

LRA502A-ET-R5  
LRA504A-ET-R5  
LRA508A-ET-R5  
LRA502A-TR-R4  
LRA504A-TR-R4  
LRA508A-TR-R4

# **Remote Access Servers**

**( Ethernet & Token Ring )**

## **Installation Guide**

---

## Copyrights

Copyright 1995-2002, Black Box Corp.

Apple, Macintosh, and AppleTalk are trademarks of Apple Computer Inc.

IBM, AT, CA/400, and PC Support/400 are registered trade marks of International Business Machines Corporation.

Microsoft, MS-DOS and Windows are registered trade marks of Microsoft Corporation.

Novell and NetWare are registered trademarks of Novell, Incorporated.

All other trademarks mentioned in this document are the property of their respective owners.

## FCC/DOC Compliance Statements

NOTE: This equipment has been tested and found to comply with the limits for a Class A Digital Device, pursuant to Part 15 of the FCC rules and to DOC Radio Interference Regulations, C.R.C., c1374. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC/DOC compliance requires that all I/O cables used with Black Box products be constructed using shielded cable, metal-shelled connectors and conductive backshells.

CAUTION: Changes or modifications to a Black Box product which are not expressly approved by Black Box Corp. may void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

---

Copyrights	ii
FCC/DOC Compliance Statements	ii
Preface	xiii vii
About this Guide	xiii vii
About the Document Set	xiv vii
Chapter 1: Introduction	1 vii
Black Box Remote Access Server	1 vii
Supported Protocols	1 viii
Dial-In	1 viii
Dial-Out	2 viii
Manager Program	3 viii
Initial Configuration	3 viii
Over the LAN	3 viii
Direct Connect	4 viii
Dial-In Connection	6 viii
Chapter 2: Black Box RAS Hardware Installation	7 viii
Hardware Overview	7 viii
Black Box Remote Access Server Models	8 viii
Front Panel	8 viii
LEDs	9 viii
Hardware Installation for Ethernet Black Box Remote Access Server	10 viii
Hardware Installation for Token-Ring Black Box Remote Access Server	12 viii
Setting the IP Address	13 viii
Modem Installation	14 viii
System Defaults	14 viii
Chapter 3: Manager Software Installation and Setup	15 viii
Manager Overview	15 viii
Connection	15 viii
Client Software	16 viii
System Requirements	16 viii
Installing Manager Software	17 viii
Connecting to the Black Box Remote Access Server	18 viii
In-band Connection	18 viii
Direct Connection	18 viii

Dial-In Connection	20	viii
Server List	20	viii
Update Firmware	22	viii
Manager Main Screen	23	viii
Menu bar	24	ix
File Menu	24	ix
View Menu	25	ix
Configure Menu	25	ix
Statistics	26	ix
Event Log	26	ix
Window Menu	27	ix
Help Menu	28	ix
Tool bar	28	ix
Chapter 4: Server Configurations	31	ix
Configuration Overview	31	ix
Open Configuration File	32	ix
Configuration File Window	33	ix
Server Options	34	ix
Server Filter Assignment	36	ix
Setting the date and time	37	ix
Serial Port Options	37	ix
User List Options	40	ix
User Records	40	ix
User List Access	40	ix
Shared User Lists	40	ix
Save Configuration File	40	ix
Download the Configuration	41	ix
Protocol Enable/Disable	42	ix
Event Log	42	ix
Dialing prefix/port	43	ix
Packet Filtering	43	ix
Chapter 5: Configuring Network Protocols	47	ix
IP Parameters	47	ix
IP Requirements	48	ix

---

Configuring IP Parameters	49 ix
Client IP Addresses	50 ix
Addresses for Direct Polling	53 ix
IP Static Routing	55 ix
Configuring IP Static Routing	55 ix
IP Filter Definition	57 ix
Add / Edit IP Filter Definition	58 x
IPX Parameters	59 x
IPX Requirements	59 x
Configuring IPX Parameters	59 x
IPX Static Routes	61 x
IPX Network Services	61 x
Configuring IPX Static Routing	61 x
MAC addresses	65 x
MAC addresses and RAS	x
Fixed MAC Addresses	65 x
IPX Filter Definition	67 x
Add / Edit IPX Filter Definition	67 x
AppleTalk Protocol	69 x
NetBEUI	69 x
Chapter 6: User Records	71 x
Overview	71 x
Configuring a User Record	71 x
Shared User Lists	74 x
Call Back Options	75 x
User Filter Assignment	77 x
Dial-In Modem Pools	78 x
Configuration Steps	78 x
Chapter 7: Dial-In	81 x
Overview	81 x
Configuring Dial-In	81 x
Using Windows 95 Dial-up Networking	82 x
What You Need	82 x
Configuring a New Connection	82 x

- Making a Dial-Up Networking Connection83 x
- Call Back Options83 x
- Using Apple Remote Access84 x
- Configuration84 x
- Chapter 8: Dial-Out85 x
- Overview85 x
- Configuring Dial-Out85 x
- Port Dial-Out Parameters86 x
- Configuration Steps86 xi
- Server Dial-Out Parameters90 xi
- Configuration Steps90 xi
- Dial-Out Modem Pools91 xi
- Configuration Steps91 xi
- Chapter 9: Network Administration93 xi
- What is SNMP?93 xi
- Configuration Steps94 xi
- Trap Hosts95 xi
- Communities and Community Tables95 xi
- Viewing Statistics97 xi
- IPX Network Numbers98 xi
- Information Presented for Ports99 xi
- Event Log101 xi
- Software Upgrades102 xi
- Chapter 10: Security103 xi
- Overview103 xi
- Server Access103 xi
- Network Access104 xi
- PAP and CHAP105 xi
- Call Back106 xi
- Generic User106 xi
- Security Services Configuration107 xi
- Administrative Privileges107 xi
- Network Access107 xi
- User List108 xi

Netware	108	xi
RADIUS	109	xi
External Hardware	111	xi
Axent	112	xi
SecurID	114	xi
NT Domain	117	xi
Generic User	118	xi
Front Panel Lock	120	xi
Chapter 11: Front Panel	121	xi
Overview	121	xi
Front Panel Language	121	xii
Navigational Rules	122	xii
Editing Fields	122	xii
Menu Structure	123	xii
Menu Descriptions	128	xii
Chapter 12: Custom Server Configuration	133	xii
Creating a Custom Modem Configuration	133	xii
Modem String Commands	134	xii
Changing Link Control Protocol Parameters	135	xii
Changing the Async Control Map	137	xii
Appendix A: Pinout and Cable Diagram	139	xii
Asynchronous Connector Pinout	139	xii
Pinout	139	xii
Null modem cable	140	xii
Introduction	140	xii
Diagram	140	xii
Appendix B: Hardware Specifications	141	xii
Glossary	143	xii
<b>Preface</b>		<b>xiii</b>
About this Guide		xiii
About the Document Set		xiv
<b>Chapter 1: Introduction</b>		<b>1</b>
Black Box Remote Access Server		1

Supported Protocols.....	1
Dial-In .....	1
Dial-Out .....	2
Manager Program.....	3
Initial Configuration.....	3
Over the LAN .....	3
Direct Connect.....	4
Dial-In Connection .....	6
<b>Chapter 2: Black Box RAS Hardware Installation .....</b>	<b>7</b>
Hardware Overview .....	7
Black Box Remote Access Server Models .....	8
Front Panel.....	8
LEDs.....	9
Hardware Installation for Ethernet RAS.....	10
Hardware Installation for Token-Ring RAS.....	12
Setting the IP Address.....	13
Modem Installation .....	14
System Defaults .....	14
<b>Chapter 3: Manager Software Installation and Setup .....</b>	<b>15</b>
Manager Overview.....	15
Connection.....	15
Client Software.....	16
System Requirements.....	16
Installing Manager Software.....	17
Connecting to the Black Box Remote Access Server .....	18
In-band Connection .....	18
Direct Connection.....	18
Dial-In Connection .....	20
Server List.....	20
Update Firmware .....	22
Manager Main Screen .....	23



Menu bar .....	24
File Menu .....	24
View Menu .....	25
Configure Menu .....	25
Statistics .....	26
Event Log .....	26
Window Menu .....	27
Help Menu .....	28
Tool bar .....	28

## **Chapter 4: Server Configurations ..... 31**

Configuration Overview .....	31
Open Configuration File .....	32
Configuration File Window .....	33
Server Options .....	34
Server Filter Assignment .....	36
Setting the date and time .....	37
Serial Port Options .....	37
User List Options .....	40
User Records .....	40
User List Access .....	40
Shared User Lists .....	40
Save Configuration File .....	40
Download the Configuration .....	41
Protocol Enable/Disable .....	42
Event Log .....	42
Dialing prefix/port .....	43
Packet Filtering .....	43

## **Chapter 5: Configuring Network Protocols ..... 47**

IP Parameters .....	47
IP Requirements .....	48
Configuring IP Parameters .....	49
Client IP Addresses .....	50
Addresses for Direct Polling .....	53
IP Static Routing .....	55
Configuring IP Static Routing .....	55
IP Filter Definition .....	57

Add / Edit IP Filter Definition .....	58
IPX Parameters .....	59
IPX Requirements .....	59
Configuring IPX Parameters .....	59
IPX Static Routes .....	61
IPX Network Services .....	61
Configuring IPX Static Routing .....	61
MAC addresses .....	65
MAC addresses and RAS .....	65
Fixed MAC Addresses .....	65
IPX Filter Definition .....	67
Add / Edit IPX Filter Definition .....	67
AppleTalk Protocol .....	69
NetBEUI .....	69

**Chapter 6: User Records ..... 71**

Overview .....	71
Configuring a User Record .....	71
Shared User Lists .....	74
Call Back Options .....	75
User Filter Assignment .....	77
Dial-In Modem Pools .....	78
Configuration Steps .....	78

**Chapter 7: Dial-In ..... 81**

Overview .....	81
Configuring Dial-In .....	81
Using Windows 95 Dial-up Networking .....	82
What You Need .....	82
Configuring a New Connection .....	82
Making a Dial-Up Networking Connection .....	83
Call Back Options .....	83
Using Apple Remote Access .....	84
Configuration .....	84

**Chapter 8: Dial-Out ..... 85**

Overview .....	85
Configuring Dial-Out .....	85
Port Dial-Out Parameters .....	86

---

Configuration Steps.....	86
Server Dial-Out Parameters.....	90
Configuration Steps.....	90
Dial-Out Modem Pools.....	91
Configuration Steps.....	91
<b>Chapter 9: Network Administration.....</b>	<b>93</b>
What is SNMP?.....	93
Configuration Steps.....	94
Trap Hosts.....	95
Communities and Community Tables.....	95
Viewing Statistics.....	97
IPX Network Numbers.....	98
Information Presented for Ports.....	99
Event Log.....	101
Software Upgrades.....	102
<b>Chapter 10: Security.....</b>	<b>103</b>
Overview.....	103
Server Access.....	103
Network Access.....	104
PAP and CHAP.....	105
Call Back.....	106
Generic User.....	106
Security Services Configuration.....	107
Administrative Privileges.....	107
Network Access.....	107
User List.....	108
Netware.....	108
RADIUS.....	109
External Hardware.....	111
Axent.....	112
SecurID.....	114
NT Domain.....	117
Generic User.....	118
Front Panel Lock.....	120
<b>Chapter 11: Front Panel.....</b>	<b>121</b>
Overview.....	121

Front Panel Language.....	121
Navigational Rules .....	122
Editing Fields.....	122
Menu Structure.....	123
Menu Descriptions .....	128
<b>Chapter 12: Custom Server Configuration .....</b>	<b>133</b>
Creating a Custom Modem Configuration.....	133
Modem String Commands.....	134
Changing Link Control Protocol Parameters.....	135
Changing the Async Control Map .....	137
<b>Appendix A: Pinout and Cable Diagram .....</b>	<b>139</b>
Asynchronous Connector Pinout .....	139
Pinout.....	139
Null modem cable .....	140
Introduction .....	140
Diagram .....	140
<b>Appendix B: Hardware Specifications .....</b>	<b>141</b>
<b>Glossary.....</b>	<b>143</b>

---

# Preface

## About this Guide

This guide is intended for network administrators or supervisors who need to know how to install and manage a Black Box Remote Access Server on their network. This guide assumes that the network administrators or supervisors have a solid understanding of their own network environments, including medium type (Ethernet or Token Ring) and protocols (IP, IPX, or AppleTalk). This guide is also for the advanced network user.

In this guide you will read about:

- System Overview

**Chapter 1** describes the Black Box Remote Access Server set of products, features and uses.
- Hardware Installation

**Chapter 2** contains the description of the RAS hardware unit and its installation instructions.
- Manager Installation

**Chapter 3** introduces the Black Box Remote Access Manager program. Instructions on installation and making a connection to a Black Box Remote Access Server are provided.
- Configuration

**Chapters 4, 5 and 6** describe the basic parameters that need to be configured on the Black Box Remote Access Server. These include naming the server, configuring serial port, LAN protocols and users.

**Chapter 12** provides details on Advanced configuration items that can be used to enhance the operation of the Black Box RAS.
- Dial-In and Dial-Out

**Chapters 7 and 8** provide details on enabling the Dial-In and Dial-Out services of the RAS. Information is also provided about third party dial-in clients.
- Network Administration

**Chapter 9** describes features of the Black Box RAS that allow network administrators to monitor the status of the RAS and its users. This includes SNMP statistics, Black Box RAS statistics and a log file of activity on the server.

- Security

**Chapter 10** describes the security features supported by the Black Box RAS and the procedures for configuring these features.

- Front Panel

The front panel of the RAS can be used for limited configuration and viewing of statistics.

**Chapter 11** describes the uses and operation of the front panel.

## About the Document Set

This guide is part of a document set that includes the following publications:

- Black Box Remote User's Guide
- Black Box Dial-Out User's Guide
- Black Box Remote Access Server Guide

---

# Chapter 1: Introduction

This chapter introduces the Black Box Remote Access Server set of products, features and functions.

## Black Box Remote Access Server

The Black Box Remote Access Server is an interface device which allows access to Local Area Networks (LANs) from the telephone network. Users can dial-in to the LAN from a remote site or dial-out from the LAN to access a remote host.

Models are available for both Ethernet and Token-Ring LANs, in 2, 4, or 8 port configurations.

### Supported Protocols

The LAN connections support the following network protocols

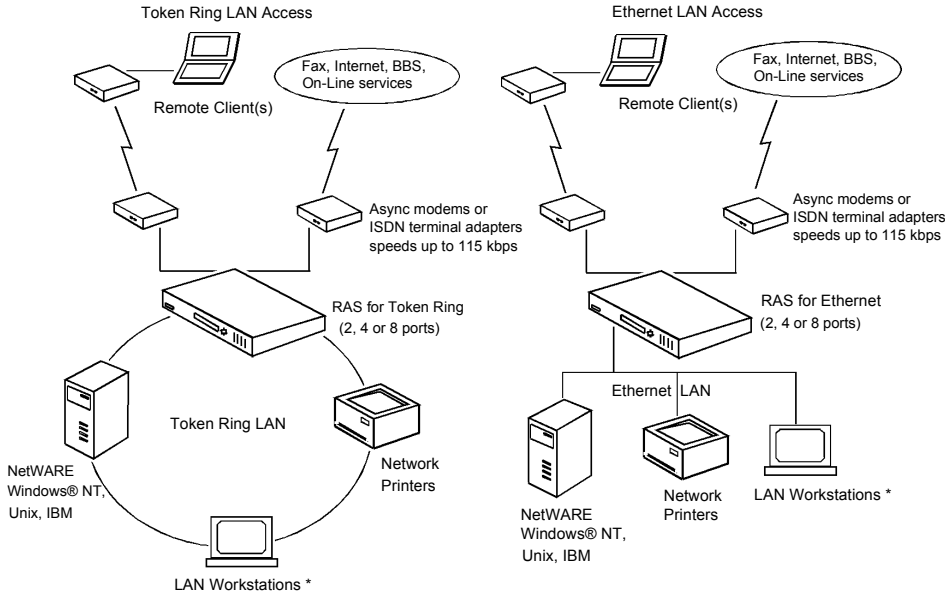
- Novell Internetwork Packet Exchange (IPX)
- Internet Protocol (IP)
- AppleTalk
- NetBios Extended User Interface (NetBEUI)
- Logical Link Control (LLC) and 802.2.

### Dial-In

The Dial-In feature allows remote users, using client software, to access a LAN and perform tasks as if they were directly attached to it, using inexpensive voice-grade telephone circuits and asynchronous modems.

Remote users can connect to the RAS with a modem using a wide variety of PPP clients or the Apple Remote Access Client. Among the PPP clients supported are the RAS Remote (for DOS and Windows 3.x), and the Windows 95 and Windows NT dial-up Networking clients. The RAS Remote software is provided with the Black Box Remote Access Server. See the *Remote User's Guide (for DOS and Windows 3.x)* for more information on the dial-in function. For more information on other client software, see "Chapter 7: Dial-In" on page 81.

## Black Box RAS Network Topology



\* Management software can be run from either a local or remote Windows® PC, Windows® 95 or Windows® NT

## Dial-Out

The Dial-Out function allows users on a LAN workstation to connect to a destination that is external to their LAN. This is done by dialing out via a RAS modem instead of a modem attached directly to the user's PC. The user can connect to a BBS, internet provider or any other service accessible by the telephone network

The benefit of sharing these modems across a network is that they can make efficient use of the hardware and phone lines that are already installed on the network.

The Dial-Out feature is accessed using the Black Box Dial-Out software. See the *Dial-Out User's Guide* for more details on the dial-out function.



## Manager Program

TheRAS Manager software is included with theBlack Box Remote Access Server. It is a Windows based program that allows network administrators to configure, monitor and manage the Black Box servers on the LAN.

## Initial Configuration

In order to configure the unit for the first time, the PC on which the manager is running must establish communication with the target Black Box server. This can be done in one of three ways:

- Over the LAN (Inband)  
By connecting both the PC and the server to the LAN, communications can be established between the two over the LAN using either IP or IPX protocols.
- Direct Connect  
By using the direct connect cable provided with the unit, a PC can establish a serial link to the server via one of the server's serial connectors.
- Dial-in Connection  
By connecting a modem to both the PC and the server, the PC can establish a link.

The following is an overview of the general steps required for each method.

### Over the LAN

1. Server Hardware Setup.  
Follow the hardware installation procedures as outlined in Chapter 2.
2. For IP networks, set the server's IP address.  
If you intend to assign an IP address to your server via BOOTP or RARP, you do not need to do anything here since these are the defaults. Otherwise, you will need to enter an IP address and subnet mask from the front panel under the **Configuration LAN** Menu. See Chapter 11 for information on using the front panel.
3. Install the manager.  
Install the manager on a LAN workstation. Ensure that the workstation is properly configured for IP or IPX. If the manager PC is setup for IP, be sure it has an IP address. See Chapter 3 for

further information.

4. Start up the manager.

The Black Box manager after startup will automatically find the server on the LAN using IP, IPX, or both.

5. Login to the server.

Select the server from the list. Then login as **superusr** with no password.

## Direct Connect

### Windows 3.1

1. Install the Black Box Remote software. Refer to the *Remote User's Guide (for DOS and Windows 3.x)* for details.

2. Configure the Black Box Remote software for direct connect and 38400 baud rate.

3. Install the manager.

Refer to Chapter 3 for further information. Reboot your PC.

**Note:** If the manager PC is to use an IP connection, it must be configured with an IP address.

4. Connect the PC and the server.

Connect the PC to the server using the supplied direct connect cable.

