is updated while there is a connection between the two devices, but not before the NETServer dials or after it hangs up. When an on-demand connection is terminated, the NETServer retains current RIP and SAP information in memory (stops aging it). It then uses these last known values to "spoof" (fake) RIP and SAP broadcasts to active LAN and WAN connections. When an on-demand connection is first created, the NETServer will immediately attempt to dial the remote location to obtain some initial RIP and SAP values.

Dial Script

Click on the Dial Script button to bring up the Location Dial Script screen.

A Dial script tells the NETServer how to establish a connection to a given location. Every location requires a dial script.

A dial script contains the character strings the NETServer must send to the modem, for example, AT commands like ATDT5551234 (tone dial the number 555-1234). The dial script also contains the replies that the NETServer should wait for before it proceeds, for example, CONNECT.

For more information on AT commands, consult your modem reference materials.

Dial Script Format

Each Send string is issued to the modem, which may forward it to the remote location. Each Expect string verifies that the previous Send string was properly received and that the NETServer should transmit the next Send string.

You can specify up to 6 Send/Expect pairs. Each Send and Expect may be up to 20 characters long. Send strings should end with the *\r* character.

Expect Strings Case-Sensitivity

Dial script Expect strings are case-sensitive. What you type must be *exactly* what the NETServer will receive. For example, if you had a dial script Expect string of *connect*, but the actual reply was *CONNECT*, the NETServer would interpret the reply as not matching the dial script.

Special Characters

The send or reply strings can contain any printing ASCII character. Also, you may use the following special characters:

\r	ASCII carriage return
\n	ASCII line feed
\0XX	octal digit in the XX
\ \	single backslash (\)
“”	an empty reply string (expect no reply)

The Last String in a Dial Script

The last string in the dial script must be an Expect string that indicates the remote location is ready to begin receiving network packets. This activates the TCP / IP protocol coming from the NETServer.

For example, when connecting to a remote NETServer, the final Expect string should be *SL/IP* or *PPP*. For other products, consult that product’s documentation.

Dial Script Example

The following Dial Command Script is an example of how to establish a connection between two NETServers which have modems supporting the AT dial command syntax:

Send	**Expect**
ATDT18005551212\r	CONNECT
\r	login:
my_location_name\r	password:
my_password\r	SL/IP

The 18005551212 would be replaced by the actual telephone number of the remote modem. *my_location_name* would be replaced by the actual user name for your location. *my_password* would be replaced by the actual password set up at the remote site for that user name.

LAN Port Configuration

The LAN Port Configuration window lets you configure the Ethernet or Token ring interface.

You must reboot the NETServer after you save changes to the LAN port.

How to . . .

Save Changes

When you are finished making changes to the network port, click on the Save button to save the changes.

> **Note:** You are saving changes to the NETServer RAM, not flash memory. To save the changes permanently to flash memory, you must select Save to FLASH from the File menu.

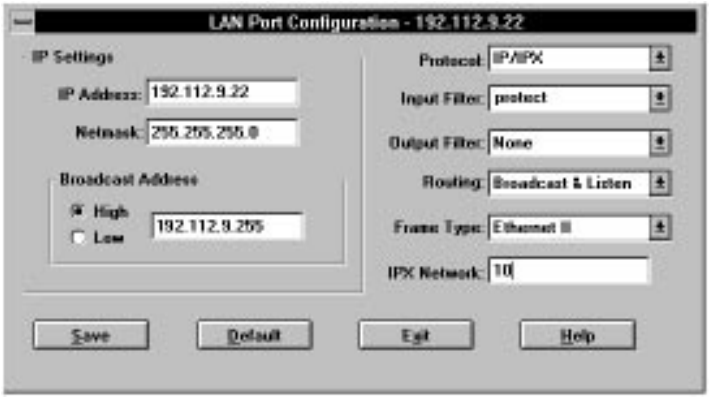
Set the LAN Port Configuration to its Defaults

Click on the Default button.

Undo Changes

Exit the screen without saving your changes.

LAN Port Parameters



IPX Parameters

IPX Network

This is the IPX network number of the LAN segment attached to the NETServer's Ethernet or Token Ring port. It corresponds to the IPX frame type described below and should be entered as an 8 -digit hexadecimal value. To find the IPX network number, use the Novell utility CONFIG on a server on the same network segment.

IPX Frame Type

The field sets the IPX frame type for the NETServer's LAN interface. You can select *Ethernet 802.2, 802.2 II, 802.3, Ethernet II, Token Ring 802.2, 802.2_II* or *Token Ring SNAP*. The default is Ethernet 802.2.

If the network segment has more than one frame type, choose the frame type that best suits your network. Keep in mind that you must enter the IPX network number associated with this frame type in IPX Network field described above.

IP Parameters

IP Address

This field contains the IP address assigned to the NETServer's LAN interface.

Netmask

This is the local network's IP subnet mask. The default is 255.255.255.0, which would be appropriate for a Class C network with no subnetting or for Class C size subnets of larger networks. You must change this value if the local network is using a different subnet mask.

Broadcast Address

The field sets the IP address that the NETServer interprets and uses as the local broadcast address.

High The bits of the host portion of a broadcast address are all ones. This is the rule for the vast majority of IP networks.

Low The bits of the host portion of a broadcast address are all zeroes. This is rare, but is still used by some systems, include SunOS 4.x (Solaris 1.x).

For example, the node 192.77.203.7 uses the default subnet mask of 255.255.255.0, which would give it a *high* broadcast address of 192.77.203.255 and a *low* broadcast address of 102.77.203.0.

Protocol

This is the protocol that the NETServer uses to communicate with the network. Default is IP. You can set the NETServer to IP, IP / IPX, or IPX.

Changes to this field do not take effect until you reboot the NETServer

IMPORTANT: Setting this field to IPX will prevent the Windows-based management software from communicating with the NETServer. If you want to use this software on an IPX network, you must select IP / IPX.

Input Filter

This filter controls which packets enter the NETServer through the Net0 (Token Ring or Ethernet LAN) interface. Packet filters control access by analyzing the header information of each packet of data received against a set of rules. If the packet meets the filter's criteria, it is allowed to pass through the interface (off the LAN and into the NETServer). The packet is discarded if it does not.

See Chapter 8 for more information on the construction and use of packet filters.

Output Filter

This filter controls which packets are allowed to exit the NETServer through the Net0 (Token Ring or Ethernet LAN) interface. Packet filters control access by analyzing the header information of each packet of data received against a set of rules. If the packet meets the filter's criteria, it is allowed out of the NETServer and onto the LAN. The packet is discarded if it does not.

See Chapter 8 for more information on the construction and use of packet filters.

Routing

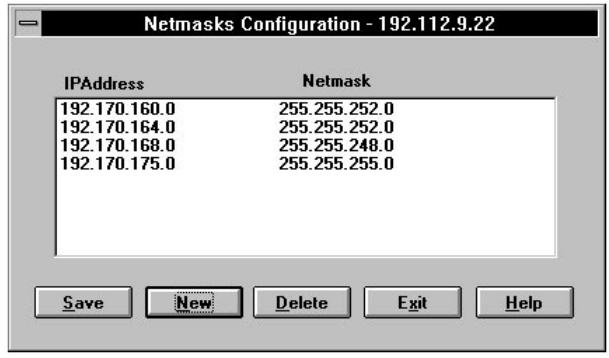
The field sets the level of RIP messaging or the exchange of dynamic routing information between the NETServer and the local network. The default is Broadcast & Listen.

Broadcast & Listen	The NETServer sends dynamic routing information to other computers attached to the local network and will use RIP information received from the LAN to dynamically update its routing table.
Broadcast	The NETServer sends dynamic routing information to other computers attached to the local network (but does not listen).
Listen	The NETServer accepts RIP information from other routers on the local network (but does not broadcast the entries in its own routing table).
None	The NETServer neither sends nor listens for RIP messages.