5. Power up the Black Box RAS.

6. Establish the connection.

Using the Black Box Remote Dialer (Windows or DOS), connect to the server. Login as **superusr** with no password.

Once this is completed, startup the manager. After selecting and connecting to the RAS, you will be asked to log in a second time. Use **superusr** again.

## Windows 95

1. Install the Manager on your PC.
2. If your Windows 95 Modem List does not have a direct connect modem type, do the following steps:
  - a) From the modem section on the **Control Panel**, select **Add modem**.
  - b) Choose to select from a list instead of auto detect.
  - c) From the modem selection list, select **Have Disk**.
  - d) Specify the drive and installation directory of the Black Box Manager. (Default is C:\raccess).
  - e) From the model list choose **Direct Connection**.
  - f) Select your COM port.
3. Set up a dial-up networking connection using the direct connection created above. Set the baud rate at 38400.
4. In your dial-up network connection, make sure that you have enabled either IP or IPX.
5. For IP connection, set your TCP/IP settings so that the client (your PC) is supplying its own IP address and enter the address you wish to use.
6. If you are using an IP connection, you will need to set up an IP address and subnet mask in the Black Box server. This can be done through the Front Panel under the **Configuration LAN** menu. See Chapter 11 for information on using the Front Panel.
7. Using the supplied cable, connect the PC to the Black Box server.
8. From Dialup networking, start the Dial-up Session. Login to the RAS as **Superusr** with no password.
9. Start up the manager. After selecting and connecting to the RAS, you will be asked to log on a second time. Use **Superusr** again.

## Dial-In Connection

If neither of the above two methods is possible, you can set up a dial-in connection.

1. Set up the Black Box RAS.

Using the Front Panel, configure the port parameters to best suit the modem you are using. Note that the modem selection at this stage is limited. You will need to use the Hayes selection. Cycle power in the Black Box RAS to ensure parameters take effect.

2. Connect your modem.

3. Set up your client software.

For information on setting up the Black Box Remote, refer to the Remote User's Guide. For Windows 95 or Windows NT, refer to your Windows documentation and Chapter 7 of this guide.

4. Establish the connection, logging on as **Superusr** with no password.

---

## Chapter 2: RAS Hardware Installation

In this chapter you will learn how to install the Black Box Remote Access Server. You will read about:

- Hardware Overview—cabling requirements, modems, telephone lines, etc.
- LEDs
- Front Panel Operation
- Hardware Installation for Ethernet
- Hardware Installation for Token-Ring
- System Defaults

### Hardware Overview

The following items were shipped to you with your Black Box RAS.

- Remote Access Server
- AC Power Cord
- Null Modem Cable
- Manager (CD-ROM)
- Remote (CD-ROM)
- RAS Dial-Out (CD-ROM)
- Documentation Set

You will also require the following items in order to complete the hardware installation.

#### Modems

Analog modems capable of at least 14.4 Kbps are recommended, or other asynchronous terminating device, such as ISDN terminal adapters for each serial port to be used.

#### Cables

**Modem Connection:** Cables required to connect the modems to the RS-232 DB9 connectors on the Black Box RAS.

**Ethernet Connection:** Cables required to attach the Ethernet LAN to either the RJ-45 connector for 10Base-T, the BNC connector for 10Base-2 (Thinnet) or the AUI connector for 10Base-5 thick Ethernet LAN's.

**Token Ring Connection:** Cables required to attach the Token Ring LAN to either the RJ45 connector for UTP connections or DB9 connection for STP connections.

**Telephone System:** Cable will be required to attach the modems or Terminal adapters to the telephone network.

## Black Box Server Models

There are three different RAS models. Each model has an Ethernet and a Token-Ring version.

- LRA502A (-ET or -TR) -R5 has Two remote ports
- LRA504A (-ET or -TR) -R5 has Four remote ports
- LRA508A (-ET or -TR) -R5 has Eight remote ports

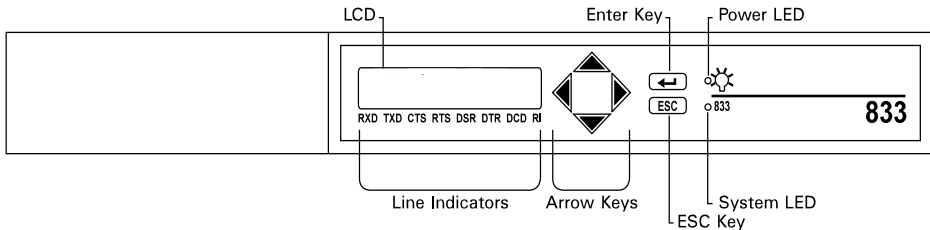
The 'e' or 't' in the module number indicates an Ethernet or Token-Ring unit.

## Front Panel

The Front Panel of the Black Box RAS consists of a keypad and an LCD display. This front panel is common to all models of RAS and can be used for obtaining system status and statistics as well as providing some limited configuration capabilities.

Use the ↵ (Enter) key to select a menu that is displayed on the LCD panel or to confirm a selection. Use the **UP** and **DOWN** arrow keys to view the options within that menu. Press the **ESC** key once to return to the previous menu, and press it several times to return to the RAS main menu. For more information about navigation and editing fields in the front panel display, see "Chapter 11: Front Panel" on page 121.

When the unit is first powered up the LCD display will cycle through the list of languages that it supports. Wait until the appropriate language is displayed and then press ↵.



## LEDs

The RAS front and back panel LEDs are described below.

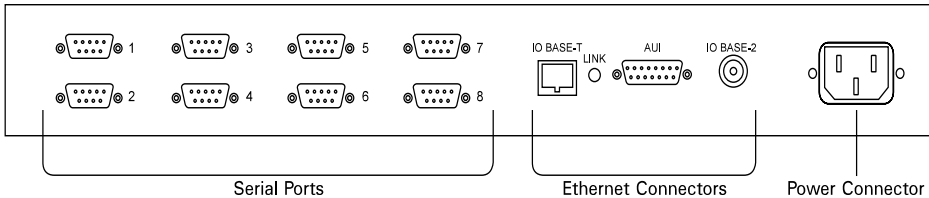
<b>LED</b>	<b>Location</b>	<b>Function</b>
Power (green)	Front	Indicates the RAS is connected to AC power.
System (green)	Front	Blinks continuously when the RAS is operational. Under normal conditions, this happens approximately 30 seconds after the unit is plugged in.
Link (yellow)	Back	Indicates a connection with a LAN.

## Hardware Installation for Ethernet Remote Access Server

The installation of the Ethernet server involves the following steps.

1. Connect the Ethernet cable to the proper Ethernet connector on the back panel of the RAS (8 port model is shown).

### Ethernet Back Panel



**Note:** Back panels for 2e, 4e, and 8e models differ only in the number of serial ports.

2. Plug the power cable into the back of the RAS and into AC power.

**Note:** Always connect the power cable into the back of the RAS before connecting it to the power source, and always disconnect the power cable from the power source before disconnecting it from the back of the RAS.

After a moment, the System (RAS) LED starts blinking and the LCD begins scrolling through the list of available languages for front panel display. When the language you wish to display appears, press  $\downarrow$ . Confirm your selection by pressing  $\downarrow$  again. The LCD then displays the main menu, which displays “RAS/ne” (where n represents the number of serial ports).

3. If you are using 10BASE-T or 10BASE-2 go to step 4. If you are using 10BASE-5 (AUI), use the front panel keypad to change the Ethernet connection type.

To change the Ethernet connection type:

- a) From the main menu, use the  $\downarrow$  key to select the **Configuration** menu.
- b) From the **Configuration** menu, use the  $\downarrow$  key, then the **DOWN** arrow key to access the **Configuration LAN** menu.
- c) From the **Configuration LAN** main menu, use the  $\downarrow$  key to access the **Connection** menu. The LCD displays the current connection type setting. Press the  $\downarrow$  key to modify the setting.



- d) Using the **UP** and **DOWN** arrow keys, select the 10BASE-5 (AUI) option, and press ↵ to confirm your selection.
- e) Reset the system by doing the following:
  - i) Press the **ESC** key until you return to the **Configuration** menu.
  - ii) From the **Configuration** main menu, use the ↵ key, then the **DOWN** arrow key to access the **Configuration System** menu.
  - iii) Select the **System Reset** option, and press ↵ twice to reset the system. The RAS main menu is then displayed.
4. The Link LED should be blinking yellow and the front panel should be displaying the main menu in the selected language.
5. Go to “Setting the IP Address” on page 13.

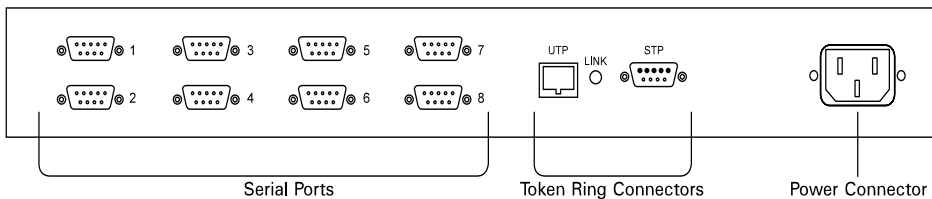
## Hardware Installation for Token-Ring Remote Access Server

The installation of the Token-Ring server involves the following steps.

1. Plug the power cable into the power connector on the back panel of the RAS (8 port model is shown).

**Note:** □ Always connect the power cable into the back of the RAS before connecting it to the power source, and always disconnect the power cable from the power source before disconnecting it from the back of the RAS.

### Token-Ring Back panel



**Note:** Back panels for 2t, 4t, and 8t models differ only in the number of serial ports.

After a moment, the System (RAS) LED starts blinking and the LCD begins scrolling through the list of available languages for front panel display. When the language you wish to display appears, press  $\downarrow$ . Confirm your selection by pressing  $\downarrow$  again. The LCD then displays the main menu, which displays “RAS/nt” (where n is the number of serial ports).

2. Use the front panel to set the Token-Ring speed to match the speed of your Token-Ring LAN.
  - a) From the main menu, use the  $\downarrow$  key to select the **Configuration** menu.
  - b) From the **Configuration** menu, use the  $\downarrow$  key, then the **DOWN** arrow key to access the **Configuration LAN** menu.
  - c) From the **Configuration LAN** menu, use the  $\downarrow$  key to access the **Connection** menu. The LCD displays the current connection speed setting. Press the  $\downarrow$  key to modify the setting.
  - d) Use the **UP** and **DOWN** arrow keys to until the appropriate speed is displayed, then press the  $\downarrow$  key to select the connection speed.
  - e) Reset the system by doing the following:
    - i) Press **ESC** until you return to the **Configuration** menu.

- ii) From the **Configuration** menu, use the  $\downarrow$  key, then the **DOWN** arrow key to access the **Configuration System** menu.
  - iii) Select the **System Reset** option, and press  $\downarrow$  twice to reset the system. The RAS main menu is then displayed.
3. The Link LED on the back panel should be blinking yellow and the front panel should be displaying the main menu in the selected language.
4. Connect the Token-Ring cable to the proper Token-Ring connector on the back panel of the RAS.
5. Proceed with "Setting the IP Address".

## Setting the IP Address

The RAS will need to have an IP address if it will be operating in an IP network. If you are not operating in an IP network or if the network supports a BOOTP or RARP server to supply an IP address to the RAS, skip the next step.

1. From the main menu, use the  $\downarrow$  key to select the **Configuration** menu.
2. From the **Configuration** menu, use the  $\downarrow$  key, then the **DOWN** arrow key to access the **Configuration LAN** menu.
3. From the **Configuration LAN** main menu, use the  $\downarrow$  key, then the **DOWN** arrow key to access the **IP Address** menu.
4. Press the  $\downarrow$  key to start editing the IP Address of the RAS. Use the Left and Right arrow keys to position the cursor. Then use the Up or Down arrow keys to change the value of a digit.
5. Reset the system by doing the following:
  - a) Press **ESC** until you return to the **Configuration** menu.
  - b) From the **Configuration** menu, use the  $\downarrow$  key, then the **DOWN** arrow key to access the **Configuration System** menu.
  - c) Select the **System Reset** option, and press  $\downarrow$  twice to reset the system. The RAS main menu is then displayed.

## Modem Installation

Install each modem that is required as follows:

1. Connect the modem cable from the serial port of the modem to the proper serial port of the server.
2. Follow the modem's installation instructions to power up the modem and connect it to the telephone network.

## System Defaults

The RAS defaults are listed below. The default settings can be changed from the front panel or the Manager program.

### System

Front Panel Lock—no password

Language—not set

### Ports

All ports enabled

Modem type - Direct

38,400 baud rate

Broadcast enabled

Multicast enabled

Dial-in enabled

Head and Address compression enabled

### LAN

Connection - BNC/10Base-T auto-sensing (Ethernet Unit)

- LAN speed - 16 Mbs (Token-Ring unit)

IP address - none

No Subnet Mask

RARP enabled

BOOTP enabled

---

## Chapter 3: Manager Software Installation and Setup

This chapter describes the RAS Manager program, its installation procedure, and method of connecting to the RAS. In this chapter you will read about:

- Manager Overview
- System Requirements
- Installing Manager Software
- Connecting to the Server via In-band and Serial links
- Manager Main Screen

### Manager Overview

The RAS Manager software is a Microsoft Windows application used to configure, monitor and manage Black Box servers. The RAS Manager can do the following:

- Create configuration files to be downloaded to RAS hardware units—different configurations can be made, saved, and downloaded.
- Upload a RAS's configuration so it can be saved, modified, used in other RASs, or compared to other configurations.
- Display statistics for a RAS.
- Display event logs for a RAS.
- Download new firmware to a RAS.

### Connection

The Manager requires a connection to be established with a Black Box remote access server. This can be accomplished in any of the following ways:

- **In-band Connection:** Connect a PC to the same network that the Black Box server is connected to, and then use the Manager software to establish an in-band connection using IP or IPX. This will depend on the network software running on the Manager PC.
- **Direct Connection:** Use the null modem cable provided with the RAS unit to connect the PC directly to a RAS serial port, and then use Dial-in client software to establish the connection.

- **Modem Serial Connection:** Use modems and Dial-in client software to connect the Manager PC to the RAS over the telephone network.

### Client Software

The Manager software will run over the following clients when using a serial connection:

- Remote (for Dos and Windows 3.x)  
(See the *Remote User's Guide* for details on installation and setup).
- Windows 95 Dial-Up Networking Client
- Windows NT 3.5 or 4.0 Dial-Up Client

### System Requirements

The minimum requirements to use the RAS Manager software are:

- PC-compatible 80386 or faster computer with the following:
  - Hard drive with at least 2 MB free storage space
  - Microsoft Windows 3.1 or higher with MS-DOS version 5.0 or higher  
*or*  
Windows 95  
*or*  
Windows NT 4.0
  - 4 MB RAM
  - Windows-compatible mouse

#### For an in-band connection - IP

- A working IP connection to the LAN. For Windows 3.1 users, a TCP/IP stack is provided on the Manager disks.

#### For an in-band connection - IPX

- A working IPX connection to the LAN.

#### For a Direct connection

- An unused serial (COM) port on the Manager PC. A buffered serial port (for example, one that uses 16550 UARTs) is strongly recommended. Serial ports on older devices are usually not

buffered.

- Dial-In Client software.
- Null modem cable that was supplied with the Black Box Server. This is connected between the serial port of the PC running the manager and a serial port on the RAS. For more information on the Null modem cable see “Appendix B: Hardware Specifications” on page 141.

### **For a modem serial connection**

- An unused serial (COM) port on the Manager PC. A buffered serial port (for example, one that uses 16550 UARTs) is strongly recommended. Serial ports on older devices are usually not buffered.
- Dial-In Client software.
- A modem cable for connection between the PC serial port and a modem.
- Analog modems capable of at least 14.4 Kbps are recommended, or other asynchronous terminating devices, such as ISDN terminal adapters.
- Voice grade telephone lines or high speed service like ISDN.

## **Installing Manager Software**

To install the Black Box Manager software, follow these steps.

1. Start Microsoft Windows.
2. Place the Black Box Manager CD-ROM in the CD-ROM drive.
3. **Windows 3.1**  
In Program Manager, choose **Run** from the **File** menu, type the CD-ROM drive letter (i.e., **D:\setup**) and press **Enter**.  
  
**Windows 95**  
Click the **Start** button , click **Run**, type the CD-ROM drive letter (i.e. ,**D:\setup** ) and press **Enter**.
4. Perform the installation by following the prompts that appear on the screen.

## Connecting to the Remote Access Server

### In-band Connection

#### IP

The RAS needs an IP address before the Manager can make a connection. This address can be acquired in the following ways:

- The Black Box server will try to acquire an IP address from a BOOTP server or an RARP server on the LAN.
- If the above step fails, then the configured IP address is used. By default, the RAS does **not** have a configured IP address.
- If an IP address has not been set in the RAS, then this must be done. An IP address can be set by using the Front Panel. See “Chapter 11: Front Panel” for instructions.

#### IPX

Nothing needs to be set up on the server to establish an IPX connection.

### Direct Connection

#### Windows 3.1

1. Install the Black Box Remote software. Refer to the *Remote User's Guide (for DOS and Windows 3.x)* for details.
2. Configure the Black Box Remote software for direct connect and 38400 baud rate.
3. Connect the PC and the server.  
Connect the PC to the server using the supplied direct connect cable.
4. Power up the Black Box RAS.
5. Establish the connection.

Using the Dialer (Windows or DOS), connect to the server. Login as **superusr** with no password.

Once this is completed, start up the manager. After selecting and connecting to the RAS, you will be asked to log in a second time. Use **superusr** again.



6. When the connection is established, start Black Box Manager.

## Windows 95

1. Install the Manager on your PC.
2. If your Windows 95 Modem List does not have a direct connect modem type, do the following steps:
  - a) From the modem section on the Control Panel, select **Add modem**.
  - b) Choose to select from a list instead of auto detect.
  - c) From the modem selection list, select **Have Disk**.
  - d) Specify the drive and installation directory of the Black Box Manager. (Default is C:\raccess).
  - e) From the model list, choose **Direct Connection**.
  - f) Select your COM port.
3. Set up a dial-up networking connection using the direct connection created above. Set the baud rate at 38400.
4. In your dial-up network connection, make sure that you have enabled either IP or IPX.
5. For IP connection, set your TCP/IP settings so that the client (your PC) is supplying its own IP address and enter the address you wish to use.
6. If you are using an IP connection, you will need to set up an IP address and subnet mask in the Black Box server. This can be done through the Front Panel under the **Configuration LAN** menu. See chapter 11 for information on using the Front Panel.
7. Using the supplied cable, connect the PC to the Black Box server.
8. From Dialup networking, start the Dial-up Session. Login to the RAS as **superusr** with no password.
9. Start up the manager. After selecting and connecting to the RAS, you will be asked to log on a second time. Use **superusr** again.

## Dial-In Connection

If neither of the above two methods is possible, you can set up a dial-in connection.

1. Set up the RAS.

Using the Front Panel, configure the port parameters to best suit the modem you are using. Note that the modem selection at this stage is limited. You will need to use the Hayes selection. Cycle power in the RAS to ensure parameters take effect.