Netmasks Table

The netmasks table is used to define netmasks for Supernetting (Classless InterDomain Routing) . See the NETServer Command Reference for more information on this technique.

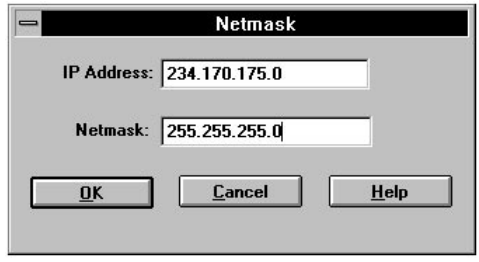
Alternatively, the netmasks table could be used to force the NETServer to advertise routes to individual hosts on a network (host-based routing) rather than a single route to the entire network. To do this, assign a netmask of 255.255.255.255.



How to...

Add a netmask

1. Click on the new button, the Add Netmask window appears.



2. Type in the IP address of the network that the netmask will apply to.
3. Type the new netmask in the Netmask box.
4. Click OK.
5. When the Netmask Configuration window reappears, click Save.

Delete a netmask

Click on the netmask you want to delete. Then, click the Delete button.

Undo your changes

Exit the window without saving them.

Ports Table (S-Port configuration)

The Ports table is used to configure the NETServer's use of devices that are connected to it by serial ports or by ports emulating serial operation.

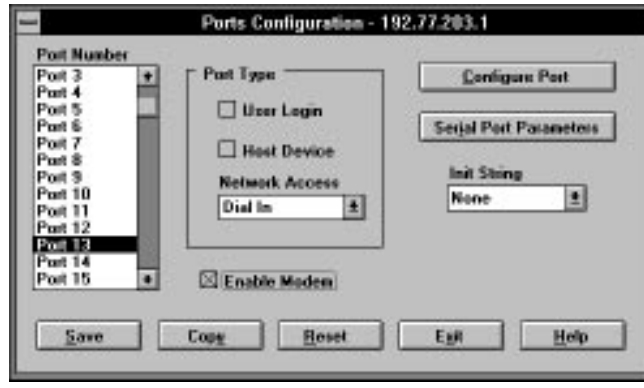
The NETServer/2, NETServer/8 and NETServer/16 all have internal serial ports (connected to modems) as well as an external serial interface.

In addition to the *CH1* serial interface, the NETServer card can configure a number of packet bus quad modems as if they were serial devices attached to the NETServer.

How to . . .

Configure a port (Quick overview)

1. Click on the port in the Port Number box.



2. If the Enable Modem box appears, the port is on a packet bus (NETServer card only). Activate the packet bus connection by checking this box.

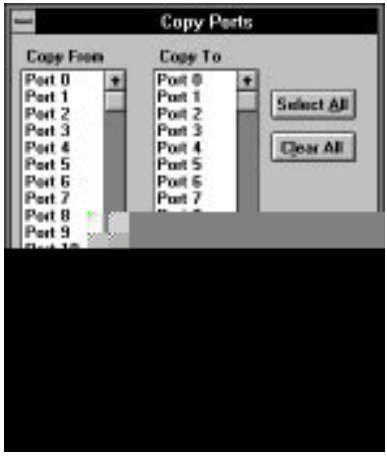
   If the Enable Modem box does not appear, the port is not on a packet bus and does not require this action.

3. Set the Port Type using the controls in the Port Type box. See *Determining a Port's Type*, later in this chapter, for an explanation of these options.

4. Click on the Configure Port button. The Port Parameters window appears. This window will display only the parameters available to the port type or types you have selected.
5. Configure the port parameters as needed for your application and then click OK.
6. When the Port Configuration window reappears, click on the Save button.
7. Click on the Reset button so your changes take effect.

Copy a Port's Entire Configuration to Another Port

1. Click on the Copy button. The Copy Ports window appears.



2. Click on the port you want to copy in the left column.
3. In the right column, click on a port or range of ports you want to copy to (You could also click Select All).
4. Click on the Copy button.
5. Click Exit.

Reset a Port

Click on the port in the Port Number box. Then click on the Reset button.

Undo changes

Exit the window without saving them.

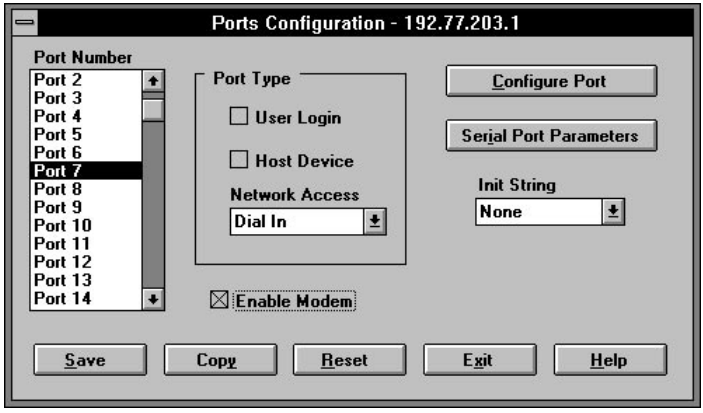
Set a Port to the Default Configuration

1. Click on the port in the Port Number box.
2. Click on the Configure Port Button
3. Click on the Default button.

Determining a Port's Type

Three fields determine what type of connection a port permits (set its port type). These fields are *User Login*, *Host Device*, and *Network Access.* The different port types are discussed below.

The default settings for a port are User Login enabled, Host Device disabled, and Network Access set to *Dial In*. This means that the port may be used for login sessions using a terminal service such as Telnet or for dial in PPP or SLIP connections, but may not be used for dial out use of any kind.



User Login

This setting allows login users to dial into the port. Once authenticated, login users are connected to a host on the local network using a service such as Telnet or Rlogin. See *Dial In Port Parameters* and *User Login Port Parameters*, later in this section, for more information on configuring User Login Ports.

Although Host Device may be enabled and Network Access may be set to *Dial In* and / or *Dial Out*, you may not set Network Access to *Hardwired* on a User Login port.

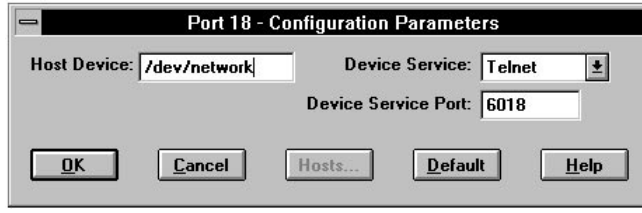
Host Device

A host device port allows IP users and hosts on the local network to attach directly to the modem's command line using a login service such as Telnet or Rlogin. This allows local users to share the port as a dial out modem.

Two pseudo TTY drivers that support the NETServer are available for UNIX hosts. A host running either one of these drivers can use a NETServer modem configured as a Host Device as if it were directly connected to the host's serial port. You can obtain these drivers (daemons call *nettty* and *in.pmd*) from the U.S. Robotics web site.

Although User Login may also be enabled and Network Access may be set to *Dial In* and / or *Dial Out*, you may not set Network Access to *Hardwired* on a Host Device port.

The Port Parameters window will look like this for a Host Device port:



Host Device

If you are not using one of the pseudo TTY drivers, type the following in this field:

/dev/network

If you are using a UNIX pseudo TTY drivers, this is the name of a UNIX pseudo TTY device listed in each host's / dev directory. See Chapter 7 for more information on using these drivers.

Device Service

Select the service that the users will login into the modem with. The default is Netdata, which provides a clear TCP connection to the port.