2. Connect your modem.
3. Set up your client software.

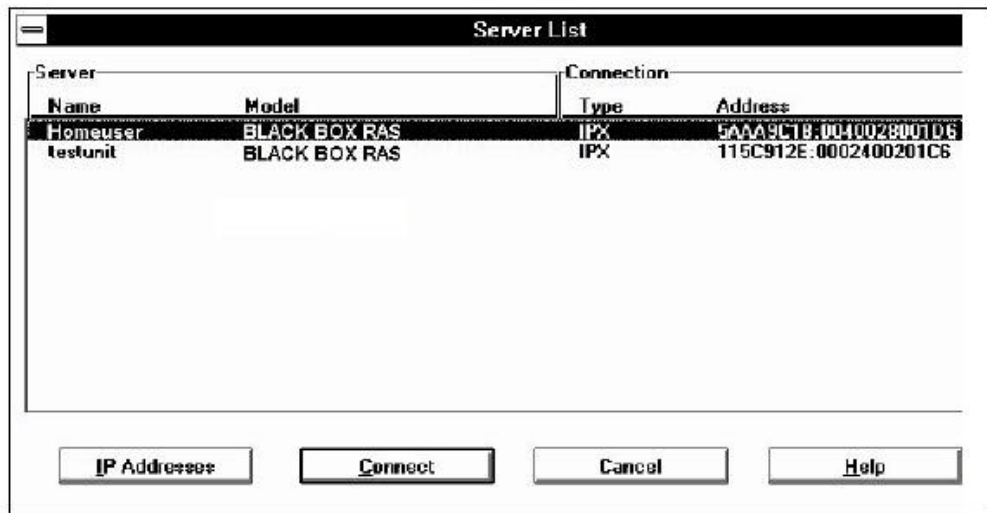
For information on setting up the Black Box Remote, refer to the Remote User's Guide. For Windows 95 or Windows NT, refer to your Windows documentation and Chapter 7 of this guide.

4. Establish the connection, logging on as superusr with no password.

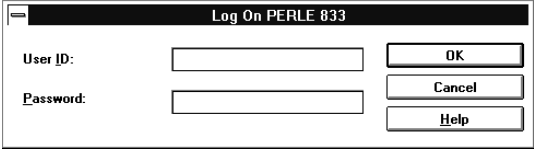
## Server List

Once the Black Box Manager is running, it automatically locates all Black Box servers and displays them in the Server List window. This is accomplished by sending out a broadcast message using the following connection types or protocols: IP , and IPX.  
To complete the connection to a server:

1. Highlight the server that you want to connect to and click Connect.



- The **Log On** dialog box will appear.



The image shows a dialog box titled "Log On PERLE 833". It contains two text input fields: "User ID:" and "Password:". To the right of the "User ID" field is an "OK" button. To the right of the "Password" field are "Cancel" and "Help" buttons.

- Enter the **User ID** and **Password** for the selected server and click **OK**.

**Note:** The default name for an unconfigured Black Box server is: **superusr** - no password. You will be required to set a password when you first configure the server.

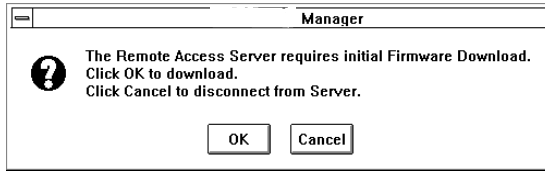
- If the **User ID** and **Password** are verified, then the Manager main screen is displayed.

**Note:** If the server you are connecting to is a new unit, you will be required to download firmware to it before you can begin configuring.

- A user can elect not to connect to a server by clicking on **Cancel** in the **Server List** window. The Manager main screen is displayed without the **Get Configuration** and **Statistics** buttons.
- If your network contains IP routers that do not route broadcast messages, then click the IP Addresses button to configure IP Addresses for Direct Polling. See "Addresses for Direct Polling" on page 53 for instructions.

## Update Firmware

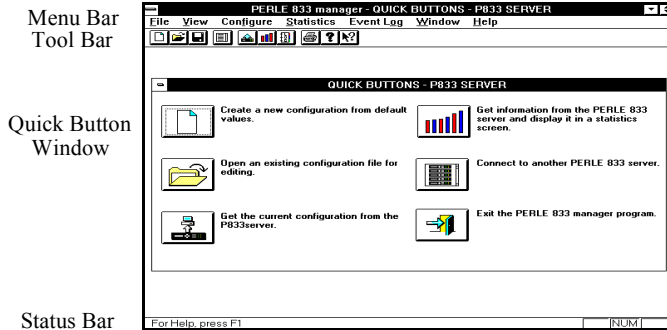
A new RAS from the factory will have a base version of the operating code (firmware). This firmware version can not be configured by the Manager and must be updated to a working version. The base version is automatically detected when the Manager makes a connection to a new RAS and **superusr** is used to log on. This process can take up to two minutes at 38400 baud. The following dialog box appears:



1. Click **OK** to start the download process.
2. After the firmware has been downloaded, the RAS will reset itself. Wait five minutes before trying to connect to the server again for configuration.
3. If the **Cancel** button is clicked, the Manager will disconnect from the RAS and display the Server list again.

## Manager Main Screen

The Black Box Manager main screen contains menus and the following tools and windows.



Menu Bar  
Tool Bar

Quick Button  
Window

Status Bar

### Menu bar

Contains menus that control the Manager and configure RASs. The Menu bar contains the following menus—**File**; **View**; **Configure**; **Statistics**; **Event Log**; **Window**; and **Help**.

### Tool bar

Makes it easier to perform some of the most-used menu functions.

### Quick Buttons window

A quick way to use the main functions of Black Box Manager. Each function is represented by a button. The **Get Configuration** and **Statistics** buttons are not available when a RAS is not connected.

### Status bar

Gives information about menus and menu items when they are selected, and about the status of some keys on the keyboard.

## Menu bar

The menu bar contains all of the menus available when running the Manager. Each menu contains a list of options that drop down from the Menu title. Some of the menu items are only active when a configuration file is open.

## File Menu

The following options appear under the **File** menu:

### **New**

Create a new configuration.

### **Open**

Open an existing configuration.

### **Close**

Close the selected configuration file.

### **Server List**

Show all Remote Access Servers found.

### **Quick Buttons**

Display the **Quick Buttons** window.

### **Save**

Save the currently-selected configuration file.

### **Save As**

Save the currently-selected configuration file as a new file.

### **Print**

Print the currently-selected configuration file.

### **Print Preview**

Show a preview of the currently-selected configuration file.

### **Print Setup**

Select a different printer or change the printer setup.

### **Numbered file names**

The most recent files that were opened are listed here. As a convenience, choose one to open that file.

### **Exit**

Quit RAS Manager. If unsaved changes have been made to any files, you will be prompted to save or cancel the changes.

## **View Menu**

The following options appear under the **View** menu:

### **Tool Bar**

This option toggles the tool bar (just below the menu bar) off and on. When the tool bar is displayed, there is a check mark next to this option.

### **Status Bar**

This option toggles the status bar (at the bottom of the screen) off and on. When the status bar is displayed, there is a check mark next to this option.

## **Configure Menu**

The **Configure** menu applies to the RAS to which the Manager is connected, and not to any configuration file. If a RAS is not connected, the options on this menu are not available. The following options appear under the **Configure** menu:

### **Get Configuration**

Upload the configuration from the connected server and display it in the **Configuration File** window.

### **Download Configuration**

Download a configuration file (or parts of it) to the RAS.

### **Reset the RAS**

Reset the RAS or selected serial ports. All user connections will be lost.

### **Set Date and Time**

Set the system date and time on the RAS.

### **Lock Front Panel**

Enabled only when connected to a server. Toggles between on and off and takes effect immediately.

### **Download Firmware**

Download a new version of operating code (firmware) to the RAS.

### **Set to Factory Defaults**

Set all parameters in the RAS to factory default values. All existing configuration parameters will be lost.

## **Statistics**

Only one option is available on the **Statistics** menu:

### **Get Statistics**

Display the **System Statistics** window. It gives information about the RAS to which the Manager is connected.

## **Event Log**

The following options appear under the **Event Log** menu:

### **Get Event Log**

View information on all activity on the server for the current session.



### **Clear Event Log**

Clear all session information from the log.

### **Change Log Filter**

Filters are available for:

- User account usage and security (log on activity, log out activity and failed log on activity)
- Configuration changes (through the manager and front panel)
- System Restarts; Errors (internal Black Box server errors)
- PPP details (changes and status information of each PPP session)
- IP details (changes and status information of each IP session).

### **Window Menu**

The following standard operations appear under the **Window** menu:

#### **Cascade**

Resize and overlap all open windows so that their title bars are visible.

#### **Tile**

Resize and arrange all windows across the work space with no overlap.

#### **Arrange Icons**

Applies only when at least one configuration window has been minimized, making it into an icon. Choose this option to arrange all icons neatly, starting in the lower left corner.

#### **Numbered file names**

The name of each open configuration file is listed at the bottom of the **Window** menu with a number to its left. The **Quick Buttons** window is also listed if it's open. Choose one item to make it current.

## Help Menu

The following options appear under the **Help** menu:

### Index

Brings up the Black Box Manager Help index.

### Using Help

Gives general information about using Windows Help.

### About Black Box RAS Manager

Display the version number of the Black Box Manager program and a copyright notice.

## Tool bar

The tool bar, located under the menu bar near the top of the screen, makes it easy to perform some often-used functions. Each function can be performed from a menu, however, using the tool bar is much faster.



### New file

Start a new configuration file with default values.



### Open file

Open an existing configuration file.



### Save file

Save the currently selected configuration file.



### Server List

Display the list of Black Box remote access servers. Select a server to make a connection.



### **Get Configuration**

Get the current configuration from the connected RAS.



### **Get Statistics**

Get the **Statistics** data from the RAS and display it in the **System Statistics** window.



### **Get Event Log**

Get the event log from the RAS.



### **Print**

Print the current configuration information.



### **About**

Display the version number of Black Box RAS Manager and a copyright notice.



### **Directed Help**

to get help information on the item.



---

## Chapter 4: Server Configurations

This chapter describes how to set up a RAS. In this chapter you will read about:

- Configuration Overview
- Opening Configuration File
- Server Options
- Port Options
- User List Options
- Downloading a Configuration

### Configuration Overview

The following steps describe the basic procedure to configure RAS. The topics are then discussed in more details in later sections.

1. Open a Configuration File.

This includes uploading a configuration from an attached RAS, opening an existing configuration file on the Manager PC, or creating a new configuration file.

2. Edit the RAS general parameters.

This includes options such as defining modem pools and giving the server a name.

3. Configure the Network Protocols.

Parameters for the protocols, IP and IPX, running on your network may need to be configured. These parameters include IP addresses, MAC addresses, or IPX frame types.

4. Configure Security features.

Access to the network is controlled by the RAS security features. A security method needs to be selected and configured.

5. Edit the RAS ports.

Configuring the ports usually involves setting the modem type, baud rate, and access.

6. Add / Edit user records.

Users are the people who will dial into the LAN through a RAS. Some of the things that can be configured for each user are: name and department, password, call back options, filters and connect time duration.

7. Save the file.

**Note:** Steps 1 through 7 (except for uploading a configuration) can be done without having a Black Box RAS connected to the PC.

8. Download the Configuration

This will copy the configuration file to the Black Box RAS and set it in the server's memory.

## Open Configuration File

The configuration file contains a detailed set of configuration data for the RAS including the server's name, network protocol parameters, serial port parameters and user records. Once a file has been created, it can be used to set the configuration for one server or it can be saved and used as a base for any number of servers. A configuration file can be opened for editing by following one of the following procedures:

### Create a New Configuration File

1. From the Manager **File** menu, select **New**.
2. The **New Configuration** dialog box appears. Select the appropriate Black Box server type. Click **OK**.
3. The **Configuration File** window will appear with the default settings for the selected server type.

### Open an Existing Configuration File

1. From the Manager **File** menu, select **Open**.
2. Select the required configuration file from the file list and click **OK**.
3. The **Configuration File** window appears with the setting of the selected configuration file.

### Get a Black Box RAS Current Configuration File

1. From the Manager File menu, select Device List.
2. The Server List window appears. Select the RAS from which you want to get the configuration file and click Connect.
3. The Log On dialog box appears. Enter a User ID and password. Click OK.  
The User ID needs administrative privileges to make a connection with the Manager.  
Note : The default administrative name for an unconfigured RAS is:  
superusr (with no password)
4. If the User ID and Password are verified, then the Manager Main screen with the Quick Button window is displayed. Click the Get the current configuration from the server button. The configuration file will be transferred from the selected server to the Manager PC.
5. The Configuration File window appears with the settings of the selected Black Box RAS.

### Configuration File Window

The Configuration File window is divided into sections which are described below.

**Server**

Server Name	LAN Connection	IP Address	MAC Address	Edit...
RAS	Auto (BNC)			

**Port**

Port:	Baud Rate:	Modem Model:	Get...
1: Enabled	38400	Direct	
2: Enabled	38400	Direct	

**User**

User ID:	Department:	Access:	Call Back:	Modem Pool:	
SuperUsr		Admin	Allowed		Add
					Copy
					Edit
					Delete
					Shared Lists

User List Access:  Public  Private

1 Users: Save Close Help

### Server section

Use this section to configure the server itself, including such things as a server name, front panel, filters, password, connection type, modem pools, IP, IPX and MAC addresses.

### Port Section

Configure the serial ports of the RAS. This includes modem type, baud rate, dial-out parameters and many other options.

### User List Section

Use this section to Add or Edit User records in the User List. This includes user names, passwords, filters, call back features, activity time-outs and privileges. Specify how the User List can be used or found.

### Server Options

Follow these steps to configure the server parameters.

1. Open the required configuration file.
2. From the Server section of the Configuration File window, click Edit. The Edit Server Options dialog box appears.

**Edit Server Options**

Server Name:

**LAN Port Configuration**

Connection:  ▾

**Protocols**

IP       Netbios       BCP  
 IPX       ABA       Bridging

Enable front panel password       Enable Stack Compression

**Set Front Panel Password**

Password:

Confirm:

Front Panel Language:  ▾

OK  
Cancel  
Modem Pool...  
MAC Address...  
IP...  
IPX ...  
SNMP...  
Dial Out...  
Security...  
Filter  
Help



3. Give the server a name by typing it in the **Server Name** field.

The server name is used to identify the remote access server on the network. It is used by router information protocols (RIP) and service advertising protocols (SAP). Make sure to use a name that properly identifies the server you are naming.

4. From the **LAN Port Configuration** drop-down list, select a connection. The options depend on the Black Box RAS model:

**Ethernet:**

Select the type of connector that will be used to connect the RAS to the network. The choices are:

- |                    |  |
|--------------------|--|
| Auto (BNC)         | This is the default. This will automatically detect whether the BNC or 10Base-T (RJ-45) connector is being used. |
| Auto (AUI)         | This choice will automatically detect whether the AUI or 10Base-T (RJ-45) connector is being used.               |
| 10Base-2 (BNC)     | The BNC connector will be used.  |
| 10Base-T           | The 10Base-T (RJ-45) connector will be used.   |
| 10Base-T (no test) | The 10Base-T (RJ-45) connector will be used. The server will not test to see if a connection has been made.      |
| AUI                | The AUI connector will be used.  |

**Token-Ring:**

Select the correct token-ring speed for the network. The choices are 16 Mbps (default) or 4 Mbps.

5. Enable all protocols that the server needs to process. A protocol is enabled by clicking on its checkbox. By default, only the IP and IPX protocols are enabled. The **Bridging** protocol is a proprietary protocol used by the Black Box Dial-In Client (version 4.8 or earlier).

Please note the following:

- If the **IP** or **IPX** protocol is disabled, then any other configuration item that uses this protocol will not be assessable.
- If a security feature that uses the **IP** or **IPX** protocol has already been configured, you will not be allowed to disable the protocol.

6. If you want a password enabled for the front panel, click on the **Enable Front Panel Password** check box and type a password of up to 8 digits long, using the digits 0-9 (no alpha characters allowed).
7. If you wish to enable Stac (software) compression, click on the **Enable Stac Compression** check box. Note that this compression is only useful in an environment where most calls are digital. On analog calls this compression technique will actually create additional overhead since the modems are already providing hardware compression of the data. The default is no Stac compression.
8. The front panel language may be changed, if desired, by selecting another language from the **Front Panel Language** drop-down list.
9. Configure the network protocol parameters that are required for your network and for the dial-in clients being used for remote access. These parameters are accessed by clicking on the **MAC Address...**, **IP...**, or **IPX...** buttons. See “Chapter 5: Configuring Network Protocols” on page 47 for a full description of the network parameters and how to configure them.
10. To configure **Modem Pools** or **Dial-Out**, see “Chapter 8: Dial-Out” on page 85.
11. To configure **SNMP**, see “Chapter 9: Network Administration” on page 93.
12. To assign **Filters**, see “Server Filter Assignment” below for more details.
13. To configure **Security**, see “Chapter 10: Security” on page 103. You should select the highest level of security supported by your network.
14. Click **OK** to save your changes or **Cancel** to exit without saving.

## Server Filter Assignment

Use this window to assign up to 10 IP and 10 IPX filters to the server. The server will process these filters from the top down, so the order may be important. See “Packet Filtering” for more details on how the filters are used.

To assign IP and/or IPX filters for the server, follow these steps:

1. Select a filter name from the Defined Filters pull-down list and click **Add** to add the filter to the Assigned Filters list.
  - You can change the order of the assigned filters by selecting a filter name from the Assigned Filters list and clicking the Move Up or Move Down buttons.

- You can delete a filter assignment by selecting a filter name from the Assigned Filters list and clicking the **Remove** button.
2. Set the **Default Action** to be taken if a packet does not match any assigned filter. The choices are to **Accept** or **Reject**.
  3. If you need to define more filters, then click the **Define** button in either the IP or the IPX section. The **IP Filter Definition** or **IPX Filter Definition** dialog box appears.
  4. Click **OK** to save your changes.

## Setting the date and time

Setting the date and time on a RAS is done separately from setting up the configuration file. The RAS must be connected to the PC running Black Box Manager. To set the date and time, follow these steps:

1. From the **Configure** menu, select **Set Date and Time**.
2. In the dialog box that appears, set the appropriate date and time, and click **OK**.

The date and time are immediately changed in the attached RAS.

## Serial Port Options

To configure the serial ports, follow these steps.

1. Select the port or ports you want to configure and click the **Edit** button.

**Note:** You can configure more than one port at a time by pressing Ctrl and clicking on more than one port. Fields that are the same among the ports are displayed; fields that are different among the selected ports are grayed out.

- The **Edit Port** dialog box appears.

The screenshot shows the 'Edit Port 1' dialog box. It features a title bar with a minus sign and the text 'Edit Port 1'. The main area contains the following elements:

- Port Disabled**
- Port Name:** 1
- Modem Model:** Direct
- Baud Rate:** 38400
- Filtering:**
  - Broadcast:** Filter
  - Multicast:** Filter
  - User Override Disabled**
- Port Access:**
  - Dial In**
  - Dial Out**
- IP Address:** (empty text field)

At the bottom of the dialog are four buttons: **Custom Modem...**, **Link Control Protocol...**, **Async Control Map...**, and **Dial Out Parameters...**. On the right side, there are three buttons: **OK**, **Cancel**, and **Help**.

- To disable the port, click on the **Port Disabled** check box.
- You should give the port a meaningful name. The name will be used in the Black Box Dial-Out software to identify ports that are available for dial-out. If the port name is left blank, the manager software automatically assigns a numeric name to this field.
- From the **Modem Model** drop-down list, select the make and name of your modem. If you can't find your modem in the list, select the one that most closely resembles your modem.
- Set the port baud rate from the drop-down list. This rate will be the fixed rate for Dial-In. This means that Dial-In callers will *always* run at this speed.  
**Note:** Since modems negotiate to a mutually agreed speed, callers with slower modems will be able to connect. The parameters should be set to the highest speed at which the attached modem can run on its serial port.
- Enter a **Dial Prefix** string if required. This number will be added to the beginning of a phone number in the following conditions:
  - If the port is used for call back.
  - If the port is used for Dial Out. The port must belong to a **Modem pool** that is configured for Dial-Out and configured with an auto-dial phone number. If the dial out client application is dialing the number, then the prefix will not be used. The field would be used if a port was connected to a PBX line. The prefix can be up to 4 characters in length.