If you are not using a pseudo TTY driver, the choices are Telnet, Rlogin, and Netdata. If you want users to be forced to login before they are allowed to use the modem, you must choose Telnet.

Device Service Port

You must assign a TCP port number to host device modems. We suggest 6000 plus the modem number. However, a port number between 10000 and 10100 should be used if you want the users to login before they are allowed to dial out with the modem.

To reach the modem's command line, a user would connect to this port specifically. For example:

Telnet NETServer 6001

However, the NETServer does not allow outsiders to Telnet to 10000 - 10100 ports directly. If such a port number had been assigned, users would be forced to Telnet to port 23 first. This allows the NETServer to authenticate users and then forward them to the proper port.

Note: If you want to create a pool of modems that are available on a first come, first serve basis, assign all modems in the pool the same TCP port number.

Network Access

The Network Access field determines if the port permits PPP or SLIP connections. You may also enable User Login and Host Device (unless Network Access is set to *Hardwired*). The default is *Dial In*.

None — The port cannot be used for PPP or SLIP connections.

Dial In — Remote users may dial in to the NETServer and establish a PPP or SLIP connection with the local network. Remote networks dialing into the NETServer in order to route IP and IPX packets onto the local network also use ports configured this way. See *Dial In Port Parameters*, later in this section, for additional settings that apply to network dial in ports.

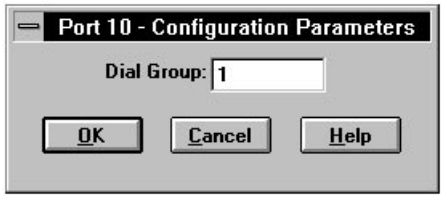
Dial Out — The NETServer uses dial out ports to establish dial out SLIP or PPP connections during LAN-to-LAN routing. Network dial out ports are also used for dialback network users. Network Dial Out ports have only one parameter (see *Dial Group*, below).

Dial In & Dial Out — This type of port supports both network dial in and network dial out.

Hardwired — User Login and Host Device must be disabled. This setting tells the NETServer's operating software that the port is connected directly to another device via a serial cable. Since the external serial port is the only serial port that can be used in this way, this setting is only valid for that port. See *Hardwired Port Parameters* for more information.

Dial Group

Network dial out ports must be assigned to a dial group. The dial group can then be assigned to one or more dial out locations.



Dial groups can have any number between 0 (default) and 99.

Dial In Port Parameters

These parameters apply to all ports that are configured for dial in. This includes both Network Dial In and User Login Ports.

Idle Time-out

This specifies how long the port can remain idle before the NETServer disconnects. Time-out range is from 0 to 240 minutes.

0 (Default) Never time-out

1 Login, password and host prompts time out in 5 minutes. However, there is no idle time-out on users who are already logged in.

2+ Login, password, and host prompts time out in 5 minutes. Users who are already logged in time out after the number of minutes specified.

Line Hang-up

This determines whether or not the port hangs up after the user session ends. The default is disabled.

If disabled, DTR does not drop after the user session ends. If enabled, the RS-232 DTR signal is momentarily dropped after the user session ends, causing the port to hang up.

Login Message

This is a message all users see before they login. The message can be up to 240 characters long. Use the caret (^) to represent a Carriage Return. All text entered after the caret will appear on the next line.

Login Prompt

This lets the system administrator customize the login prompt the user sees. The Login Prompt can be up to 15 characters.

If you include the string *$hostname* in the login prompt of a port configured for user login, the NETServer will insert the name of the port default host. If the port is configured for network dial in, but not user login, the NETServer will not display a host name. The default is *$hostname login:*, which displays the name of the port default host, followed by *login:*.

If you use quotation marks when you enter this string (either as delimiters or as punctuation), they will appear in the prompt.

Note: Many automated login scripting systems expect a login prompt to end in *login:*. Putting any character after the colon will cause some login scripts to crash.

Security (Pass-Thru Login)

This determines whether or not a user must be part of the NETServer User Table or the RADIUS users file to establish a connection with a host.

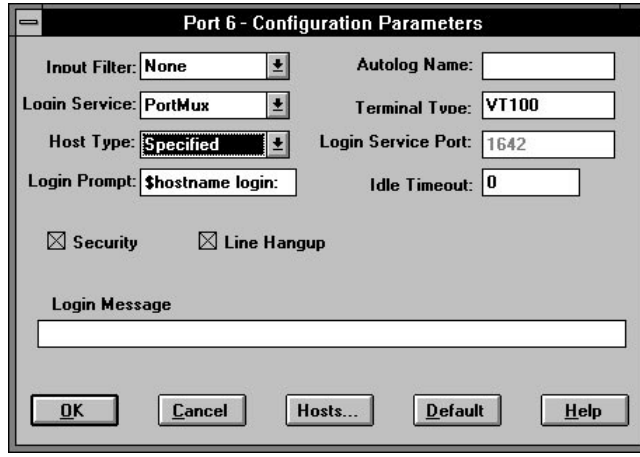
If security is left at its default (enabled) the NETServer will hang up on any users not in the User table or the RADIUS users file.

If security is disabled, users not in the user table are passed onto the host specified for the port without being authenticated. RADIUS will not be consulted. For example, you may wish the host to authenticate its own users, rather than using the NETServer to do this.

Note: If security is disabled, network users who are not part of the User Table are treated as if they are login users and passed on to the Default Host (or an alternate host).

Login Port Parameters

These parameters apply only to ports with User Login enabled.



Autolog Name

A user that enters the autolog name is automatically logged into the host. The autolog name can be up to 8 characters long.

Host Type

This field tells the NETServer what to do with users connected to this port who do not have a host specified in their user table entries.

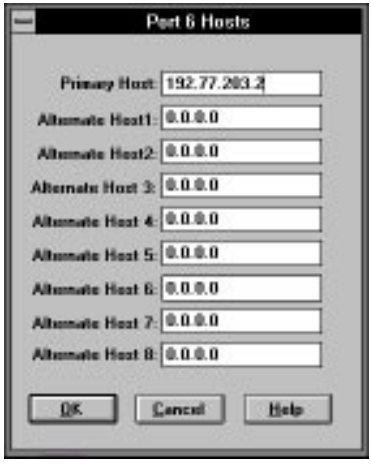
Default The port uses the Default Host and Alternate Host fields in the Global Configuration Table.

Prompt When users dial in, the port displays a host prompt. Users then type in the name or IP address of the host they want to connect to.

Specified The port uses the hosts specified by clicking on the *Hosts...* button.

Hosts...

When you click on this button, the screen below appears. These hosts are used only when the Host Type field is set to *Specified.*



You may enter host names or IP addresses for a Primary Host and up to eight Alternate Hosts. If for some reason the Primary Host is unavailable, the port will try to establish a session with the Alternate Hosts (in order).

Input Filter

This specifies an access filter that determines which hosts users connecting to this port are allowed to establish sessions with.

When a user specifies a host, the IP address of that host is compared against the permitted / denied IP addresses of the filter. If access is permitted, the user is allowed to establish a session with that host.

> **Note:** The access filter for an individual login user may override the filter specified here if the *access* parameter is set to *on* (This parameter is configurable at the command line only).

Information on creating packet filters can be found in Chapter 8.

Login Service

If a user does not have a user table entry and Pass-Thru Login is enabled, the NETServer will use the service specified here to connect the user to a host:

Telnet Supported by most TCP/IP computers, Telnet lets the user log in to hosts that support it. If you set a terminal type, Telnet will pass that information to the host. Otherwise, it negotiates a standard, Network Virtual Terminal interface (ASCII dumb terminal).

Rlogin Although originally available only on (BSD) UNIX machines, Rlogin has now spread to some other IP systems. Unlike Telnet, Rlogin allows a user logged into a host to access their accounts on other (trusted) hosts without reentering a password. Rlogin requires that you specify a terminal type.

PortMux (Default) Multiplexes many Telnet sessions, requiring fewer connections. This greatly reduces Telnet protocol overhead. PortMux is recommended for high bandwidth applications, such as the terminal server application X-Remote.

PortMux requires that the host be running the PortMux daemon (*in.pmd*). Note that this daemon also allows the host to use NETServer ports set to Host Device as pseudo TTYs.

Netdata Unlike Telnet, Rlogin, and PortMux, Netdata is not actually, a login service. Netdata is a direct (clear TCP) connection to a given TCP port number. 8-bit data is exchanged without interpretation. Such connections may be used by dial in applications that require a socket interface.

Login Service Port

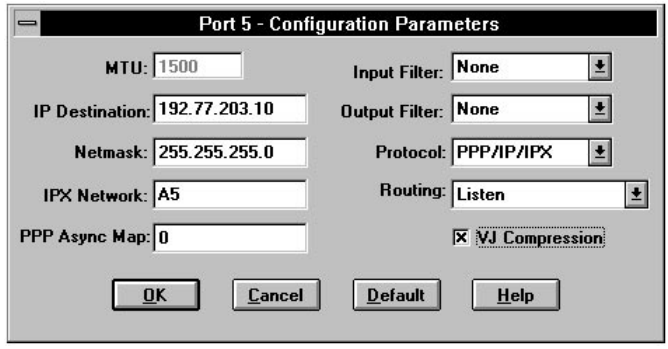
This is the TCP service port of the Login Service you selected in the previous field. We recommend that you leave this at the Login Service's default service port: Telnet (23), Rlogin (513), Netdata (6000), and PortMux (1642). Note that you cannot change the PortMux service port from its default.

Terminal Type

This is required only if Login Service is set to Rlogin. Telnet will use this information if it is provided or default to dumb terminal mode if it is not provided. This sets the login user's TERM environment variable for the session. You can find this information in the host's termcap or terminfo databases.

Hardwired Port Parameters

The parameters described below apply only to those ports whose Network Access field has been set to Hardwired.



Input Filter

Select the filter that controls what packets received from the remote site are permitted into the NETServer. See Chapter 8 for more information on packet filters.

IP Destination

This is the IP address of the remote site. If the destination is set to 255.255.255.255 for PPP connections, the NETServer will try to negotiate the remote IP Address. If set to 0.0.0.0 for PPP connections, the port is disabled.

IPX Network

This is the IPX network number of the serial cable connecting the NETServer to the other device. Note that the IPX network number must be unique to the networks on both ends of the serial connection.

MTU

The Maximum Transmission Unit is the largest frame or packet that can pass through this interface. If an IP packet's size is greater than the MTU setting, it's broken down into smaller pieces. IPX packets larger than the MTU are discarded.

PPP connections are set between 100 and 1500 (default is 1500). SLIP connections are set between 100 and 1006 (default 1006).

> The MTU must be 1500 for IPX connections.

Netmask

This is the remote network's Netmask. The default is 255.255.255.0, which would be appropriate for a Class C network with no subnetting or for Class C size subnets of larger networks. You must change this value if the local network is using a different subnet mask.

Output Filter

Select the filter that controls what packets are allowed to be sent to the remote site. See Chapter 8 for more information on packet filters.

PPP Async Map

The PPP protocol supports the escaping of non-printing ASCII characters. Escaping means that specific characters won't be sent, but will be replaced by a special set of characters. The remote site then interprets this special set of characters as the original characters

The PPP Async Map is a bit-map of the 32 ASCII control characters (the first 32 characters of the ASCII set) expressed as an eight-digit hexadecimal value. The order is big endian, which means that the low bit of the last hex digit corresponds to the first ASCII character, "null", and so on.

The default is 00000000 (do not escape any characters) We recommend that you do not change this field unless it is specifically required by your network.

Protocol

Default is SLIP. This field indicates what protocol the NETServer should use to encapsulate packets bound for the remote user or host.

Your options are PPP / IP, PPP / IP / IPX, PPP / IPX, and SLIP.

Routing

This field determines whether the port exchanges RIP messages (dynamic routing information) across the hardwired serial link. The default is Listen.

Listen	The NETServer does not send routing information, but does accept route information from the remote device.
Broadcast	The NETServer sends route information across the serial link as part of its normal RIP messaging, but will ignore routes received.
Broadcast & Listen	The NETServer both sends and receives routing information across the serial link.
None	The NETServer does not exchange routing information with the device on the other end of the serial link.

VJ Compression

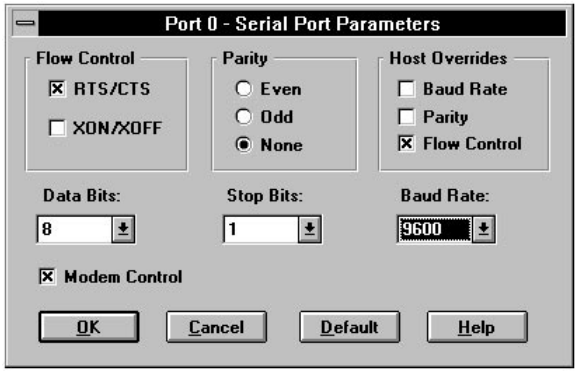
This field determines whether Van Jacobson TCP / IP header compression is used. The default is disabled.

Compression can improve TCP / IP session performance if both sides of the link support this option. Note that both sides of a SLIP connection must be configured identically. With PPP connections, however, if compression is enabled and the remote site doesn't support it, the NETServer disables compression.

Serial Communications Parameters

The following parameters configure the connection between the NETServer and the devices attached to its S-ports (usually modems). Naturally, the parameters used for configuring the real serial interfaces can be very different than the parameters used to configure packet bus ports emulating serial interfaces.

External Serial port only: These parameters may be overridden by DIP switch settings. Since DIP switch settings may vary from NETServer to NETServer, please consult the documentation specific to the NETServer you are configuring for more information.



Baud Rate

This is the baud rate between a serial port and whatever device (modem) is attached to it. Note that you cannot set the baud rate of packet bus ports since the packet bus has a fixed baud rate.

Databits

This is the number of data bits per character that the port is configured for. The default is 8.

Flow Control

This determines the type of flow control a serial port will use. Packet bus ports do not use these settings.

XON/XOFF Sets a serial port to software flow control. ASCII control characters stop and start the flow of data. Not recommended.

CTS/RTS Sets a serial port to hardware flow control. The RTS signal is raised or lowered on the RS-232 interface to indicate when it can and cannot receive data. The CTS signal is raised or lowered when it can or cannot send data.

Host Overrides

If a port is configured for host device use, you may choose to let the hosts override the communications settings of the port using software control. By default, all of the override settings are off.

Serial ports may be configured to allow overrides of flow control, databits, parity and baud rate.

Packet bus ports may be configured to allow overrides of databits and parity only.

Modem Control

This sets the serial port's Carrier Detect operations. If Modem Control is off, the NETServer ignores a carrier detect coming from the port. If Modem Control is on, the NETServer pays attention to the carrier detect signal.

In practice, modem control should be enabled for all modem ports that are configured for User Login and / or Network service. Modem control should be disabled only for ports that are configured for Host Device, but are not also configured for User Login and / or Network service.

Note: The Windows management software will automatically configure modem control when you set the port type.

Parity

This is the port's parity setting. The default is None.