8. Optionally, enter an **IP address** for this port. The network portion of the address must be the same as network portion of the server's IP address. The IP address will be assigned to the client who dials into this port.
  9. The **Filtering** option can be used to either enable or disable the RAS's ability to filter out Broadcast and Multicast frames (both types or just one) from being sent over the dial-in link to the Black Box Remote. The settings of these filters depend on the protocol used. For example, for IPX, you would normally set **Broadcast** and **Multicast** to **Filter**. However, the NetBEUI protocol or LLC protocol needs to have the **Multicast** set to **Pass**. As well some software applications may require these message frames. See your network administrator for the correct settings. To configure the filter feature:
    - a) Select **Pass** from the drop down lists if required for the **Broadcast** and **Multicast** fields.
    - b) The Remote has the option to override the options set here in the RAS. If the **User Override Disabled** field is checked, then the Remote will not be able to use its override function.
  10. Set any other necessary parameters. These include:
    - **Dial-In/Dial-Out** port access. A check means enabled. If neither is checked, then the port can only be used for call back.
    - **Link Control Protocol** parameters (see "Chapter 12: Custom Server Configuration" on page 133).

*Note:* Most users will not need to change these parameters because this is an advanced feature that affects very few users.
    - **Async Control Character Map** (see "Chapter 12: Custom Server Configuration" on page 133).

*Note:* Most users will not need to change this parameter because this is an advanced feature that affects very few users.
    - **Dial-Out** parameters (see "Chapter 8: Dial-Out" on page 85).
  11. Click **OK**.
- Follow these same steps for any other ports that need to be configured.

## User List Options

### User Records

To add or edit the user records, see “Configuring a User Record” on page 71.

### User List Access.

The RAS can be configured to share its list of User records with other RAS servers on the LAN. This feature allows the administrator to store all user records in up to two servers instead of storing a copy of the User List on every server on the LAN. To configure:

Select the access privilege for the User List configured on the RAS. The options are:

#### Public

The User List will be accessible to any remote RAS on the LAN which has been configured for Search Remote.

#### Private

The User List will be accessible only to users that connect to the local RAS. However, the local RAS can access the User Lists on other RAS servers on the LAN if the local server is configured for **Search Remote**

### Shared User Lists.

Click the **Shared Lists** button to configure the RAS to access the User Lists on other servers. See “Shared User Lists” on page 74 for configuration instructions.

## Save Configuration File

The configuration file should be stored on the Manager PC’s local drive for backup purposes. To save the configuration file, follow one of the procedures below:

### Save a New Configuration File

1. From the Manager **File** menu, select **Save As**.
2. Enter a file name for the new configuration and click **OK**.
3. The Manager will save the configuration in a new file with the specified name.

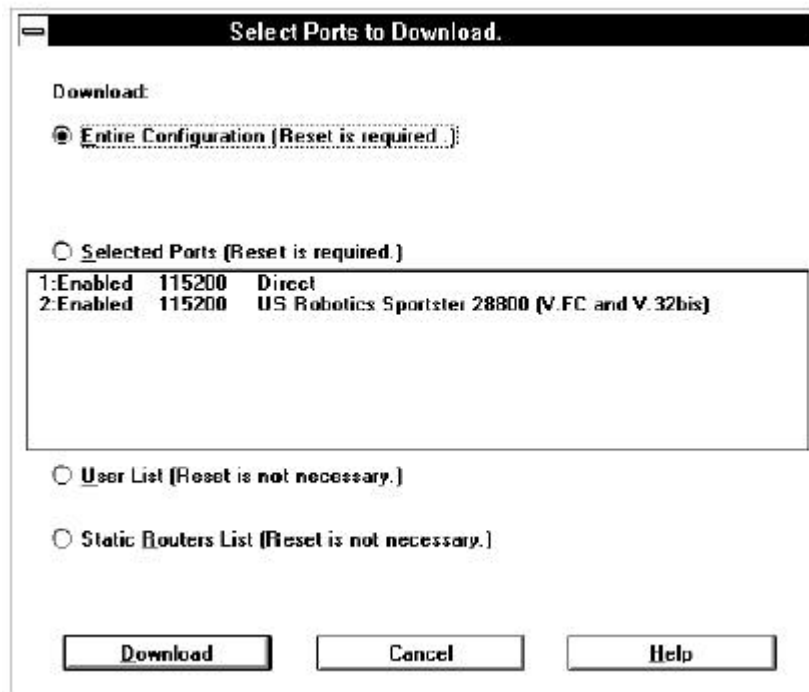
### Save an Existing Configuration File

1. From the Manager File menu, select Save.
2. The Manager will save the changes to the configuration in the existing file.

### Download the Configuration

The configuration file needs to be downloaded to a RAS for the parameters to take effect. The entire configuration can be downloaded or just certain sections such as user records or port configuration. If only sections of the configuration are downloaded, the RAS does not have to be reset. The following steps describe how to download a configuration:

1. Make sure that the Manager PC is connected to the RAS and that the appropriate configuration file has been opened.
2. From the Configure menu, select Download Configuration.
3. The Download Configuration dialog box appears. Click the radio button beside one of the following options:



### Entire Configuration

The entire configuration file is downloaded and the RAS must be reset before the configuration changes take effect.

### Selected Ports

Select one of the listed ports. Only the configuration for this port will be downloaded. The port must be reset before the changes take effect.

### User List

There is no reset required for this option. The changes will take effect the next time a new or modified user tries to make a connection.

### Static Router List

This will replace the existing list in the RAS and will take effect immediately.

4. Click on the **Download** button. The Manager will download the selected portions of the configuration file. If the download selection requires a reset of the server or serial port, the Manager will ask for a confirmation of the reset.

**Note:**  Any existing user sessions will be terminated when the RAS is reset or a port is reset

## Protocol Enable/Disable

The IP, IPX, Netbios, ARA, BCP and bridging protocols can be turned off and on. At the Server Level, the unit will prevent any connections with the disabled protocols and also will not use it for its own purposes (i.e. security access). This feature will also be available at the User Level.

## Event Log

The Event logging function has been improved to provide consistent and pertinent information. The new or improved messages are:

**Dial-in begin, Dial-in end**

**Call-back event ( including the call back number )**

**Dial-out begin, Dial-out end**

The Dial-out number will be logged where it is known. If the number is provided by the application (i.e. DUN), it will not be logged. The workstation address from where the dial-out initiated will be logged.



## Dialing prefix/port

This feature is useful in a callback environment. The user will be able to configure a dialing prefix on a port basis. The prefix will be added to the beginning of the phone number for dialing. This is useful if you have some modems on PBX lines, and some that are not. This feature can also be used for dial-out purposes but will only function when the 833 is dialing the number. If the application ( ex. DUN ) is dialing the number, the prefix will not be applied.

## Packet Filtering

The Packet Filtering feature allows the Black Box Server to accept or reject incoming data packets that match an entry on a list of defined filters. The filters are based on protocol, and packet addresses.

Up to 50 IP and 50 IPX filters can be defined with the following parameters:

- IP filters can specify Address, Mask, Sub-protocol, and port.
- IPX filters can specify Network, Node, Socket and Sub-protocol

After the filters have been defined, then up to 10 IP and 10 IPX filters can be assigned to the RAS or to each user or to both.

Filters will be used by the Black Box Server in the following way:

1. The user record for the dial-in user will be checked. If the record has been configured to Disable Server Filters, then only the user assigned filters will be checked. Proceed to point 4.
2. Incoming data packets are compared with the filters assigned to the server starting with the first filter in the Server Filter Assignment list. As soon as the packet matches one of the filters, then the packet is accepted or rejected and no further checking is done.
3. If the packet does not match any of the filters assigned to the server, then the user record will be checked. If there are no user assigned filters, then the server default action will be carried out to accept or reject the packet and no further checks are done.
4. The incoming data packet will be compared to the filters assigned to the user, starting with the first filter in the User Filter Assignment list. As soon as the packet matches one of the filters, then the packet will be accepted or rejected.
5. If the packet does not match any user assigned filters, then the user default action will be carried out to accept or reject the packet.

To configure IP Filters:

1. From the server section of the configuration file window, click the **Edit** button. The **Edit Server Options** dialog box that appears.
2. Click the **IP** button. The **Edit IP Profile** dialog box appears.
3. Click the **Define Filters** button. The **IP Filter Definition** dialog box appears.

To configure IPX Filters:

1. From the server section of the configuration file window, click the **Edit** button. The **Edit Server Options** dialog box that appears.
2. Click the **IPX** button. The **IPX Frames and Network Numbers** dialog box appears.
3. Click the **Define Filters** button. The **IPX Filter Definition** dialog box appears.

To assign filters to the Black Box server:

1. From the server section of the configuration file window, click the **Edit** button. The **Edit Server Options** dialog box that appears.
2. Click the **Filter** button. The **Server Filter Assignment** dialog box appears.

To assign filters to a user:

1. From the users section of the configuration file window, click **Add**. The **Add User** dialog box appears.
2. Click the **Filter** button. The **User Filter Assignment** dialog box appears.

Packet filtering works in conjunction with the **RADIUS** and **Shared User List** security systems.

**Shared User List** - Filters can be configured and assigned to a user record on the Remote RAS. These records will be sent to the Local RAS when a user dials in and makes a connection.

**RADIUS** – To use packet filtering with the Radius security server:

1. Define the filters on the RAS Server.
2. Configure the user record on the Radius server with the names of the filters to be assigned to the User.
3. When a user dials into the RAS, the name of the filters will be sent from the Radius server to the RAS.



---

# Chapter 5: Configuring Network Protocols

This chapter will provide information and configuration instructions on the network protocols supported by the RAS.

In this chapter you will read about:

- IP parameters, configuration, filters and static routing
- IPX parameters, configuration, filters and static routing
- MAC Addressing
- AppleTalk protocol
- NetBEUI

## IP Parameters

### IP (Internet Protocol) Address

The IP address is a 4 byte number that uniquely identifies a host on the IP network. The IP address consists of a network number, which is the same for every host on the subnet, and a host number, which must be unique for each host on the subnet. The IP address is specified in dotted decimal notation.

### Subnet Mask

A subnet is a logical subsection of an IP network. The Subnet Mask indicates the network portion of the IP address. Enter an IP network mask address in the Subnet Mask field if there is a specific mask that your network requires.

### Default Gateway

The Default Gateway is used to forward IP packets to IP hosts which are not on the local network.

### BOOTP

The RAS can retrieve an IP address for itself from a Bootstrap Protocol (BOOTP) server located on the LAN. When the RAS is first started up, a BOOTP request is sent every 3 seconds (up to 5 times). If a valid IP address is received, the RAS uses it.

## RARP

The RAS can retrieve an IP address from a Reverse Address Resolution Protocol (RARP) server. On start-up a RARP request is sent every 3 seconds (up to 5 times). If a valid response is received, then the IP address is used.

## IP Requirements

This section discusses the requirements to run the RAS on an IP network.

1. IP address for the RAS. This address will be obtained using the following ways. The Black Box RAS will try each of these methods in the order they are described until a valid address is found.
  - a) Acquire an IP address from a BOOTP server.
  - b) Acquire an IP address from an RARP server.
  - c) Use the configured IP address.
2. Subnet Mask.
3. Default Gateway address.
4. IP address for any routing based dial-in clients. This address can be configured in the following ways. The RAS will look at each of these methods in the order they are described until a valid address is found.
  - a) Client specifies an IP address at connect time.
  - b) The user record has been configured with an IP address.
  - c) The serial port to which the client is connecting has been configured with an IP address.
  - d) The RAS has been configured with an IP address pool.
  - e) The Dynamic Host Configuration Protocol (DHCP) server supplies the IP address.

**Note:** The Perle Remote does not need an IP address. It uses only MAC addressing for directing data packets. However, since users may be running IP applications on a PC running the Perle Remote, they will still need an IP address. The address in this case will need to be configured on the PC.

## Configuring IP Parameters

To configure IP parameters, follow these steps.

1. If you are to use a BOOTP or RARP server on your network for IP address acquisition, then install and set up this server.
2. From the Server section of the **Configuration File** window, click **Edit**.
3. From the **Edit Server Options** dialog box, click on the **IP** button.
4. The **Edit IP Profile** dialog box appears

5. Locate your cursor in the **IP Address** field and edit the number. The subnet mask number is automatically generated following the standard network class rules. You should only change this if your network has special requirements.
6. Enter an **IP address** for a Default Gateway if your network is equipped with a Gateway.
7. The RAS will search for an IP address in both a BOOTP and RARP server by default. If you do not have one of these servers on your network, then clear the check boxes beside the appropriate server field.
8. To define filters, click the **Define Filters** button. See “IP Filter Defintion” on page for more details.
9. To configure IP addresses for dial-in Client users, click the **Client IP Addresses** button and enter the required data. See “Client IP Addresses” on page 50.

10. Click **OK** in the **Client IP Address** dialog box, and click **OK** in each subsequent dialog box until the **Configuration File** window is visible again.
11. The RAS allows you to set up a unique IP address for each user. The address is configured in the user records. If you want to specify an IP address for a user, see “Chapter 6: User Records” on page 71.
12. The RAS allows you to set up a unique IP address for each port on the RAS. If you want to specify an IP address for a serial port, see “Serial Port Options” on page 37.

## Client IP Addresses

An IP address is required for any user that dials into a IP network through the RAS using a routing client such as Windows 95 and Windows NT.

To configure Client IP Addresses:

1. From the Server section of the **Configuration File** window, choose **Edit**. In the **Edit Server Options** dialog box that appears, click on the **IP** button. The **Edit IP Profile** dialog box appears.
2. Click on the **Client IP Address** button. The **Client IP Address** dialog box appears.

The screenshot shows the 'Client IP Addresses' dialog box. It is divided into several sections:

- IP Address Assignment:** Contains five checked checkboxes:  Client,  User List,  Port,  IP Address Pool, and  DHCP.
- DHCP:**
  - Addressing Mode:** Radio buttons for  Discover and  Specify.
  - IP Address:** A text input field with an **Add** button to its right and a list box below it with a **Remove** button to its right.
  - Lease Duration:** A text input field containing the number '3'.
  - Reconnect Enable
- IP Address Pool:**
  - Address:** A text input field.
  - Count:** A text input field.
  - A list box below these fields.
  - Add** and **Remove** buttons to the right of the list box.
- DNS/WINS Server IP Address:**
  - Primary DNS:** Text input field.
  - Secondary DNS:** Text input field.
  - Primary WINS:** Text input field.
  - Secondary WINS:** Text input field.
- Buttons:** **OK**, **Cancel**, and **Help** buttons at the bottom.



3. In the IP Address Assignment area, check one or more of the following checkboxes to specify how the dial-in client is assigned an IP address. The server will use all selected methods in the order they are listed below. The search will stop when a valid address is found.
  - a) **Client** - Dial-in client provides his own address. This address is entered when the dial-in client is configured.
  - b) **User List** - The RAS's user list can be configured to have an IP address for each user. If you want to specify an IP address for each user, see “Configuring a User Record” on page 71.
  - c) **Port** - Each of the dial-in ports can be configured to have an IP address. See “Serial Port Options” on page 37.
  - d) **IP Address Pool** - A pool of addresses can be defined on the server. An address is selected from that pool and relayed on to the client.
  - e) **DHCP** - Upon client connection the DHCP server is contacted and an IP address is obtained. Except for the Client option, the RAS will pass the IP address to the Client software when a user dials in and makes a connection.

#### 4. **IP Address Pool**

If the IP Address Pool option has been selected in the IP Address Assignment section, then the IP Address Pool configuration section is enabled. A pool of IP addresses can be created and the first available address will be assigned to a dial-in client when a connection is made. The number of addresses in the pool can be as high as the number of serial ports on the RAS being configured.

##### **Adding IP address(es) to the Pool**

- a) Enter an **IP address** in the **Address** field.
- b) Optionally enter a value in the **Count** field.
- c) Click the **Add** button.
- d) The address or range of address will be displayed in the IP Address Pool list.

##### **Removing an IP Address from the Pool**

- a) Select the **IP address** from the IP Address Pool list.
- b) Click the **Remove** button.
- c) The address will be deleted from the IP Address Pool list.

### 5. DHCP

DHCP (Dynamic Host Configuration Protocol) permits the management of IP addresses (and other IP related options) from a single location. DHCP Servers are used to assign addresses to Hosts (PC's) that do not require a fixed or static IP address. Upon connection the RAS will obtain a IP address lease from the DHCP server and relay the address on to the client. The RAS will maintain and renew the lease as necessary. The DHCP server will also return Primary and Secondary DNS (Domain Name Server) IP addresses as well as Primary and Secondary WINS (Windows Internet Name Server) IP Addresses. WINS is also sometimes referred to as NetBios Name Server. If the client is configured to accept these parameters from the RAS these will be passed on to the client.

If the DHCP option has been selected in the IP Address Assignment section, then the DHCP configuration section is enabled. Select or enter the following data as required.

#### Address Mode

- 1) Select Discover to allow the RAS to find any DHCP server on the local network with an available address.
- 2) Select Specify to configure the IP addresses of the DHCP servers. Up to four DHCP server addresses can be configured. If one is not responding or does not have any IP addresses available the next one will be tried.

#### Adding a DHCP IP address

- a) Enter an **IP address** in the **IP Address** field.
- b) Click the **Add** button.
- c) The address will be displayed in the IP Address list.

#### Removing a DHCP IP Address

- a) Select the **IP address** from the IP Address list.
- b) Click the **Remove** button.
- c) The address will be deleted from the IP Address list.

#### Lease Duration

This field specifies the length of time that the DHCP server will allow the RAS to use the IP address on behalf of the client. The range is 1 to 99 hours. The default is 3 hours. Longer lease time will increase the chances that a client can reconnect to the RAS and get the same IP address.

**Reconnect Enable**

Click on this check box to allow a dial-in user to disconnect and then reconnect at a later time and retain the same IP Address.

**Note:** If the lease on the IP address has expired, then another user may have been assigned that address.

**Note:** This feature requires that all dial-in users have a unique User ID.

**6. DNS/WINS Server IP Address**

For networks that do not have DHCP server, a Primary and Secondary DNS and WINS server IP address can be configured in the RAS. The address will be passed to the dial-in client when a connection is made.

**Addresses for Direct Polling**

When IP routers are configured not to route IP broadcast messages, the manager is unable to detect the presence of any Black Box servers that are not on the local LAN segment.

The Direct IP Address Polling feature enables the user to configure the IP addresses of the servers that are on remote LAN segments. The manager can poll these addresses directly so that the servers can be found.

To add RAS IP addresses to the polling list:

1. Enter the Black Box server's name in the **Server Name** field. The name consists of up to 15 alphanumeric characters.
2. Enter the **IP Address** for the server in dotted decimal notation.

3. Click the **Add** button. The entry will be added to the list. The list is sorted alphabetically according to the **Server Names**.
4. Click **OK**. The list of addresses will be stored on the Manager PC's hard disk in a file called `remhosts.ini`.
5. The **Server List** dialog box will re-appear. The Manager program will now send messages directly to the addresses contained in the IP address list. If a response is received then the entries in the Server List will be enabled.
  - If no response is received, then the entry in the Server List will be disabled and the Model field will be filled with asterisks (`*****`).
6. See “Server List” on page 20 for instructions on how to make a connection to a server.