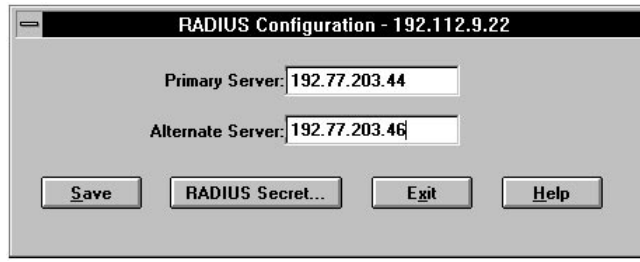
Stopbits

The number of stop bits used for the port. The default is 1.

RADIUS Configuration

This menu selection configures the NETServer's interaction with a RADIUS security server (such as the security option in Total Control Manager). The instructions below assume that RADIUS is already up and running on a workstation on your network.

1. Select RADIUS from the Tables Menu.



RADIUS Configuration Screen

2. The RADIUS Configuration screen appears. Type the name or IP address of your RADIUS security server in the Primary Server box.
3. If you wish to use an alternate RADIUS security server, you may also enter its name or IP address.
4. Click on the RADIUS Secret button. The RADIUS Secret Validation window appears.

This window sets the key that the NETServer uses to encrypt user IDs and passwords and that the RADIUS server uses to decrypt them. The encryption key can be up

to 15 characters long. The RADIUS server(s) must be set to the same encryption key.

5. Type the encryption key in the Secret field. Note that the encryption key is represented by asterisks.
6. Verify by typing the encryption key a second time (in the Verify Secret field)
7. Click OK.
8. Save your changes by clicking on the Save button.

Static Route Configuration

Static routes are required when the NETServer is not listening for RIP messages or when the network(s) attached to the NETServer cannot or do not run the RIP protocol.

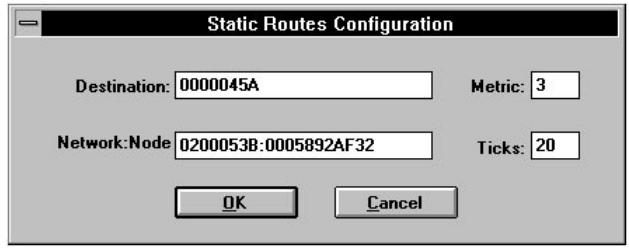
If your network does run RIP, you can use static routes to override the dynamic routes that RIP generates.

Note: Although the routes table may contain dynamic routes as well as static routes, this window will only display the static (user defined) ones.

How to . . .

Add a Route

1. Select Routes from the table menu.
2. When the Static Route Configuration window appears, click on the tab for the type of route you are adding (IP or IPX).
3. Click on the New button. The Route Configuration window appears.



4. Fill in the fields and then click the OK button.
5. Remember to click on the Save button before you leave the Static Route configuration window.

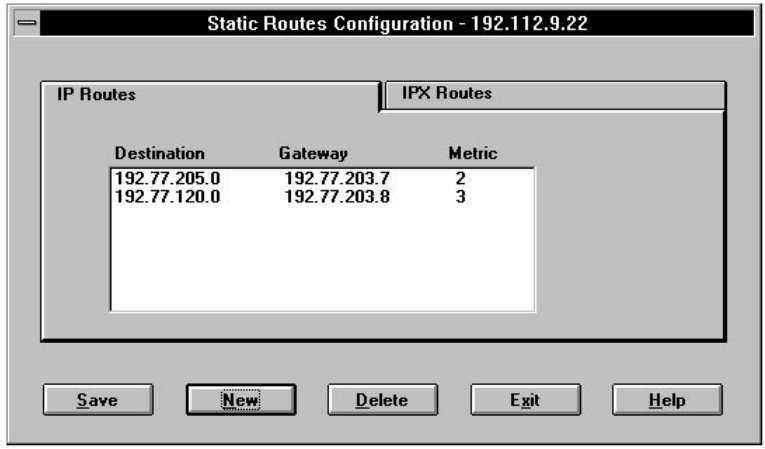
Delete a Route

1. Select Routes from the Tables menu
2. When the Static Route Configuration window appears, click on the tab for the type of route that you want to delete (IP or IPX).
3. Click on the route that you wish to delete.
4. Click on the Delete button.
5. Click on the Save button.
6. Remember to click on the Save button before you leave the Static Route configuration window.

Edit a Route

1. Select Routes from the Tables menu
2. When the Static Route Configuration window appears, click on the tab for the type of route that you want to edit (IP or IPX).
3. Click on the route you want to edit.
4. Click on the Configure button. The Routes Configuration window appears.
5. Make the changes and click the OK button.
6. Remember to click on the Save button before you leave the Static Route configuration window.

IP Routes Table Parameters



Destination

This is the IP address of the host or network to which the NETServer needs to send packets.

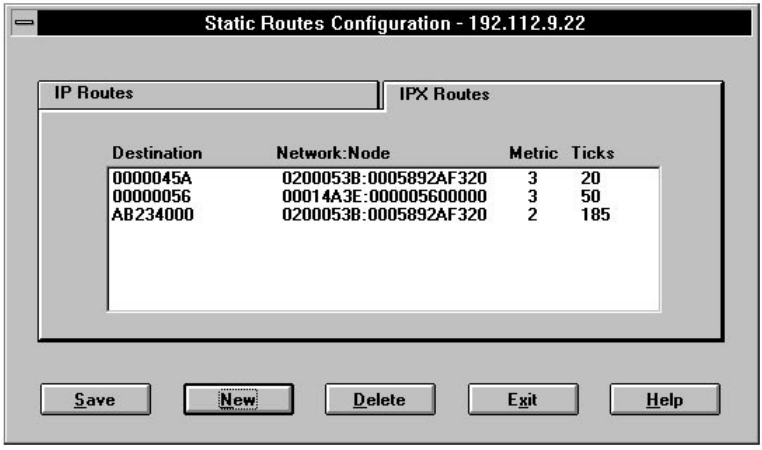
Gateway

This is the IP address of the gateway through which packets should be forwarded in order to reach the destination.

Metric

This is the number of hops or intervening gateways between the NETServer and the destination.

IPX Routes Table Parameters



Destination

This is the IPX network number of the host or network to which the NETServer needs to send packets.

Network Node

This is the network node address of the gateway, bridge or router the packets will be forwarded through in order to reach the destination. The format for the network node address is an eight digit hexadecimal address followed by a colon, and then a 12 digit hexadecimal address—for example 0200053B:00005892AF32.

Metric

This is the number of hops or intervening gateways between the NETServer and the destination.

Ticks

This is how many clock ticks it will take to send a packet via a particular route. According to Novell, a tick is approximately 1/18th of a second (there are 18.21 ticks in a second).

SNMP Configuration

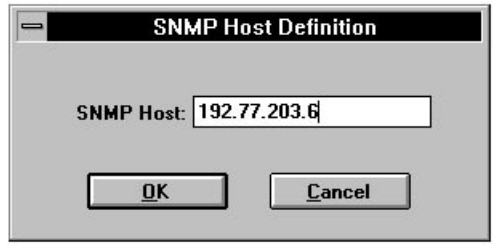
The NETServer provides support for using the Simple Network Management Protocol (SNMP) and supports industry standard MIB-II variables. These variables are fully described in your MIB-II documentation.

How to . . .

Add SNMP Hosts to the Hosts Box

Note that this box is only used when Host Type is set to Specified.

1. Click on the New button. The Host Definition window appears.



2. Type the name or IP address of the new host.
3. Click OK
4. Remember to click on Save before you exit the SNMP window.

Delete an SNMP Host from the Hosts Box

1. Click on the Host you want to delete.
2. Click on the Delete button.

Undo changes

Exit the window without saving them.

Global SNMP Parameters

These settings are global SNMP settings. For information on SNMP read parameters, see *SNMP Read Parameters.* For information on SNMP write parameters, see *SNMP Write Parameters*.