To remove IP addresses from the polling list:

1. Select the entries in the IP Address list that you want to remove. The **Ctrl** and **Shift** keys can be used to select multiple entries.
2. Click the **Remove** button. The entries will be removed from the list.
3. Click **OK** to save the new list to the `remhosts.ini` file.

### **remhosts.ini File**

This file contains the list of IP addresses for Direct Polling. It is located in the installation directory for the Black Box Manager program (default is `C:\raccess`). It is read and written to be the IP Address for Direct Polling dialog box.

Each entry is kept on an individual line. The server name starts in the first column followed by the IP address. If the server name contains any spaces, then the entire server name will be enclosed in quotes. The server name and the IP address will be separated by at least one space or tab character.

## IP Static Routing

The RAS has room for 100 entries in its IP Routing Information Protocol (RIP) table. In some large networks, there are more than 100 servers. As a result, some of the RIP table entries will be overwritten and some of the routes will be unavailable.

Static routing lets the network administrator configure the RAS with only the server address routes that are required. Dynamic routing is disabled and the routing table will not change.

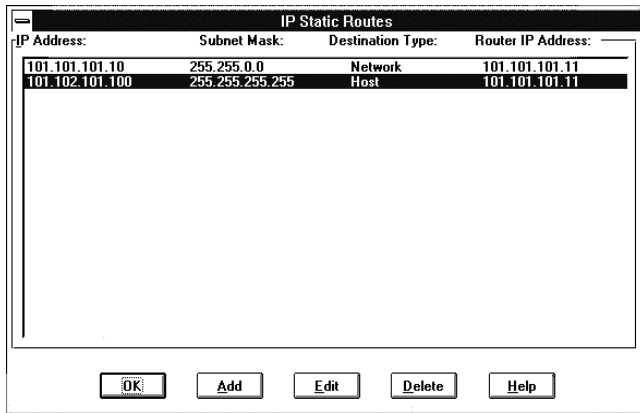
**Note:**  The RAS Manager when used with an in-band connection will broadcast a message to find all RASs on the network. If Static Routing is enabled for a RAS, then a static route to the Manager's network will need to be configured. This is required for the RAS to respond to the Manager's broadcast message.

## Configuring IP Static Routing

1. From the Server section of the **Configuration File** window, click the **Edit** button.
2. From the **Edit Server Options** dialog box, click on the **IP** button.
3. In the **Edit IP Profile** dialog box, click the **Enable IP static routing** check box.

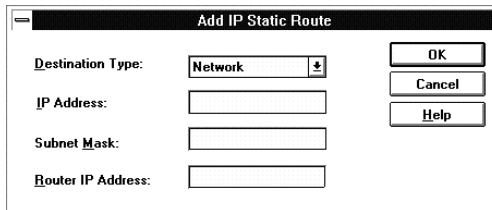
**Note:** Dynamic routing will be disabled. If new servers are added to the network, then the routing for these will need to be added to the static routing table.

- Click on **Static Route** button. The **IP Static Routes** dialog box appears.



A list of all IP static routes currently configured are displayed. You can **Add** a new entry, or **Edit** or **Delete** an existing highlighted entry.

- To configure a new static route, click the **Add** button.
- To edit an existing entry, select an entry from the table and click the **Edit** button.
- The **Add or Edit Static Route** dialog box appears. Enter the following parameters.



### Destination Type

The IP destination type. If the destination type is Host, the Subnet Mask is not user-selectable.

### IP Address

The IP address for the destination server.

**Subnet Mask**

The IP subnet mask for the destination. If the Destination Type is Host, this value is not user-selectable.

**Router IP Address**

The IP address of the router used to send packets to the destination.

8. Click **OK** to return to the **IP Static Route** dialog box.
9. Click **OK** in the **IP Static Route** dialog box to save the static route entries.

## IP Filter Definition

Use this window to create and manage the list of up to 50 filters for the IP protocol. IP filters can specify the Address, Mask, Sub-Protocol and Port of the IP packet. The filters can accept or reject incoming packets based on source and destination addresses.

To add a filter definition:

1. Click the **Add** button.
2. The **Add IP Filter Definition** window will appear.

To edit a filter definition:

1. Select a filter from the list.
2. Click the **Edit** button.
3. The **Edit IP Filter Definition** window will appear.

To delete a filter definition:

1. Select a filter from the list.
2. Click the **Delete** button.
3. The filter definition will be deleted.

## Add / Edit IP Filter Definition

To complete or modify the filter definition, enter the information in the following fields:

### Name

The filter name can be up to 8 characters in length. You will use the name to assign filters to the server or user. The name can also be used when adding filters to a user record on a RADIUS security server.

### Filter Action

Select whether to **Accept** or **Reject** incoming IP packets if the packet matches all parameters defined in this filter. The default setting is **Reject**.

### Source Address

This field is the IP address of the station that is sending the IP packet. The address should be entered in dotted decimal notation.

### Source Mask

This feature masks off both the filter source address and the packet source address by using the Boolean AND function. If the two results are equal, then the address matches.

### Destination Address

This field is the IP address of the station to which the IP packet is being sent. The address should be entered in dotted decimal notation.

### Destination Mask

This feature masks off the filter destination address and the packet destination address by using the Boolean AND function. If the two results are equal, then the address matches.

### Protocol

The entries are TCP, UDP, ICMP, and Other.

- If you select TCP or UDP, the Port Number section appears. Enter the Source and Destination in the corresponding fields.
- If you select Other, make an entry in the **Protocol** field.

Once you have entered the correct information, click **OK** to save your changes.



## IPX Parameters

### Auto

The Auto setting will automatically determine the IPX framing type on the network. When the RAS is powered up, it sends a message encoded in each frame type and waits for a response. It detects only the first framing type found. If your network has multiple frame types, you need to manually enable each type.

### Specify Manually (802.2; 802.3; SNAP; Ethernet II)

Manual specification is useful for a multiple frame environment.

### Dial-In Network

Dial-In Network is an IPX network to which all remote Dial-In IPX clients are connected. The RAS appears as the IPX router with the LAN attached to one side and all of the Dial-In clients attached to the other side.

## IPX Requirements

This section discusses the requirements to run the RAS on an IPX network.

1. IPX network number and frame type for the server. This information is usually determined automatically by the RAS.
2. IPX number for dial-in clients. The RAS can determine this automatically.

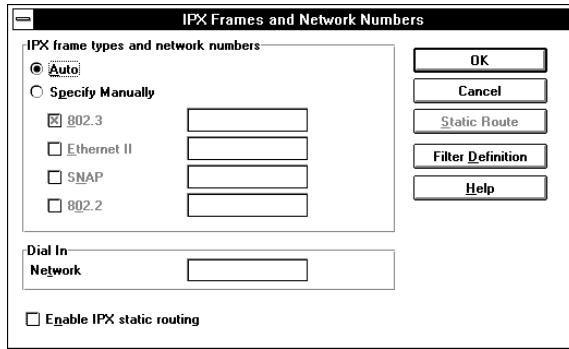
**Note:** The Perle Remote does not need an IPX network number if it is using the NetBUEI/LLC protocol. It uses MAC addressing for directing data packets.

## Configuring IPX Parameters

To configure IPX parameters, follow these steps.

1. From the Server section of the **Configuration File** window, click the **Edit** button.
2. From the **Edit Server Options** dialog box, click the **IPX** button.

- The **IPX Frames and Network Numbers** dialog box appears.



- Click the **Auto** radio button to let the RAS determine the frame type and network numbers it needs to route IPX frames.

or

Click on **Specify Manually** if you want to control the frame types to be enabled. Frame types that are unavailable appear grayed-out and cannot be selected.

- Click the check box next to each frame type you want to enable for this RAS. Leave the address field blank to have the server supply a network address.
  - If you type a *fixed* NetWare IPX network address, the RAS will not update network numbers to resolve conflicts for that frame type. The address field contains up to 8 hexadecimal digits. Do not enter FFFFFFFF or 0, as these addresses are reserved.
- The RAS will by default determine a suitable network number for the Dial-In connections. If your network application requires you to set a fixed value, then enter this value in the Dial-In Network field.

## IPX Static Routes

The RAS has room for 100 entries in its IPX Routing Information Protocol (RIP) table. In some large networks, there are more than 100 servers. As a result, some of the RIP table entries will be overwritten and some of the routes will be unavailable.

Static routing lets the network administrator configure the RAS with only the server address routes that are required. Dynamic routing is disabled and the routing table will not be changed.

**Note:**  The RAS Manager when used with an in-band connection will broadcast a message to find all RASs on the network. If Static Routing is enabled for a RAS, then a static route to the Manager's network will need to be configured. This is required for the RAS to respond to the Manager's broadcast message.

## IPX Network Services

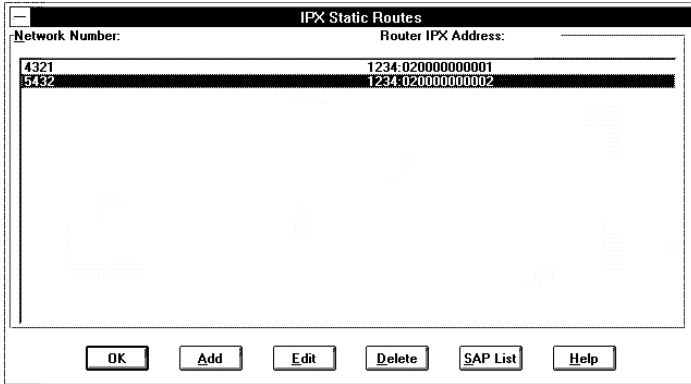
The RAS also keeps a 100 entry Service Advertising Protocol (SAP) table. This table will contain a list of IPX network service programs and their locations within the IPX network. When IPX Static Routing is enabled, SAP entries need to be made for each network service available at each of the IPX static routings.

## Configuring IPX Static Routing

1. From the Server section of the **Configuration File** window, click the **Edit** button.
2. From the **Edit Server Options** dialog box, click on the **IPX** button.
3. On the **IPX Frames and Network Numbers** dialog box, click the **Enable IPX Static Routing** check box. The option for IPX frame types and network numbers will change to **Specifying Manually**. Select at least one frame type, and enter a network number for each frame type you select. Static routing cannot automatically determine network numbers.

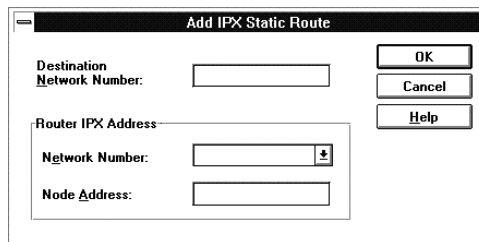
**Note:** Dynamic routing will be disabled. If new servers are added to the network, then the routing for these will need to be added to the static routing table.

- Click on the **Static Route** button. The **IPX Static Routes** dialog box appears.



A list of all the IPX static routes currently configured are displayed. You can Add a new entry or Edit or Delete an existing highlighted entry. For each IPX static route, a list of IPX services that are available at the IPX destination can be created.

- To configure a new static route, click the **Add** button.
- To edit an existing entry, select an entry from the table and click the **Edit** button.
- The **Add or Edit IPX Static Route dialog box** appears. Enter the following parameters.



### Destination Network Number

The IPX network number for the destination. This can be up to 8 digit hexadecimal numbers.

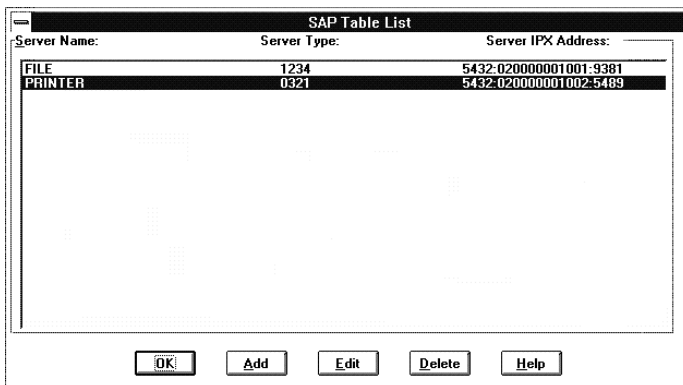
### Network Number

The IPX network number for the router on the local LAN. Only those network numbers that you have already given to frame types are listed.

### Node Address

The IPX node address of the router on the local LAN. This is a 12 digit hexadecimal number.

8. Click **OK** to save the entry and return to the **IPX Static Route** dialog box.
9. To configure SAP entries for an IPX static route, select an IPX static route entry and click the **SAP List** button. The **SAP Table List** dialog box appears.



A list of all the SAP table entries currently configured for the selected IPX static route are displayed. You can **Add** a new entry or **Edit** or **Delete** an existing highlighted entry.

10. To configure a new SAP entry, click the **Add** button.
11. To edit an existing entry, select an entry from the table and click the **Edit** button.

12. The **Add or Edit SAP Entry** dialog box appears. Enter the following parameters.

The screenshot shows a dialog box titled "Add SAP Entry". It contains the following fields and buttons:

- Server Name:** An empty text input field.
- Server Type:** An empty text input field.
- Server IPX Address:** A sub-section containing three fields:
  - Network Number:** A text input field containing the value "5432".
  - Node Address:** An empty text input field.
  - Socket Number:** An empty text input field.
- Buttons:** Three buttons are located on the right side: "OK", "Cancel", and "Help".

**Server Name**

The server name of the IPX static route destination. The name can be up to 48 characters long.

**Server Type**

The server type of the IPX static route destination. This is a 4 digit hexadecimal number.

**Network Number**

The IPX static route table network number for the destination that you have already entered. Not user-selectable in this dialog box.

**Node Address**

IPX node address for the destination. This is a 12 digit hexadecimal number.

**Socket Number**

IPX socket number for the destination. This is a 4 digit hexadecimal number.

13. Click **OK** to save the entry and return to the SAP table list.

## MAC addresses

This section will be of concern to you if you use the Perle Remote with the NetBEUI/LLC protocol.

Media Access Code (MAC) addresses represent the physical address of a network. When the Perle Remote is used with the NetBEUI/LLC protocol, these address are used to send and receive messages to the LAN services.

Each RAS model has several MAC addresses for communication on the LAN. One MAC address is assigned to the RAS itself, and one MAC address is assigned to each serial port. A two-port server requires a minimum of three addresses, and an eight-port server requires a minimum of nine addresses. These address have default values when the server is shipped from the factory. These should not need to be changed.

If fixed MAC addresses are assigned to any users, then these default values have to be modified.

### MAC addresses and Black Box RAS

A RAS's MAC addresses are set at the factory to unique values. If you need to change from the default MAC addresses, you can use address values that end in 00 in the range of 020000000000 to 02FFFFFFF00 (for Ethernet) and 400000000000 to 40FFFFFFF00 (for Token Ring).

### Fixed MAC Addresses

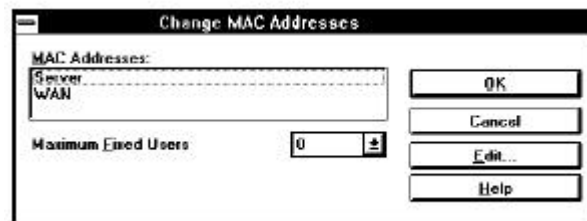
The Perle Remote software when running with the NetBEUI/LLC protocol needs to have a MAC address to communicate properly with the LAN services. Some applications need to know this address when the Perle Remote PC is powered up. As well some applications ( i.e. AS/400 Client Access) required a dial-in user to have the same MAC Address each time they dial-in to the network. These conditions are satisfied by configuring a fixed MAC address for each user on the RAS in the user profile. The user would then configure the Perle Remote with this same fixed address.

To configure fixed MAC address on the RAS, you must change the base modem port address to a user defined value. You must also indicate the maximum number of fixed MAC address users allowed in the network.

**Note:**  The RAS will respond to all addresses in the range selected (base address plus number of modem ports plus number of fixed MAC address users).The number of fixed MAC address users in no way limits the total number of users.

**To configure fixed MAC addresses, follow these steps:**

1. From the Server section of the **Configuration File** window, click the **Edit** button.
  - a) From the **Edit Server Options** dialog box, click on the **MAC Addresses** button.
  - b) A dialog box appears displaying the MAC address of the connected RAS, and the base asynchronous WAN (serial ports) MAC address.



2. Select the WAN MAC address and click the **Edit** button.
3. In the dialog box that appears, type in the new 12-digit hexadecimal MAC address, and click **OK**. Make sure you comply with the numbering restrictions which were described above.

**Note:** When the WAN base address is modified, then the MAC address for a specific serial port is found by adding the port number to the base address and subtracting 1.

<b>Base Address</b>	<b>Port 5 Address</b>
020012345600	020012345604

4. Set the number of fixed address users to the closest value equal to or greater than the actual number of fixed address users required in the network.
5. Click **OK** in the **Change MAC Addresses** dialog box, and click **OK** in each subsequent dialog box until the Configuration File window is visible again.
6. To set the fixed MAC address for each user, see "Chapter 6: User Records" on page 71. The address will be automatically assigned to each user from the MAC address pool.



## IPX Filter Definition

Use this window to create and manage the list of up to 50 filters for the IPX protocol. IPX filters can specify the Network, Node, Socket and Sub-Protocol. The filters can accept or reject incoming packets based on source and destination network and node addresses and socket numbers.

To add a filter definition:

1. Click the **Add** button.
2. The **Add IPX Filter Definition** window will appear.

To edit a filter definition:

1. Select a filter from the list.
2. Click the **Edit** button.
3. The **Edit IPX Filter Definition** window will appear.

To delete a filter definition:

1. Select a filter from the list.
2. Click the **Delete** button.
3. The filter definition will be deleted.

### Add / Edit IPX Filter Definition

To complete or modify the filter definition, enter the information in the following fields:

#### Name

The filter name can be up to 8 characters in length. You will use the name to assign filters to the server or user. The name can be used when adding filters to a user record on a RADIUS security server.

#### Filter Action

Select whether to **Accept** or **Reject** incoming IPX packets if the packet matches all parameters

defined in this filter. The default setting is **Reject**.

### **Source Network Address**

The address of the network that contains the station that is sending the IPX packet. It can be up to 8 characters long.

### **Source Node Address**

Enter the node address of the station that is sending the IPX packet. It consists of 12 hexadecimal characters.

### **Source Socket Number**

The socket number on the station that is sending the IPX packet. The socket number can be up to 4 hexadecimal characters.

### **Destination Network Address**

The address of the IPX network that the IPX packet is being sent to.

### **Destination Node Address**

The node address that the IPX packet is being sent to.

### **Destination Socket Number**

The socket number that the IPX packet is being sent to.

### **Packet Type**

The entries are RIP, SAP, SPX, NCP, and Other.

- If you select Other, make an entry in the **Type** field. The field can be up to 3 numeric characters.

Once you have entered the correct information, click **OK** to save your changes.

## AppleTalk Protocol

The RAS has built-in support for the AppleTalk Network protocol. This allows an Apple Remote Access (ARA) client running on a Macintosh to dial-in to the server and access the AppleTalk network.

The AppleTalk protocol is always available in the RAS and no special configuration is required. For more information, see “Using Apple Remote Access” on page 84.

## NetBEUI

The RAS supports the NetBios Extended User Interface (NetBEUI) protocol. This permits third party clients (Windows 95 and Windows NT) to be used in a NetBios environment.

There is no configuration required to use this feature.

**Note:** □ The RAS supports up to 10 sessions per connection using NetBios. The maximum sessions in the client NetBEUI configuration must be set to a value of 10 or lower.