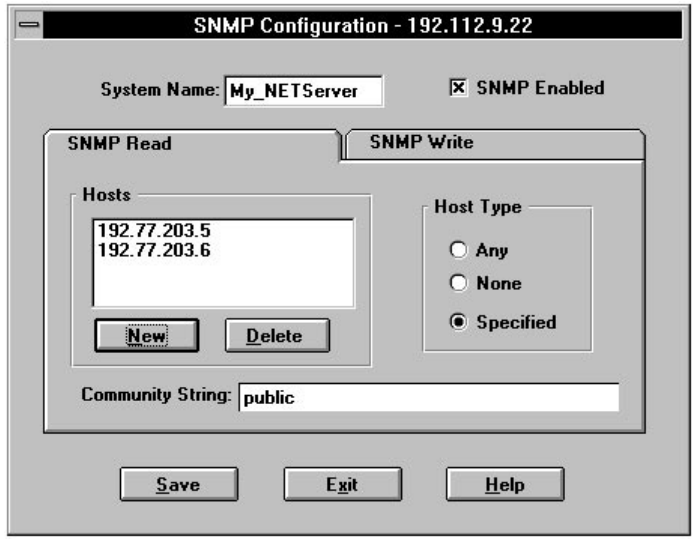
System Name

This is the global SNMP system name. It is used as the system identifier in CHAP requests and for LAN to LAN routing. It is also the name used to identify the NETServer in SAP broadcasts.

SNMP Enable

Default is disabled (box is not checked). If disabled, the NETServer ignores SNMP requests. If enabled, the NETServer permits SNMP Set requests.

SNMP Read Parameters



Hosts

If the Host Type is set to *Specified*, this box lists the SNMP hosts that may retrieve information from the NETServer.

Host Type

This specifies which hosts that may issue SNMP queries to the NETServer. The default is any.

Any Any host with the correct read community may retrieve SNMP data from the NETServer.

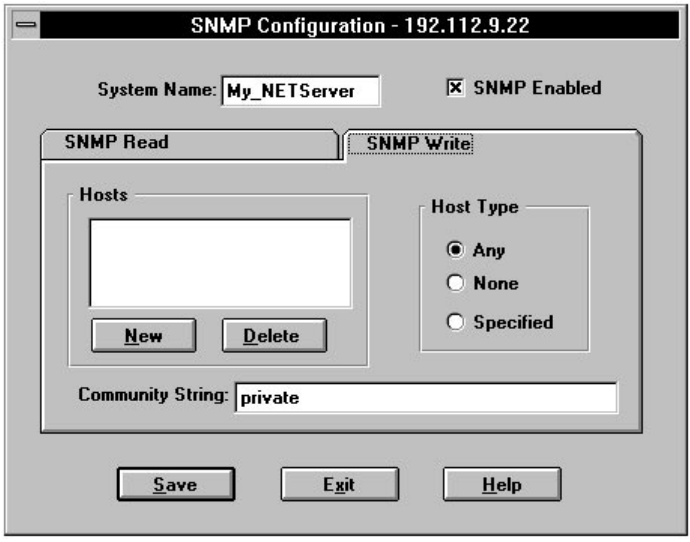
None The NETServer will not respond to any attempts to retrieve SNMP data.

Specified A specific list of hosts may retrieve SNMP data from the NETServer. Use the New and Delete buttons to add or delete SNMP hosts to the Hosts box.

Community String

The SNMP read community is a kind of password. Only devices that know the correct Read Community string may read the NETServer's MIB information. The default is *public*.

SNMP Write Parameters



Hosts

If Host Type is set to *Specified*, this box lists the SNMP hosts that may write information to the NETServer.

Host Type

This field sets the type of SNMP host that may write to the NETServer.

Any Any host with the correct read community may write SNMP data on the NETServer.

None The NETServer will not respond to any attempts to set SNMP data.

Specified A specific list of hosts that may write SNMP data to the NETServer. Use the New and Delete buttons to add or delete SNMP hosts.

Community String

The SNMP write community is a kind of password. Only devices that know the correct Write Community string may read the NETServer's MIB information. The default is *private*.

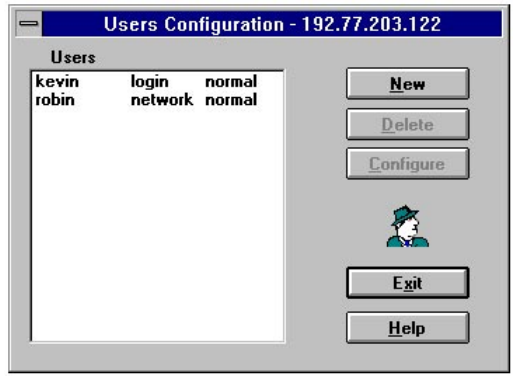
User Table Configuration

The User Table defines users who may dial into the local network to become virtual nodes or to establish login sessions with local hosts.

How to . . .

Add a User to the Table

1. Select User from the Table menu.



2. Click on the New button. The default user type screen appears (the Network User Parameters screen).
3. If creating a login user, set the user type to Login. (The Login User Parameters screen appears).
4. Type the user name in the Name Field.
5. Set the parameters needed by the user.
6. Click on the OK button.

Delete a User

1. Select User from the Table menu.
2. Click on the user you want to delete.
3. Click on the Delete button.

Edit a User

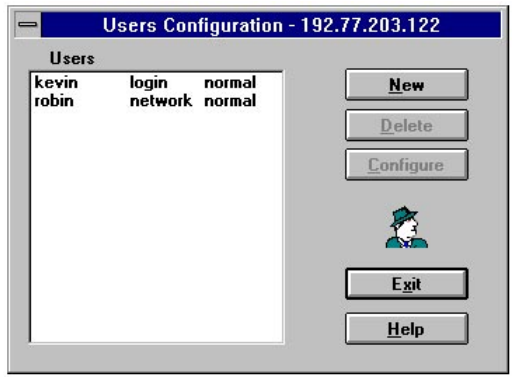
1. Select User from the Table menu.
2. Click on the user you want to edit.
3. Click on the Configure button. Depending upon the type of user you are editing, the Login User Parameters or Network User Parameters screen appears.
4. Make changes as needed.
5. Click on the OK button to return to the User Table Configuration screen.

Set the User Parameters to the Default Configuration

When you are in the Login User or Network User Parameter windows, you can set the parameters to the default configuration by clicking on the Default button.

User Table Configuration Parameters

The User Table Configuration screen has a Users box that contains all the users in the Users Table.



When you click on New or select a user to configure, either the Network User Parameters screen or the Login User Parameters screen appears. The fields that follow appear in both. See *Login User Parameters* and *Network User Parameters* for specific information on each screen.

Name

This is the name of the user. The User Name can be up to 8 characters long. User names are case sensitive.

You cannot have a login and network user with the exact same user name (both spelling and case). For example, you cannot have both a login user and a network user named *Bob*. However, a login user *Bob* and a network user *BOB* are allowed.

Password

Click on the Password button to set the user's password. The User Password Validation dialog box appears.

Type in the password and then verify it. Click OK when finished. The password can be up to 15 characters long and is case-sensitive.

If you want to allow a user who already has a password to go back to using no password, click on *Set to No Password.*

User Type

This is the type of user. The default is Network User.

Login User Login Users emulate terminals connected to an IP host. The NETServer logs these users into a host using a login service such as Telnet or Rlogin.

Network User Network Users become virtual nodes on a network (with their own IP addresses and / or IPX Network Numbers) via a PPP or SLIP connection.

Normal or Dialback Access

This box selects either normal or dialback use. The default is Normal.