---

## Chapter 6: User Records

This chapter describes the uses and configuration steps for the RAS user records. In this chapter you will read about:

- Overview of the User Records
- Adding or editing Users
- Shared User Lists
- Call Back Options

### Overview

The RAS can be configured with a set of user records (known as the User List) which contain profile information about users of the server. These records have the following purposes.

- The records are used for password authentication if the RAS has been configured for **User List** security. See “Chapter 10: Security” on page 103 for more details.
- The records provide information on Call Back options and inactivity time outs for both **User List** and some third party security services.
- At least one user record with administrative privileges must be entered for each RAS. This allows access by the manager program for configuration or monitoring purposes.

The User List can be configured with 256 users. Each user can be configured with up to 5 call back numbers or a maximum of 512. (Average of 2 call back numbers per user).

### Configuring a User Record

New user records can be added, existing records can be edited, copied or deleted. To perform any of these configuration functions, follow these steps:

1. Select or open the proper configuration file as described on page 32.
2. From the Users section of the **Configuration File** window, you can:
  - a) Click the **Add** button to add a new user.
  - b) Select an existing user record and click the **Edit** button to change the user’s information.

- c) Select an existing record and click the **Copy** button. This will create a new user record and copy most of the information from the existing record.
  - d) Select an existing record and click the **Delete** button to remove the user record from the configuration file. Click **OK** to confirm the deletion.
3. The **Add User** or **Edit User** dialog box will appear (except after deleting a record). Enter the following parameters as required.

The screenshot shows the 'Add User' dialog box with the following fields and options:

- User Disabled
- User ID:
- Department:
- Expires:
- Protocols:
  - IP
  - Netbios
  - BCP
  - IPX
  - ABA
  - Bridging
- Administration Privileges
- Set Password:
  - Password:
  - Confirm:
- Activity Time Out:
  - Disabled
  - If inactive  minutes
- Addresses:
  - Fixed MAC Address:
  - IP Address:
- Connect Time:
  - Unlimited
  - Maximum  minutes

Buttons on the right: OK, Cancel, Call Back Options..., Filter, Help.

### User Disabled

A user record is enabled by default. If you want to prevent a user from using the RAS but want to keep the record in the configuration file, then click on the check box.

### User ID

Enter the name of the user. This field is up to 8 characters long. The name is used in combination with the password for log on authorization for **User List** security.

### Department

The department name is for information purposes only. It is not used for granting privileges or access.

### Expires

This option will disable user records on a specific date. Click the check box and enter the date on which the user record should become disabled.

### Protocol Enable/Disable

Disable any **Protocols** that the user should not have access to by removing the check in the check box. All protocols are enabled by default. However, if the server has any protocols disabled, then that protocol will show as disabled for the User.

### Administration Privileges

A user with administration privileges can use the Black Box Manager program to configure this RAS. Click on the check box to enable.

**Note:**  At least one user record must be created with administration privileges for each RAS to allow access by the RAS Manager program.

### Set Password

The password is used for access authentication purposes. Enter a 1 to 8 character password and then enter it again in the **Confirm** field.

**Note:** The **Set Password** fields will be disabled if a third party security service has been configured for the RAS unless the user has been given administration privileges.

All users with administration privileges will be required to enter a valid password.

### Fixed MAC Address

If the RAS has been configured for Fixed MAC addressing (see “Fixed MAC Addresses” on page 65) then each user can be assigned a MAC address using this field. Click the check box and an address will be assigned by the RAS from the fixed MAC address pool and displayed in the address field. If user records are deleted, their reserved addresses are released back into the pool. Fixed MAC addresses only work with a Perle Remote using the NetBEUI/LLC protocol.

### IP Address

Enter an IP address if you want IP addresses assigned for dial-in users on a per user basis (see “IP Requirements” on page 48 for more information on assigning IP address). This address only affects third party routing based dial-in clients (i.e. Windows 95) when they connect to the server. The network portion of the address must be the same as the network portion of the server’s IP address.

### Activity Time Out

This feature will disconnect a dial-in user after a time limit has passed where there is no user activity on the link. The default is to disable this feature and let the user stay connected until they disconnect. To configure an **Activity Time Out**, click the **If inactive** radio button and enter a time value in minutes.

**Note:** Certain protocols may generate data traffic even though the user may not be performing any functions. This may cause the connection to stay open even when the user is inactive.

Use caution when setting this option. Users who are connected to a network when this timer expires will be disconnected, which may adversely affect the operation of certain applications.

### Connect Time

This feature will disconnect a dial-in user after a preset time limit, regardless of activity. The default is to allow the user Unlimited connection time. To configure a time limit, click the **Maximum** radio button and enter a value for the connect time in minutes.

4. Click on the **Call Back Options...** button if these options are required. See “Call Back Options” on page 75 for instructions on how to configure these options.
5. Click on the **Filter** button to assign filters for the user. See “User Filter Assignment” on page 67 for more details.
6. Click **OK** to save add this user record to the user list.
7. Repeat steps 2 through 6 for each user you want to add.

## Shared User Lists

The Shared User List feature allows a RAS to access the User Lists of specified remote RAS servers on the LAN. Two Remote Servers can be defined for the local server. When a user connects to the RAS, a search for the user record will occur in the following order:

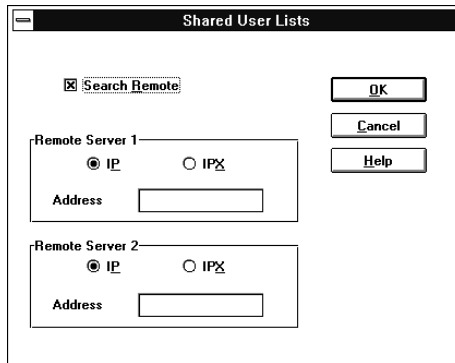
1. Local User List.
2. User List on Remote Server 1.
3. User List on Remote Server 2.

**Note:**  This option will work only if the remote Black Box servers defined below have been configured for Public User List Access.



To configure Shared User Lists:

1. Select or open the proper configuration file as described on page 32.
2. From the Users section of the **Configuration File** window, click the **Shared Lists** button. The **Shared User Lists** dialog box appears.



3. Set the check box of the **Search Remote** field to enable the RAS to search on remote servers.
4. Specify the location of **Remote Server 1** and optionally **Remote Server 2** by:
  - a) Select the Protocol supported by the remote server. The options are **IP** and **IPX**.
  - b) If **IP** is selected, enter the **IP Address** of the remote server. The address should be in dotted decimal notation.
  - c) If **IPX** is selected, enter the **Name** of the remote server. The name can be up to 15 alphanumeric characters.
5. Click **OK**.

## Call Back Options

Call back is a feature of the RAS which can provide an additional level of security and at the same time allows for centralized billing for telephone charges. When a remote user calls in to a RAS and Call Back has been set up, the RAS will disconnect and then call the user back according to the RAS's configuration for the user.

## Call Back Security

Call Back Security is controlled from the Black Box server. The settings can be either Disabled, Required, or Allowed. When Required is selected, the user must be called back by the server. If Call Back is not Requested on the dial-in client, then the Black Box server will disconnect the user and will not call back.

The RAS can be requested to dial back on one of five phone numbers it stores. (Since the actual phone number is never transmitted on the serial line, an unauthorized user cannot attach to the RAS.)

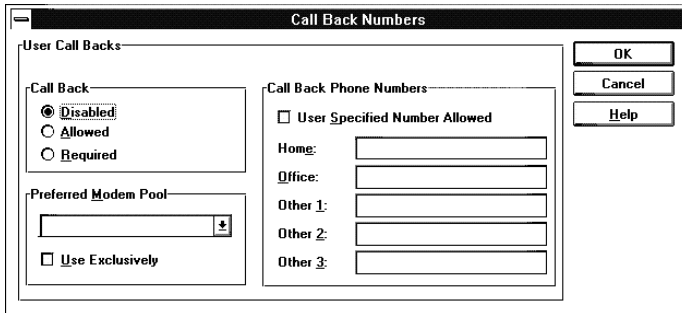
## Centralized Billing

Call Back can be used to centralize all phone charges for the Black Box server. The network administrator configures the RAS for Required Call Back. All dial-in clients will have to request Call Back and as a result all telephone charges for the server will be billed to the telephone lines connected to the server

To set up the Call Back Options:

1. From the Users section of the **Configuration File** window, click on **Add** to add new users, or select an existing user and click **Edit**.
2. If necessary, configure a **User ID**, **Department** and **Password** for this user, and then press the **Call Back Options** button.

The **Call Back Options** dialog box appears.



3. Click the radio button for the **Call Back** option. The choices are:
  - **Disabled** - Call back will not be used.
  - **Allowed** - Call Back will be used if the dial-in user requests the feature.
  - **Required** - Call back must be used. If the dial-in user does not request call back, the RAS will disconnect the user and not call back.
4. Enable the **User Specified Number Allowed** feature if required by clicking the check box. If call back is enabled, this feature allows a user to specify a call back number whenever the RAS is called.
5. Up to five predefined telephone numbers can be entered for the call back option.
6. If you want to assign this user to a specific modem pool for Call Back, then make a selection in the **Preferred Modem Pool** drop down list.

**Note:** Dial-In Modem Pool must be configured before a selection can be made. See “Dial-In Modem Pools” below for configuration instructions.

If you click the **Use Exclusively** check box, the user will not be called back if a modem in the pool is not available.

If you do not check the **Use Exclusively** box, the user will be called back using another pool if no modems are available in the selected pool.
7. Click **OK** to save the Call Back Options.

## User Filter Assignment

Use this window to assign up to 10 IP and 10 IPX filters to the user record. The server will process these filters from the top down, so the order may be important.

To assign IP and/or IPX filters for the user, follow these steps:

1. Select a filter name from the Defined Filters pull-down list and click **Add** to add the filter to the Assigned Filters list.
  - You can change the order of the assigned filters by selecting a filter name from the Assigned Filters list and clicking the Move Up or Move Down buttons.
  - You can delete a filter assignment by selecting a filter name from the Assigned Filters list and clicking the **Remove** button.

2. Set the **Default Action** to be taken if a packet does not match any assigned filter. The choices are to **Accept** or **Reject**.
3. If you want server to override the server assigned filters and only use the user assigned filters, then click the check box on the **Disable Server Filters** field.
4. If you need to define more filters, then click the **Define** button in either the IP or the IPX section. The **IP Filter Definition** or **IPX Filter Definition** dialog box appears.
5. Click **OK** to save your changes.

## Dial-In Modem Pools

A modem pool is a modem or group of modems on a particular RAS which can be used for Call-Back, Dial-Out or both. This section describes the configuration and use of the Modem pools for Dial-In services (see “Dial-Out Modem Pools” on page 91 for more information).

The purpose of dial-in modem pools is to group together modems or ports that have been configured with similar parameters (i.e. same baud rate, or modem speed). As well, selected dial-in users can be assigned to the modem pools. This in effect limits the use of modem pool to the selected users. Up to 4 modem pools may be defined.

By default, no modem pools are defined. Call Back and Dial-Out are disabled.

### Configuration Steps

Follow the steps below to define a modem pool on a RAS.

1. Open the desired configuration file.
2. From the Server section of the **Configuration File** window, choose **Edit**.

- From the **Edit Server Options** dialog box, click the **Modem Pool** button. The **Define Modem Pools** dialog box appears.

The screenshot shows the "Define Modem Pools" dialog box. It features a title bar with the text "Define Modem Pools". Below the title bar is a section labeled "Modem Pools" which is divided into two columns. The left column is titled "Name:" and contains four radio buttons, each followed by a text input field. The right column is titled "Port and Modem Model:" and contains a list of eight items: "1:Direct", "2:Direct", "3:Direct", "4:Direct", "5:Direct", "6:Direct", "7:Direct", and "8:Direct". Below the "Modem Pools" section are two checkboxes: "Call Back" and "Dial Out", and a text input field labeled "Phone number:". At the bottom of the dialog are four buttons: "OK", "Cancel", "Delete", and "Help".

- Click the radio button to the left of the top **Name** field, and place the text cursor in that field. Type a descriptive name for this modem pool.
- Choose the modem or modems that will be in this pool from the list of **Ports and Modem Models** at the right of the dialog box. To select more than one, press and hold the **Shift** key and click on the desired modems.
- Click the **Dial In** check box.
- Click **OK** to return to the **Edit Server Options** dialog box. Click **OK** to save the modem pool.



---

## Chapter 7: Dial-In

This chapter provides the details for configuring the RAS for Dial-In. It also describes some third party dial-in clients and any special considerations that are required for their use.

### Overview

Dial-In allows remote users, using client software, to access a LAN and perform tasks as if they were directly attached to it, using inexpensive voice-grade telephone circuits and asynchronous modems.

### Configuring Dial-In

To configure the RAS for dial-in:

1. Each port that will be used for dial-in will need to have the **Dial-In** function enabled. See “Serial Port Options” on page 37.
2. A User record must be added to the User List for each dial-in user for security access. If the User List will be used, see “Chapter 6: User Records” on page 71. This is the default security method. If third party security options will be configured, see “Chapter 10: Security” on page 103.
3. A network protocol appropriate address (i.e. IP address, or MAC address) must be configured for each dial-in user. This will depend on the network protocol being used on the LAN and the dial-in client being used to access the LAN. See “Chapter 5: Configuring Network Protocols” on page 47 for details.
4. Provide users with the necessary information for them to access the RAS. This will include:
  - User Name
  - Password
  - MAC address for Perle Remote users if they are using Fixed MAC addressing.
  - Call Back options.
5. Download the Configuration File to the RAS. See “Download the Configuration” on page 41.
6. Users need to install and configure their dial-in client. Refer to the client installation manual for instructions. For the Perle Remote, see the *Perle Remote User's Guide*.

## Using Windows 95 Dial-up Networking

Windows 95 contains all of the features necessary to connect with the Black Box server. With the instructions in this chapter, connecting to your LAN through the RAS using a dial-up connection is a simple matter.

### What You Need

The first step in connecting to a RAS is to contact your network administrator to work out the details of your User ID and password, as well as the phone number and other settings you may need to know about. You may want to ask about IP addressing or Netware addressing features available to you. You also need to perform the following tasks before configuring a connection.

1. Install a modem. 14.4 Kbps or higher is recommended.
2. Obtain a Windows 95 set of install disks or CD ROM for files that may be required.

### Configuring a New Connection

The following steps will create a new connection for dial-up networking.

1. Locate the Dial-Up Networking icon and open it. It may be under My Computer on the desktop, or under Accessories in the Program group.
2. Enter the name of your New Connection. For example, you may enter **RAS**. Also, select the modem type and line speed you will be using. Click on **Next**.
3. Enter the telephone number of the modem to which you wish to connect. Click on **Next**.
4. After this process, Windows 95 creates an icon with the name of your Network Connection in the Dial-Up Networking folder.

**Note:** Depending upon how your computer is configured, you may need to install networking software manually using the Network icon in the control panel. If you will be supplying an IP address from your PC, the network portion of your address must match the network portion of the RAS's IP address.



## Making a Dial-Up Networking Connection

1. Open the icon with the name of the Network Connection you want to make.
2. Fill in the required User ID and password information, and click on **Connect**. If everything has been installed properly, the connection to the RAS will pass you to your LAN.
3. When your LAN sign-on screen appears, perform a normal log in.

## Call Back Options

The RAS supports Call Back with the Window 95 dial-in client. To use this feature, the RAS must be configured with the desired Call Back options. See “Call Back Options” on page 75 for configuration instructions. Following is a list of these options and how Windows 95 operates with them.

### Disabled

- Call back not used

### Required

- Call back must be used.
- If CANCEL is selected in the **Windows 95 Client Callback** dialog box, then the connection will not be established.

### Allowed

- The client has the option of using call back.
- If CANCEL is selected in the **Windows 95 Client Callback** dialog box, then the connection will be established without call back.

## Call Back Phone Numbers

- If any phone numbers have been configured in the RAS’s **Call Back Phone Numbers** list then the first configured number will be used (order is home, office, other1, other2, other3). The **User Specified Number Allowed** check box has no effect.
- If the phone number list is empty and the **User Specified Number Allowed** check box is enabled, then the Windows 95 Client user will be allowed to enter a phone number for call back.

## Using Apple Remote Access

The RAS has built-in support for Apple Remote Access (ARA). Using Apple remote Access Client software, your Macintosh can communicate with another Macintosh or an AppleTalk Network. The RAS supports both ARA Version 1 and 2.

In some instances, the modem scripts that are supplied with the Apple Remote Access (ARA) client software may not work with the RAS. It is recommended that you use Version 2 ARA client software.

If you are using a Version 1 ARA client, you must change the modem initialization settings for the RAS. Version 1 ARA software requires that the modem does not negotiate compression or error correction. Other dial-in clients and protocols will still work in most cases, but performance for these clients could be degraded. See “Creating a Custom Modem Configuration” on page 133.

If you are using a Version 2 ARA client, the modem settings as shipped by Apple may not work. As with the Version 1 client, you may disable error correction in the server. However, you can retain your server settings by changing the modem configurations used with the ARA software. See your modem vendor for these files. Also, the Apple Remote Access Modem Toolkit Version 2.0 available from Apple will permit you to create custom modem configurations.

## Configuration

To configure the Apple Remote Access Client, see your Apple Remote Access Client User’s Guide for details.

Because ARA is always available in the RAS, no special configuration is required to enable ARA. However, the client name and password must match the name and password of a user record configured in the RAS. The name and password are used to access the RAS only, and do not correspond to names and passwords used to access other Macintoshes. See “Chapter 6: User Records” on page 71 for more details on configuring a user record.

The RAS also supports Call Back. To enable this option, you must set Call Back to Required in the Black Box Manager and provide your home phone number. See “Call Back Options” on page 75 for more information. The client does not support other phone numbers or the **Call Back Allowed** option.

---

## Chapter 8: Dial-Out

This chapter provides the details for configuring the RAS for the Dial-Out.

### Overview

The Dial-Out support by the RAS allows users on a LAN workstation to connect to a destination that is external to their LAN. This is done by dialing out via a Black Box server modem instead of a modem attached directly to the users's PC. For dial-out users, the benefit of sharing these modems across a network is that they can make efficient use of the hardware and phone lines that are already installed on the network.

The user can connect to a BBS, internet provider or any other service accessible by the telephone network.

### Configuring Dial-Out

A summary of the configuration steps for dial-out are provided in this section. Later sections in this chapter will provide more details.

1. Each port that will be used for dial-out will need to have the **Dial-Out** function enabled. See "Serial Port Options" on page 37.
2. Configure the Dial-Out parameters for each port.
3. Configure the dial-out parameters for the server.
4. Configure Modem Pools.
5. Provide users with the necessary information for them to access the RAS. This will include:
  - Modem Pool and /or Line Names.
6. Download the Configuration File to the RAS. See "Download the Configuration" on page 41.
7. Users need to install and configure the RAS Dial-Out software on their PC. Refer to the *Black Box Dial-Out User's Guide*.

## Port Dial-Out Parameters

The Dial-Out parameters options are used to set up default communication options and flow control. While the client has the option to override these settings, these are the default parameters the client will use if the “use server defaults” option is enabled in the client software.

**Note:** It is important to note that the Flow Control and other parameters match the modem they are being set up for. If the settings are different, a connection may not be possible.

### Configuration Steps

Follow the procedure below to configure the Dial-Out parameters.