Normal Once the user's name and password are verified, the user immediately begins an active session.

Dialback Once the user's name and password are verified, the NETServer disconnects and dials a pre-defined telephone number (login user) or location (network user).

Login User Parameters Window

Access Filter

This specifies an access filter that determines which hosts this user is allowed to establish sessions with (useful when Host is set to *Prompt*).

When the user specifies a host, the IP address of that host is compared against the permitted / denied IP addresses of the filter. If access is permitted, the user is allowed to establish a session with that host.

> **Note:** The input filter for the port the user is connected to will override the filter specified here if the port's *access* parameter is set to *off* (This parameter is configurable at the command line only).

Information on creating packet filters can be found in Chapter 8.

Dialback Number

Required only for dialback users. This is the pre-defined number that the NETServer will dial after verifying the user's name and password. It can be any valid string, and can include AT-compatible modem command characters. You do not need to include the *AT* part of the AT command (the NETServer does that for you). For example, T1-800-555-5555 or 5551234.

Host

This determines which host the login user will establish a session with. The default is *Default*.

Default The user is connected to the host specified for the port he or she is using. If no host is specified for the port, the global default host is used.

If the Default Host is unavailable, the login user will be connected to an alternate host.

Prompt After user name and login are verified, the user is prompted to enter the name or IP address of a host.

Specified The user is connected to a specific host. Type the name or IP address of the host in the box on the right.

Login Service

Default is Telnet. The NETServer uses the service specified here to log the user into the desired host. Valid options are:

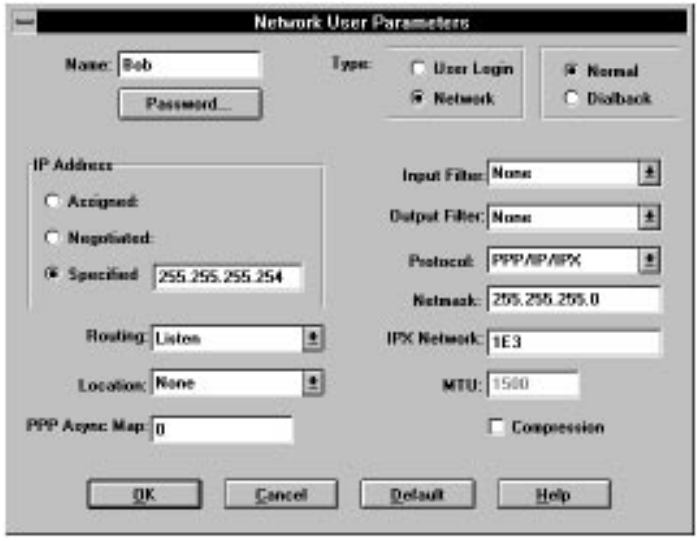
Telnet Supported by most TCP/IP computers, Telnet lets the user log in to hosts that support it. If you set a terminal type for the port the user connects to, Telnet will pass that information to the host. Otherwise, it defaults to dumb terminal mode.

Rlogin Although Rlogin was originally a (BSD) UNIX only protocol, it is now supported by some non-UNIX machines as well. Unlike Telnet, Rlogin allows a user logged into a host to access their account on other (trusted) hosts without reentering a password. Rlogin requires that you specify a terminal type for the port.

PortMux Multiplexes many Telnet sessions, requiring fewer connections. This greatly reduces Telnet protocol overhead. PortMux is recommended for high bandwidth applications, such as the terminal server application X-Remote. PortMux requires that the host run a special PortMux daemon (in.pmd). Note that this daemon also allows the host to use NETServer ports set to Host Device as pseudo TTYs (see Chapter 7). A UNIX version of the PortMux daemon is available on the U.S. Robotics web site.

Netdata Unlike, Telnet, Rlogin and PortMux, Netdata is not actually a login service. Netdata is a direct (clear TCP) connection to a given TCP port number. 8-bit data is exchanged without interpretation. Such connections may be used by dial in applications that require a socket interface.

Network User Parameters Window



Compression

This field determines whether Van Jacobson TCP / IP header compression will be used between the remote site and the NETServer. The default is no compression.

Compression can improve TCP / IP session performance if both sides of the link support this option. Note that both sides of a SLIP connection must be configured identically. With PPP connections however, if compression is enabled and the remote site doesn't support it, the NETServer disables compression.

Input Filter

Enter the name of the packet filter that will screen all packets received from the user.

See Chapter 8 for information on creating packet filters.

IP Address

This is the IP address that the user has for the duration of the connection. There are three options: *Assigned*, *Negotiated*, and *Specified*.

Assigned — You may select this option only if you have specified an IP address block in the Assigned Address field of the Global Configuration window. The NETServer assigns the remote user a temporary IP address from this block of addresses.

Negotiated — PPP connections only. The NETServer attempts to learn the remote IP address using IPCP negotiation.

Specified — The user's IP address is specified here.

IPX Network

To the networks on either end of an IPX dial connection, the virtual link between the NETServer and the remote device will appear to be a physical network segment. This is a unique IPX network number assigned to that virtual network segment. It must be unique on both the NETServer's local network and any network attached to the dial in user.

Location

Dialback users only. When the user is authenticated, the NETServer disconnects and makes a connection with the specified location selected here (must be created in the location table).

MTU

The Maximum Transmission Unit specifies the size of the largest packet that can be sent to this user. IPX connections will discard larger packets. IP connections will fragment larger packets prior to transmission. Normally, this should be set to the largest value that both the user and the local network can handle.

Valid PPP MTUs range from 100 to 1500 (default 1500). Note that PPP allows a remote system to negotiate a smaller MTU if needed. SLIP MTUs range from 100 to 1006 (default 1006).

> MTU must be set to 1500 for IPX connections.

Netmask

This is the network user's IP subnet mask. The default is 255.255.255.0, which would be appropriate for a Class C network with no subnetting or for Class C size subnets of larger networks. You must change this value if the user requires a different subnet mask.

Output Filter

Enter the name of the packet filter that will screen all packets sent to the user.

See Chapter 8 for information on creating packet filters.

PPP Async Map

The PPP protocol supports the escaping of non-printing ASCII characters. Escaping means that specific characters won't be sent, but will be replaced by a special set of characters. The remote site then interprets this special set of characters as the original characters

The PPP Async Map is a bit-map of the 32 ASCII control characters (the first 32 characters of the ASCII set) expressed as an eight-digit hexadecimal value. The order is big endian, which means that the low bit of the last hex digit corresponds to the first ASCII character, "null", and so on.

The default is 00000000 (do not escape any characters) We recommend that you do not change this field unless it is specifically required by your network.

Protocol

This field indicates what protocol the NETServer should use to encapsulate packets exchanged with the user. The default is SLIP (IP only).

Your options are PPP / IP, PPP / IP / IPX, PPP / IPX, and SLIP.

Routing

This field determines whether the NETServer exchanges dynamic routing information with the user. The default is None.

Broadcast The NETServer sends RIP messages to the user, but does not listen for RIP updates from the user.

Listen The NETServer listens for RIP messages from the remote user, but does not send them.

Broadcast The NETServer sends RIP messages to the user and listens for RIP messages received from the user.

None The NETServer does not exchange RIP messages with the user.

Appendix A

Virtual Ports

When an ISDN call comes in, the NETServer dynamically allocates bandwidth for the connection as signaled by the ISDN D-channel. This has the effect of creating a virtual port that the NETServer's operating software can interact with as it would one of the quad modem ports.

Note: The initial release of the NETServer PRI firmware supports connections of single B-channel size only.

Since these ports are dynamically created, they cannot be configured beforehand. The NETServer itself configures these ports as required for the connection.