1. Open the configuration file for the appropriate RAS.
2. In the Port section of the **Configuration File** window, select the port or ports you want to configure and click the **Edit** button.
3. Click the **Dial-Out Parameters** button. The **Dial-Out Default Parameter for Port** dialog box appears:

The screenshot shows a dialog box titled "Dial Out Default Parameters for Port 1". It is organized into three columns:

- Communication parameters:**
  - Baud Rate: 38400
  - Parity: NONE
  - Data Bits: 8
  - Stop Bits: 1
- Flow Control:**
  - No flow control
  - Xon/Xoff flow control
    - Xon: 11H
    - Xoff: 13H
  - Hardware flow control
- Data Forwarding:**
  - Packet size: 140 bytes
  - Character timeout: 60 msec
  - Packet timeout: 720 msec
  - Trigger characters: (empty field)

At the bottom of the dialog are three buttons: OK, Cancel, and Help.

4. Set the following parameters as required:

---

## Communication Parameters

### Baud Rate

The line speed used to transfer the data. Select the maximum speed supported by both the modem and the communications program. The default rate is “38400” baud.

### Parity

Select the parity type that matches the setting at the calling destination (contact the destination site to verify this information) and in the dial-out client communications program. The default setting is “NONE”.

### Data Bits and Stop Bits

Select the data bits and stop bits that match the settings used at the calling destination and in the dial-out client communications program. The default settings are “8” data bits and “1” stop bit.

### Flow Control

Select whether or not you want to use flow control and, if so, the type of flow control. Flow Control regulates the flow of traffic between the server port and the modem. Match the selection to a comparable setting in the communications program.

Select one of the following options:

- No flow control.
- Xon/Xoff flow control (to use the software flow control). The Xon/Xoff fields display standard industry values. You should never need to change these values.
- Hardware flow control. This is the default setting and one that can be used throughout the system, including the server, client, application and modem for almost all situations.

## Data Forwarding

### Packet Size

Enter the size of the individual network transmissions. “Packets” are blocks of data transmitted on a network. Consider the following implications before you make any changes to the default setting. Setting the number lower results in more frequent network transmissions because packets are always sent when they are full. This change results in higher network traffic. Due to these implications, do not change the packet size unless you have a specific reason to do so. The default setting is “140” bytes. The minimum is 1 and the maximum settings is 512. If you do change the packet size, review the setting for packet timeout.

### Character Timeout

Enter the duration of the character timeout in milliseconds. “Character Timeout” is the maximum amount of time that can elapse without a character being sent. The packet is transmitted after the time period has elapsed. Consider the following implications before you make any changes to the default setting. Setting the number lower can improve the responsiveness of the system if you are typing data, but may result in higher network traffic. To ensure this setting is valid, make sure the number is lower than the “Packet timeout” number. Network packets are always sent when they are filled, or if the packet timeout expires. The default installation setting is “60” milliseconds. The minimum is 0 and the maximum is 65535. A value of “0” disables the timer.

### Packet Timeout

Enter the duration of the packet timeout in milliseconds. “Packet Timeout” is the maximum amount of time that a packet will wait for data before the packet is sent. Packet timeout begins countdown when the first character is placed in a packet. Consider the following implications before you make any changes to the default setting. If the typical data transmission is smaller than a packet, lower the number. This can improve the responsiveness of the system. The default installation setting is “720” milliseconds. The minimum is 0 and the maximum is 65535. A value of “0” disables the timer.

## 5. Trigger Characters

Set trigger characters only if you have very specific communications needs. They are not for general use. Click on the **Trigger Characters** button and the **Trigger Character for Port** dialog box appears

Trigger Characters for Port 1

Trigger Characters

Enter up to 16 trigger characters in decimal or hexadecimal (value followed by the letter H).

1. <input type="text"/>	2. <input type="text"/>	3. <input type="text"/>	4. <input type="text"/>
5. <input type="text"/>	6. <input type="text"/>	7. <input type="text"/>	8. <input type="text"/>
9. <input type="text"/>	10. <input type="text"/>	11. <input type="text"/>	12. <input type="text"/>
13. <input type="text"/>	14. <input type="text"/>	15. <input type="text"/>	16. <input type="text"/>

OK Cancel Help

A trigger is a character that forces the transmission of a network packet. Data characters accumulate in packets when they are received from the phone line or sent from the modem. These packets are sent under one of the following circumstances:

- a packet is filled
- a character timeout occurs
- a packet timeout occurs
- a trigger character is encountered.

Enter up to 16 characters in decimal or hexadecimal (followed by the letter H). The default setting is none, that is, the 16 boxes are empty.

*Case scenario:*

If you are doing many file transfers and you know that each data transmission block ends with a consistent, unique end character, then you can define this character as a trigger. This will ensure that when a block of data has been received, it is forwarded immediately.

6. Click **OK** on the **Trigger Characters for Port** dialog box to accept the changes.
7. Click **OK** on the **Dial-Out Default Parameter for Port** to accept the dial-out parameter changes or click **Cancel** to exit without saving.

## Server Dial-Out Parameters

The server dial-out parameters apply to all dial-out connections. Client Timeout is the only configurable parameter.

### Configuration Steps

Follow the procedure below to configure the Dial-Out parameters.

1. Open the configuration file for the appropriate RAS.
2. In the Server section of the **Configuration File** window, click the **Edit** button.
3. From the **Edit Server Options** dialog box, click the **Dial-Out** button.
4. The **Dial-Out** dialog box appears. Enter a value for the Client Timeout period in minutes. The RAS will periodically check to make sure the client is connected to the LAN. If the client has been disconnected for the Client Timeout period, then the modem can be released. The default is 1 minute.
5. Click **OK**.



## Dial-Out Modem Pools

A modem pool is a modem or group of modems on a particular RAS which can be used for Call-Back, Dial-Out or both. This section describes the configuration and use of the Modem pools for Dial-Out. See “Dial-In Modem Pools” on page 78 for more information.

The purpose of dial-out modem pools is to group together modems or ports that have been configured with similar parameter (i.e. same baud rate, or modem speed). Up to 4 modem pools may be defined.

By default, no modem pools are defined. **Call Back** and **Dial-Out** are disabled.

### Configuration Steps

Follow the steps below to define a modem pool on a RAS.

1. Open the desired configuration file.
2. From the Server section of the **Configuration File** window, choose **Edit**.
3. From the **Edit Server Options** dialog box, click the **Modem Pool** button. The **Define Modem Pools** dialog box appears.

4. Click the button to the left of the top **Name** field, and place the text cursor in that field. Type a descriptive name for this modem pool.
5. Choose the modem or modems that will be in this pool from the list of Ports and Modem Models at the right of the dialog box. To select more than one, press and hold the **Shift** key and click on the desired modems.

6. Click the **Dial Out** check box.
7. Normally, the dialing function is performed by the communication application on the dial-out client PC. However, if a phone number is entered in the **Dial Out Phone Number** field, the server will automatically do the dialing as soon as a connection request is received from the client. In this case the application would not do the dialing. Up to 24 phone number digits can be entered.  
*Note:*  The Black Box Dial-Out client software can be configured with a phone number instead of a pool or a port name. In this case, any available dial-out port will be assigned to the client and the dialing function will be performed by the server.
8. Click **OK** to return to the **Edit Server Options** dialog box. Click **OK** to save the modem pool.

---

## Chapter 9: Network Administration

This chapter provides information that an administrator needs when managing a RAS on a LAN. In this chapter you will read about:

- SNMP and how to use it
- Viewing Statistics
- Log File
- Software Upgrades

### What is SNMP?

SNMP, or Simple Network Management Protocol, is a command/response protocol used for managing IP devices on a network. It facilitates communication between the SNMP Manager and SNMP Agents.

The SNMP Manager issues requests for status, performance and configuration information. The information acquired is usually displayed and used for network administration.

SNMP Agents run on network devices and respond to commands issued by the SNMP Manager. Depending on the source and access privileges of the request, SNMP Agents may or may not issue the requested information. Access levels range from:

- No Access—the SNMP Manager does not have access privileges.
- Read-Only—the SNMP Manager can read the information only but can not edit it.
- Read/Write—the SNMP Manager can read and edit the information.

The RAS runs the SNMP Agent and supports the following RFCs:

- 1157 - A Simple Network Management Protocol (SNMP)
- 1213 - Internet Standard MIB (MIB II)
- 1215 - SNMP traps
- 1471 - Point-to-Point (PPP)
- 1573 - Extensions to MIB II
- 1643 - IEEE 802.3 Ethernet
- 1659 - RS-232 hardware devices
- 1742 - AppleTalk
- 1743 - IEEE 802.5 Token Ring

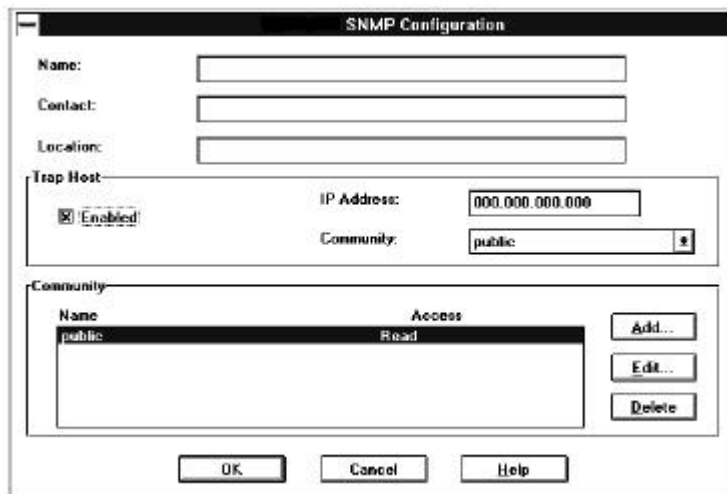
What is SNMP?

---

SNMP Agents can also send out unsolicited messages, called traps.

### Configuration Steps

1. Open the required configuration file.
2. From the Server section of the **Configuration File** window, click the **Edit** button.
3. On the **Edit Server Options** dialog box, click the **SNMP** button.
4. The **SNMP Configuration** dialog box appears.



The image shows the 'SNMP Configuration' dialog box. It has a title bar with the text 'SNMP Configuration'. Below the title bar are three text input fields labeled 'Name:', 'Contact:', and 'Location:'. Below these is a 'Trap Host' section containing a checked checkbox labeled 'Enabled', an 'IP Address:' field with the value '000.000.000.000', and a 'Community:' field with the value 'public'. Below the 'Trap Host' section is a 'Community' section with a table. The table has two columns: 'Name' and 'Access'. The first row contains 'public' and 'Read'. To the right of the table are three buttons: 'Add...', 'Edit...', and 'Delete'. At the bottom of the dialog box are three buttons: 'OK', 'Cancel', and 'Help'.

### Administrative Information

The following is used by the network administration to manage the RAS.

1. In the **Name** field, enter an **SNMP name** for the server. This name is not related to the device name assigned in the RAS configuration page.
2. Enter the name of the person responsible for managing the RAS in the **Contact** field.

3. In the **Location** field, enter a description of the physical location of the RAS.

*Note:* You can enter a maximum of 255 characters in the **Contact**, **Name**, and **Location** fields.

## Trap Hosts

A trap host is an IP workstation which is set up to receive SNMP trap messages. When the SNMP Agent detects a serious condition or activity, it will send a “trap” to a specified host, known as the trap host. The trap host must be a member of a community which is known to the SNMP Agent.

The RAS sends trap messages when the unit restarts and when it detects an invalid logon attempt.

### Configuration

1. To enable the trap host, click on the **Trap Host** check box.
2. In the **IP address** field, enter the **IP address** of the trap host.
3. In the **Community** field, select a community from the pull-down menu. The trap host is now set.

## Communities and Community Tables

Not everyone on the network can access the information controlled by an SNMP Agent. Access on the RAS is restricted through the use of communities and community tables.

A community is a group of users having a defined Name and a defined Access level.

The RAS supports up to five SNMP communities. The default community is “public”.

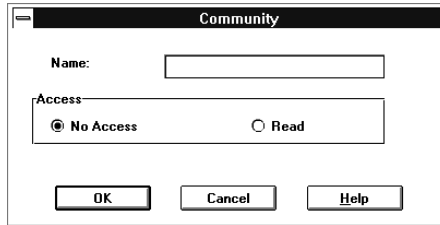
Community tables act like passwords by controlling access to the database. They list all SNMP communities and their corresponding access levels.

When the SNMP Agent receives a request for information, it will look for the name of the requestor in the community table. If the name cannot be found, then the request is denied and an error is returned to the user. If the name is found, the SNMP Agent then checks the community’s access level. If the access level of the community is equivalent or greater to the access level of the request, then the request is accepted.

Communities can be added, deleted or edited by users having proper access privileges.

## Adding Communities

1. In the Community Table area of the SNMP Configuration screen, click on **Add**. The **Community dialog box** appears:



The image shows a dialog box titled "Community". It has a "Name:" label followed by a text input field. Below that is an "Access:" label followed by a container with two radio buttons: "No Access" (which is selected) and "Read". At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

2. In the **Name** field, enter the SNMP community name.
3. Click on the appropriate access level check box.
4. Click **OK** to add the new SNMP community to the community table.

## Editing Communities

1. Select the community name to be edited, and click on **Edit**.
2. In the **Community** dialog box, change the **Name** field and set the access level as necessary.
3. Click **OK**.

## Deleting Communities

1. In the Community Table area of the SNMP Configuration screen, select the community you wish to delete.
2. Click on **Delete**.

**Note:** You cannot delete the “public” SNMP community. However, its access level can be changed.

## Viewing Statistics

To view statistics on an attached RAS, choose **Get Statistics** from the **Statistics** menu. The manager will get the statistics data from the server and display it in the **System Statistics** window. The data is described below:

**System Statistics**

Server

Name:	NCG 8e	Firmware Version:	3.90
Time:	Thursday Apr 10 1997 13:35:06	Received:	9572890
Up Time:	6 days 02 hrs 57 mins	Transmitted:	2645415
		Overruns:	1335

Port Status:	Bytes		Frames/Sec:	CRC Errors:	Overruns:	Utilization:
	Received:	Transmitted:				
1:Idle	0	0	0	0	0	0%
2:Idle	8468	364318	0	0	0	0%
3:Idle	77675	74049	0	0	0	0%
4:Idle	0	0	0	0	0	0%
5:Idle	0	671850	0	0	0	0%
6:Idle	0	0	0	0	0	0%
7:Idle	0	0	0	0	0	0%
8:Idle	0	644928	0	0	0	0%

Port 1

User/Department:	Baud Rate: 38400	Enabled: Dial In
------------------	------------------	------------------

Addresses : Port 1	Modem Type:
MAC:	Direct
IP:	

### Server Name

The identifying name given to this server.

### Time

The date and time that the statistics were recorded.

### Up Time

The amount of time since this server's last reset.

### Firmware Version

The firmware revision level of the attached RAS.

### Received

The total number of frames bridged from LAN to the modem ports.

### Transmitted

The total number of frames bridged from the modem ports to the LAN.

### Overruns

The number of times that heavy traffic caused the buffers to be filled to the point of overflow on the LAN interface.

### LAN Connection

The type of network connection. If the server has been configured to auto-detect the network type (the default), this field displays Auto (click on the **LAN** button for this information).

### Server MAC Address

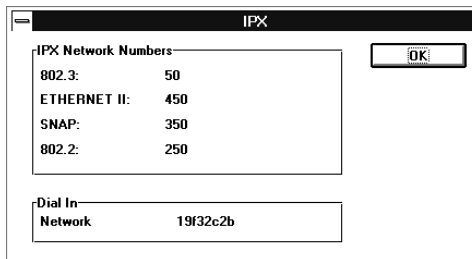
The main MAC address of the server itself. (Click on the **LAN** button for this information.)

### IP Address

The main IP address of the server itself. (Click on the **IP** button for this information.)

### IPX Network Numbers

The IPX network numbers for enabled frame types and the Dial-In network (click on the **IPX** button for this information). The following window appears.





**IPX Network Numbers**

The IPX network numbers assigned to the enabled frame types.

**Dial In**

The IPX network number assigned to the dial-in connections.

**Information Presented for Ports****Status**

The operating status of the indicated port. One of the following will be displayed:

- Idle
- Dial-In
- Dial-Out

**Bytes Received**

The total number of bytes received on the selected port.

**Bytes Transmitted**

The total number of bytes transmitted on the selected port.

**Frames/Sec.**

The number of frames per second passing through this port.

**CRC Errors**

The number of PPP Cyclic Redundancy Check errors that were received on this port.

**Overruns**

The number of times the buffers on this port overflowed.

**Utilization**

The percentage of the bandwidth of this port that is currently being used.

### **User/Department**

The User ID and department name (if any) of the user currently using this port. If the port is currently unused, this field is blank.

### **Baud Rate**

The rate at which the user is communicating.

### **Enabled**

Indicates what is currently enabled on the port. One of the following will be displayed:

- None
- Dial In
- Dial Out
- Dial-In/Dial-Out

### **Port MAC Address**

The MAC address defined for this port. If a fixed address user is connected, the MAC address assigned to this user is displayed. This information appears at the bottom of the screen.

### **Port IP Address**

The IP address of this port, if one has been assigned. If client-specified IP addresses have been enabled, the IP address of a Windows user choosing this option will be displayed. This information appears at the bottom of the screen.

## Event Log

The RAS records many of the events and activities that can be performed on the server by the manager during configuration as well as events from normal dial-in and dial-out use. This event log can be used to monitor the RAS for proper usage and for tracking some kinds of problems.

The type of events captured by the server are:

- User account usage and security (log on, log out, and failed log on activities)
- Configuration changes (through the manager and front panel)
- System Restarts
- Errors (internal RAS errors)

To access the Event Log, the Black Box Manager PC must connect to a RAS. The following operations are supported and are accessed through the Managers's Event Log menu.

### Get Event Log

This will get the event log file from the connected RAS and display the data in a scrollable Window. The columns in the table are date, time, event and user name if applicable.

### Change Log Filter

The type of events recorded by the RAS can be controlled. The Change Log Filter lets the user select any of the event types listed above. Only those events will be recorded.

### Clear Event Log

This will clear all the data from the connected server's log file.

## Software Upgrades

Firmware is the basic operating code of aRAS. When new versions of firmware become available, they can be conveniently downloaded to your RAS.

**Note:** Be sure all users are disconnected before performing a download. Any existing user sessions will be abruptly terminated when the RAS is reset.

To download firmware, follow the steps below.

1. Make sure the RAS is properly connected to the PC running Black Box Manager.
2. From the **Configure** menu, select **Download Firmware**.
3. Select the appropriate file to download from the file list and click **OK**.
4. A confirmation dialog box will appear stating the version of the firmware file you have selected. Click **OK** to begin downloading the file.
5. After the download has completed, the RAS will reset and disconnect the Manager program.
6. Wait at least 5 minutes before attempting to connect to the server again.

---

# Chapter 10: Security

This chapter explains the access security features supported by the RAS and provides the configuration instructions.

In this chapter you will read about:

- Security Overview
- Supported Security Features
- Security Configuration
- Front Panel Lock

## Overview

The RAS has a multiple-level security system that controls access both to the server itself and to the network.

### Server Access

The RAS has two methods to control access to the server's internal configuration settings.

#### Administrative Privileges

The RAS will only accept a connection from the Black Box Manager program if the user has been configured with administrative privileges. The user record for this administrator must be stored as part of the RAS configuration file and have a valid password.

Regardless of the authentication method used, you will always require a record in your **User List** for the user with administrative privileges.

#### Front Panel Password

A password can be assigned to the RAS's Front Panel keypad and LCD display. This password would lock out unwanted users from the front panel so that they could not change the server's settings.