For example, the NETServer will respond to a dial in ISDN call with a virtual port configured to support both user login and network dial in. From then on, the login proceeds normally, the NETServer sends a login prompt out to the dial in user. If the user replies to the prompts, the connection proceeds according to his or her user table entry. PAP and CHAP authentication can also be used for PPP login.

Note: The initial release of the NETServer primary rate ISDN firmware does not support network dial out or host device dial out over ISDN. Check your release notes for added feature support.

When a connection is torn down, the virtual port is terminated and its bandwidth is returned to the pool of available resources.

Service Profiles

When the NETServer creates a virtual port for a dial in connection, it tries to match the call to an appropriate service profile, a template for virtual port configuration. To do this, it searches the Call Mapping Table for an entry that matches the dialed number (DNIS), the called number (ANI) or both.

If there is no matching entry in the Call Mapping Table, the NETServer looks for a rate adaption protocol (such as V.110 or V.120) specified in the ISDN D-channel.

> **Note:** Neither V.110 or V.120 are supported in the initial release, which supports only a clear, synchronous ISDN channel (no rate adaption protocol).

If no protocol is specified in the D-channel, or if the D-channel specifies that no protocol will be used, the NETServer takes the call and uses the default service profile for no protocol, *default_sync*.

If a rate adaption protocol supported by the NETServer is found, the NETServer accepts the call and maps it to the default service profile for that protocol. The initial release does not support any rate adaption protocols.

If the D-channel specifies a protocol that the NETServer does not support, the NETServer will not accept the call.

Creating your own service profiles

In rare cases, ISDN call signaling may be incorrect for some calls (you will probably never see this). This is almost certainly the result of the call passing through an older switch that doesn't fully support ISDN. Such switches may not properly forward D-channel data. If this happens, certain calls will simply fail to connect.

If you suspect that the D-channel signaling is incorrect or you want to force a specific configuration, you can create your own service profile, which essentially tells your NETServer not to believe the local telco switch. To use your own service profile you have to do three things:

1. Add a new service profile
2. Configure it
3. Create at least one call mapping table entry that uses the new profile
4. Save your work

Step 1 - Add a new service profile

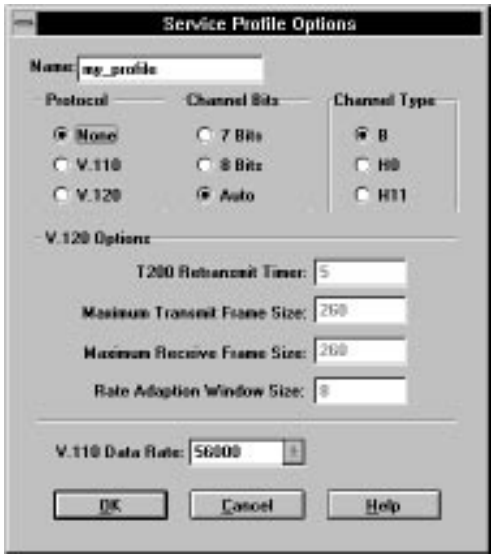
a. Select ISDN PRI, Service Profile from the Table menu. The Service Profile Configuration window appears.

b. Click on New. Enter the name of the service profile. The name can be up to 32 characters long.

Step 2 - Configure the service protocol

The initial release of the NETServer PRI firmware supports three service profile parameters, *Data Rate, Protocol,* and *Channel Type.*

You can also configure the default service profile for any rate adaption protocol. This allows you to configure all calls using that protocol that do not have an entry in the call mapping table. Default service profiles cannot be deleted. *default-sync* is the only default service profile supported by the initial release.



Data rate

This parameter configures the capacity of the bearer channel. In the United States, service is more than likely 8-bit. In Europe, you are more likely to find 7-bit. In either case, it is usually safest to go with the default setting, *auto*.

force-7bit	Forces all incoming calls to use a data rate of 56 Kbps
force-8bit	Forces all incoming calls to use a data rate of 64 Kbps
auto	Incoming calls will be automatically switched between 56 Kbps and 64 Kbps as dictated by ISDN D-channel signaling.

Protocol

This configures the rate adaption protocol. These settings override D-channel signaling. Note that you cannot change the protocol of a default service profile.

none	The NETServer to try to answer these calls as clear, synchronous connections.
V.110	The NETServer will try to answer these calls using V.110
V.120	The NETServer will try to answer these calls using V.120.

Note: Although the NETServer Manager software supports V.110 and V.120 configuration for forward compatibility, these options cannot be used with the initial release of the NETServer PRI firmware. Check your release notes for more information on protocols supported by the latest release.

Channel Type

This configures the maximum size of the data channel. The NETServer will reject all calls signaled as larger than the channel size specified here.

Note: The initial release of the NETServer PRI firmware supports only channel Type B.

V.120 Options

These options apply specifically to the V.120 protocol.

T200 Retransmit Timer	The number of seconds to wait for a packet acknowledgment before attempting error recovery (retransmitting the packet). The default is 5.
Max. Transmit Frame	The largest frame that may be sent across the link. This value corresponds to the ISDN N201 parameter. The default is 248 bytes with a maximum of 260.

> **Note:** Because of protocol overhead, the actual amount of data sent or received is one or two bytes less than the value configured here.

Max. Receive Frame	The largest frame that the NETServer will accept from the link. Larger packets will be discarded. You must configure the N201 parameter on the remote device equal to or lower than this value. The default is 260 bytes (the maximum).
Window Size	The maximum number of frames that the NETServer will transmit without receiving an acknowledgment. This corresponds to the ISDN "k" parameter. The default is 8.

V.110 Data Rate

This sets the speed (in bps) of V.110 connections.

Step 3 - Configure Call Mapping

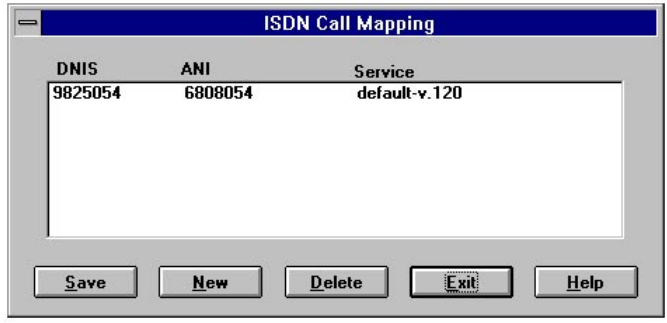
Entries in the call mapping table allow you to dictate which service profile will be used based on the number users are dialing (DNIS), the number users are calling from (ANI), or both.

The NETServer will try to match the ANI and DNIS numbers of in incoming call to a service profile in the following order:

1. An entry that matches both the ANI and the DNIS numbers.
2. An entry that matches just the ANI number
3. An entry that matches just the DNIS number

Adding a call map entry:

a. Select ISDN PRI, Call Maps from the Table menu. The ISDN Call Mapping window appears.



b. Click on New. The Call Mapping Configuration window appears.

c. Pull down the Service Profile box and select a profile

d. Fill out one or both of the *Number* fields. These fields are strings of characters representing phone numbers. The exact format of these strings will vary . Check with your telco provider to find out the format of DNIS and ANI numbers provided by your local ISDN switch.

ANI If you enter a number here, it will be compared to the number from which a call originates. If there is a match, the profile selected in the Service Profile box will be used.

DNIS If you enter a number here, it will be compared to the number dialed. If there is a match, the profile selected in the Service Profile box will be used.

> **Note:** If both DNIS and ANI numbers are entered, the profile selected will only be used if both numbers are matched.

e. When you are finished, click OK.

Step 4 - Save your work

Click Save before you leave the ISDN Call Mapping window.

Alphabetical Index

E

F

G

H

I

L

M

N

T

U

V

W