## Network Access

Network Access is controlled by selecting a password authentication security service for the RAS. The RAS supports password authentication plus some third party services. Only one of these services can be active at one time. The services are:

### User List

Passwords will be authenticated by using the RAS's user record database called the **User List**. The name and password entered by a dial-in user are verified against the **User List** before access to the LAN is granted. see "Configuring a User Record" on page 71 for instructions on how to create the **User List**.

If a third party security service is selected, the **User List** can still be used to set up specific user privileges on the RAS (i.e. Call back options, MAC address, Connection times etc.).

The passwords are authenticated using the Password Authentication Protocol (PAP) or the Challenge-Handshake Authentication Protocol (CHAP).

You must select either PAP or CHAP, or both.

### Netware

Netware Bindery or Netware Directory Services (NDS) contain a user profile database that is stored on a Netware server. The RAS will ask the Netware server to authenticate the password against the database before allowing the user access to the LAN. The RAS **User List** will not be used for password authentication. However, they can be used for setting user privileges.

The Netware authentication works by sending a request to a specific Netware server.

In an NDS environment, a particular server is normally used to house the user database. The address should be provided and the server will respond appropriately to security requests.

### RADIUS

Remote Authentication Dial In Users Services (RADIUS) is an open standard network security server. User records are created on the RADIUS Server. The RAS will ask the RADIUS server for authorization before allowing a dial-in user access to the LAN. Call back phone number, activity time-out and connect time-out can also be stored in the RADIUS user record. The RAS will obtain these values from the RADIUS server after password authentication and use them for processing the dial-in connection. The RAS User List will not be used for password authentication. However, they can be used for setting user privileges not supported in the RADIUS Server.

## External Hardware

Passwords will be authenticated by an external security device that is physically connected between a RAS serial port and its modem. These devices send login requests to the dial-in clients. The clients must support a TTY or terminal mode to complete the login process. The **RAS User List** base will not be used for password authentication.

This option can also be used if you want to have no authentication. Use with caution.

## Axent

Axent (formerly AssureNet) is a software-based security server that provides user authentication using their SecureNet Key cards. The RAS will ask the Axent server to start the authentication process. The Axent server will then prompt the dial-in user for their name and a security token from the key card. The dial-in client software must support a TTY or terminal mode to display the Axent prompts.

## SecurID

This feature enable customers with a SecurID ACE Security Server to make use of this server for dial-in user authentication. Once a client dials into the RAS and a modem connection is established, the RAS will ask the SecurID server to start the authentication process. The SecurID server will then prompt the dial-in user for their name and the Passcode according to the SecurID token instructions. The dial-in client software must support a TTY or terminal mode to display the SecurID prompts.

## NT Domain

NT Domain enables the RAS to use a Windows NT's domain user database for dial-in user authentication. The Black Box server will collect the userid and password from the dial-in client and will forward an authorization request to the Primary Domain Controller (PDC). This feature will work with the Perle Remote Client as well as other PPP clients such as Windows 95 and NT. The clients must support the Password Authentication Protocol (PAP).

## PAP and CHAP

The Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP) are the security features of the PPP protocol. These protocols provide the means to authenticate a user name and password. The **User List** service and some of the third party services require that the dial-in client software support PAP or CHAP.

CHAP provides a higher level of security and should be used when possible. PAP can be selected at the same time to accommodate Dial-in clients who do not support CHAP.

## Call Back

The Call back feature of the RAS can provide an additional level of security. When a remote user calls in to a RAS and Call Back has been set up, the RAS will disconnect and then call the user back according to the RAS's configuration for the user. The RAS can be requested to dial back on one of five configured phone numbers it stores. Since the actual phone number is never transmitted on the serial line, an unauthorized user cannot attach to the RAS.

See “Call Back Options” on page 75 for configuration steps.

## Generic User

The Generic User is a local user record that determines a user's privileges on the RAS when the user's name is not found in the **User List**. It is used only if security has not been configured for **User List** password authentication. Dial-in clients must support PAP or CHAP to be able to use the Generic User record.



## Security Services Configuration

The configuration steps to setup the security features of the RAS are described in the following sections.

### Administrative Privileges

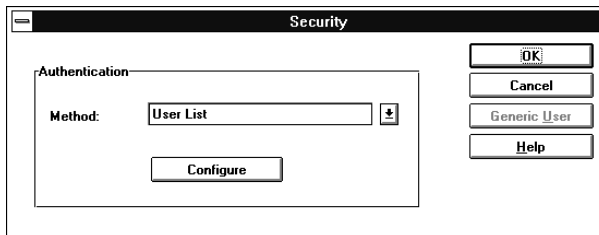
To create a user record with administrative privileges, See “Configuring a User Record” on page 71.

**Note:**  A new RAS has a default user record with the name: **superusr** - no password.  
This user name has administrative privileges.

### Network Access

To configure network access security, a password authentication service must be selected for the RAS, and then the parameters for the service are configured. If supported, a Generic User can also be configured. The steps are:

1. From the Server section of the **Configuration File** window, click the **Edit** button.
2. On the **Edit Server Option** dialog box, click the **Security** button. The **Security** dialog box appears.

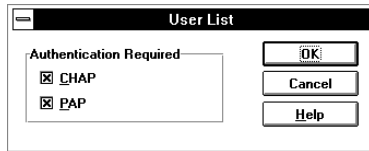


3. From the **Authentication Method** drop down list, select the required security service.
4. Click on the **Configure** button if the service has any parameters to set. See the sections below for instructions on the selected service.
5. Click the **Generic User** button (if enabled) to change any parameters. See “Generic User” on page 118 for instructions.
6. Click **OK** to save the security configuration.

## User List

To configure the **User List** security service:

1. From the **Security** dialog box, select **User List** from the **Authentication Method** drop down list.
2. Click on the **Configure** button. The **User List** dialog box appears.



3. Click on the check boxes for the Authentication protocol supported by the dial-in clients. Select **PAP** or **CHAP** or both.

If both are checked, the server will first attempt to authenticate using CHAP. If this is not supported by the client, it will then use PAP.

4. Click **OK**.
5. Create user records for all dial-in users. See “Configuring a User Record” on page 71.

## Netware

The Netware security service uses the PAP security protocol. The Dial-in client must support PAP. Authentication is always done using the Netware server configured below.

ARA clients are not supported in this mode.

If you want to use any of the following user-based features, you will need to define a user record in the User List for each user or define the generic user record which applies to all users who do not have their own specific record.

- Activity Timeout
- Connect Time
- Callback
- Preferred Modem Pool

To configure the Netware security service:

1. From the **Security** dialog box, select **Netware** from the **Authentication Method** drop down list.
2. Click on the **Configure** button. The **Netware** dialog box appears.

3. Enter the following parameters:

#### **Server Name**

The name of the Netware server the database resides on.

#### **Netware Group Name**

The name of the group on the Netware server that the authorized users belong to. This is an optional field.

The group name provides added access control. All network users will have a user record in the database. However, by specifying a group, only the users in the group will have dial-in access to the network.

4. Click **OK**.
5. Create user records for all dial-in users on the Netware server.

## **RADIUS**

If you want to use any of the following user-based features, you will need to define a user record in the User List for each user or define the generic user record which applies to all users who do not have their own specific record.

- Activity Timeout
- Connect Time
- Callback
- Preferred Modem Pool

With RADIUS authentication you may also setup the following parameters in your RADIUS User Records.

- Callback number
- User IP address
- Activity timeout
- Connect time

### Callback number

If a user has a record in the **User List**, the callback information will be taken from there. Otherwise, the callback enabling will be taken from the **Generic User Record** and the number will come from the RADIUS User Record.

### User IP Address

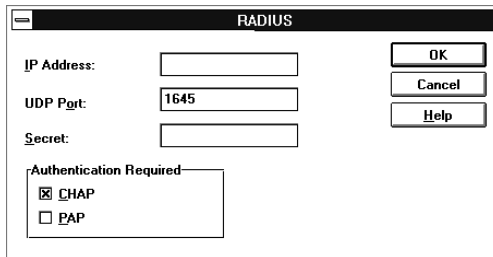
If an IP address is specified in the RADIUS User Record, this address will be passed to an IP client dialing in. If an IP address is not specified, the RAS will resolve the IP address in the usual manner.

### Connect Timeout / Activity Timeout

The RAS will use these values if they are specified in the RADIUS file. Otherwise, it will use either the generic user record or the specific record, if it exists.

To configure the RADIUS security service:

1. From the **Security** dialog box, select **RADIUS** from the **Authentication Method** drop down list.
2. Click on **Configure**. The **RADIUS** dialog box appears.



The image shows a dialog box titled "RADIUS". It contains the following fields and controls:

- IP Address:** A text input field.
- UDP Port:** A text input field containing the value "1645".
- Secret:** A text input field.
- Authentication Required:** A section containing two checkboxes:
  - CHAP
  - PAP
- Buttons:** Three buttons are located on the right side: "OK", "Cancel", and "Help".

3. Enter the following parameters:

**IP Address**

The IP address of the RADIUS server.

**UDP Port**

The UDP port that the RADIUS server uses to communicate. The default is 1645.

**Secret**

The secret key that is shared between the RAS and the RADIUS server to encrypt the data. This key must match the one configured on the RADIUS server.

**Authentication**

The passwords are authenticated using (PAP) or (CHAP). You must select either PAP or CHAP, or both. The dial-in clients for all users must support either PAP or CHAP. If both are checked the server will attempt to authenticate over CHAP first.

4. Click **OK**.
5. Create user records for all dial-in users on the RADIUS server.

**Note:** If call back is configured in the user records on the RADIUS server, the Generic User record on the RAS must have the Call Back option set to Allowed or Required.

## External Hardware

To configure the External Hardware security service:

1. From the **Security** dialog box, select **External Hardware** from the **Authentication Method** drop down list.
2. There are no configuration parameter for this service.
3. Click **OK**.
4. Set up the External security device.

**Note:** The external hardware option should be used with caution because it relies totally on the external hardware for security. There is no internal security in the RAS with this option.

## Axent

If you want to use any of the following user-based features, you will need to define a user record in the **User List** for each user or define the generic user record which applies to all users who do not have their own specific record.

- Activity Timeout
- Connect Time
- Callback
- Preferred Modem Pool

If you are connecting using an ARA connection, you may want to contact Axent to obtain a drop-in module that will allow ARA clients to connect in this environment.

To configure the Axent security service:

1. From the **Security** dialog box, select **Axent** from the **Authentication Method** drop down list.
2. Click on **Configure** button. The **Axent** dialog box appears.

The screenshot shows the Axent configuration dialog box. It features a title bar with the text "Axent". Below the title bar, there are several sections of controls:

- Protocol:** Two radio buttons are present: "ICP/IP" (unselected) and "IPX/SPX" (selected).
- Agent Key:** A text input field containing a series of asterisks.
- Confirm Agent Key:** A text input field containing a series of asterisks.
- Agent ID:** A text input field containing the text "PERLE".
- Primary Server Address:** A section containing three text input fields: "Network", "Node", and "Socket". The "Socket" field contains the value "4545".
- Backup Server Address:** A section containing three text input fields: "Network", "Node", and "Socket". The "Socket" field contains the value "4545".

On the right side of the dialog, there are three buttons: "OK", "Cancel", and "Help".

3. Enter the following parameters:

### Protocol

Select the network protocol which will be used to communicate with the Axent server. The choices are IPX/SXP and TCP/IP. The protocol chosen will change the Primary and Backup Server Address fields described below.

**Agent Key**

Enter the Agent Key for the RAS. This is a 1 to 16-digit hexadecimal number and must match the value that is configured on the Axent server. The Key is used to authenticate the RAS as a valid Axent agent.

**Confirm Agent Key**

Re-enter the Agent Key value in this field for confirmation

**Agent ID**

Enter the Agent ID for the RAS. This field can be from 1 to 16 alphanumeric characters and must match the ID configured on the Axent server. This ID is used to authenticate the RAS as a valid Axent agent.

**Primary Server Address**

Configure the address for the Primary Axent server by entering values for the following fields. Note that the fields shown depend on the network protocol chosen.

For the IPX/SXP protocol, the fields are:

**Network**

The Network number is an 8-digit hexadecimal number of the network to which the Axent Server is connected.

**Node**

The network node of the Axent Server. This is a 12-character hexadecimal number for the network node to which the device is connected.

**Socket**

The socket number for the Axent Security Service. This is a 4-character hexadecimal number. The default is 4545.

For the TCP/IP protocol the fields are:

**IP Address**

The IP address of the Axent server.

**TCP Port**

The TCP port number of the Axent Security Service. This is a 4-character decimal number. The default is 2626.

### Backup Server Address

If you have a backup Axent server connected to your network then configure its address using these fields.

4. Click **OK**.
5. Create user records for all dial-in users on the Axent Defender security server.

## SecurID

SecurID enables the RAS to use the ACE/Server from Security Dynamics for user authentication. The ACE/Server is a software based security server that provides user authentication using a memorized personal identification number (PIN) and a code generated by the SecurID token. The RAS will ask the ACE/Server to start the authentication process. The dial-in user will then be prompted to enter their name and the PASSCODE according to the SecurID token instructions. The dial-in client software must support a TTY or terminal mode to display the SecurID prompts.

If you want to use any of the following user-based features, you will need to define a user record in the **User List** for each user or define the generic user record which applies to all users who do not have their own specific record.

- Activity Timeout
- Connect Time
- Callback
- Preferred Modem Pool

To configure the SecurID Security feature:

1. From the **Security** dialog box, select **SecurID** from the **Authentication Method** drop down list.



- Click on **Configure** button. The **SecurID** dialog box appears.

The SecurID dialog box contains the following elements:

- Master IP Address:** An empty text input field.
- Slave IP Address:** An empty text input field.
- Master UDP Port:** A text input field containing the value "5500".
- Slave UDP Port:** A text input field containing the value "5500".
- Buttons:** "OK", "Cancel", and "Help" buttons are positioned to the right of the input fields.
- Encryption Type:** A section with two radio buttons: "DES" (unselected) and "SDI" (selected).
- Client/Server Protocol:** A section with a checked checkbox labeled "Version 2.3 Enhancement".
- Reset Node Secret:** An unchecked checkbox at the bottom of the dialog.

- Enter values for the following parameters:

#### Master IP Address

The IP address of the Master SecurID server.

#### Slave IP Address

The IP address of the Slave SecurID server.

#### Master UDP Port

The UDP port number of the SecurID service on the Master server. This is a 4 character decimal number. The default is 5500

#### Slave UDP Port

The UDP port number of the SecurID service on the Slave server. This is a 4 character decimal number. The default is 5500

#### Encryption Type

Click the type of data encryption to be used when communicating with the SecurID server. The choices are **DES** or **SDI**.

## Client/Server Protocol

### Version 2.3 Enhancement

Check this box to enable the RAS to use the security enhancements of the Client/Server communication protocol offered in version 2.3 of the ACE/Server software. This is the default setting.

If you are using an ACE/Server with version 2.2 software then remove the check from this box.

### Reset Node Secret

The Node Secret is a pseudorandom string that is sent to the RAS server by the SecurID server the first time the RAS sends an authorization request. The Node Secret is used to encrypt the data that is sent between the RAS and the SecurID server.

Do not check this box unless there is a mismatch between the node secret in the RAS and the SecurID server and you must reset the Node Secret to blank. This would occur if a RAS is moved to a different network with a new SecurID server.

**Note:** If the Node Secret is reset, or the Black Box server is reset to factory defaults, then the SecurID server must be configured to re-send the Node Secret to the RAS.

4. Click **OK**.

## NT Domain

NT Domain enables the RAS to use a Windows NT's domain user database for dial-in user authentication. The RAS server will collect the userid and password from the dial-in client and will forward an authorization request to the Primary Domain Controller (PDC). This feature will work with the Perle Remote Client as well as other PPP clients such as Windows 95 and NT. The clients must support the Password Authentication Protocol (PAP).

The RAS **User List** will not be used for password authentication.

Enter values for the following fields to configure the NT Domain security feature on the RAS server:

### Protocol

Select the network protocol which will be used to communicate with the PDC. The choices are IPX and IP.

### Default Domain Name

Identify the NT domain by entering the Domain Name. The Domain name can be up to 16 characters long.

### IP Address

If the network protocol used to communicate with the PDC is IP then enter the PDC's IP address. This value must be configured if the PDC is not on the same IP subnet as the RAS.

### Allow User Specified NT Domain

Click the check box to allow a dial-in user to specify a domain to which they belong. The RAS server will send the authorization request to this domain instead of the default domain. A user would enter their userid in the format "domain\userid".

## Generic User

When using a security system such as Axent or SecurID, you may want to provide additional RAS functionality even though the user has not been directly authenticated by the RAS. This can be done by setting up a generic user record which is used whenever a user connects.

To configure the Generic User parameters:

1. On the **Security** dialog box, click the **Generic User** button. This button is enabled only if the Authentication method currently selected supports the Generic User. The **Generic User** dialog box appears:

The screenshot shows a dialog box titled "Generic User". It is divided into four main sections:

- Activity Time Out:** Contains two radio buttons. The first is "Disabled" and is selected. The second is "If inactive" followed by a text input field and the word "minutes".
- Roaming Call Back:** Contains three radio buttons: "Disabled" (selected), "Allowed", and "Required".
- Connect Time:** Contains two radio buttons. The first is "Unlimited" and is selected. The second is "Maximum" followed by a text input field and the word "minutes".
- Preferred Modem Pool:** Contains a dropdown menu and a checkbox labeled "Use Exclusively".

On the right side of the dialog, there are three buttons: "OK", "Cancel", and "Help".

2. Enter the following parameters:

### Call Back

This feature will cause the server to disconnect users when they dial in and then call the users back at the telephone numbers they specified when they dialed in. The choices are:

- **Disabled** - Call back will not be used.
- **Allowed** - Call Back will be used if the user dialing in requests the feature.
- **Required** - Call back must be used. If the user dialing in does not request call back, the RAS will disconnect the user and not call back.

### Activity Time Out

Closes the connection with a user after a configurable time period with no user activity on the link.

### Connect Time

Shuts down the remote connection, regardless of activity, at the end of a configurable time period.

**Preferred Modem Pool**

If you want to assign generic users to a specific modem pool for Call Back, then make a selection in the **Preferred Modem Pool** drop down list.

**Note:** Dial-In Modem Pool must be configured before a selection can be made. See “Dial-In Modem Pools” on page 78 for configuration instructions.

If you click the **Use Exclusively** check box, the user will not be called back if a modem in the pool is not available.

If you do not check the **Use Exclusively** box, the user will be called back using another pool if no modems are available in the selected pool.

3. Click **OK**.

## Front Panel Lock

If you want to prevent tampering through the front panel, you can password protect it. To assign a password to lock the front panel, follow these steps.

1. Open the required configuration file for a RAS.
2. From the Server section of the **Configuration File** window, click on the **Edit** button.
3. On the **Edit Server Option** dialog box, click the **Enable Front Panel Password** check box.
4. Enter a password. The password can be up to 8 characters long using digits 0-9.
5. Re-enter the password in the **Confirm** field.
6. Click **OK**.
7. Download the configuration file to the RAS.

---

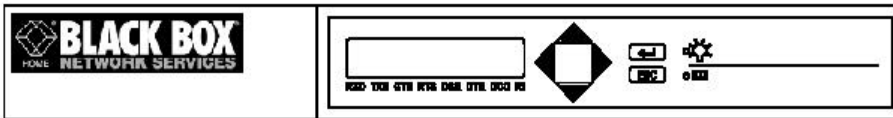
## Chapter 11: Front Panel

This chapter contains the following information about the RAS Front Panel:

- Front Panel Overview
- A list of navigational rules for movement through the front panel menus
- The front panel menu structure
- Each front panel screen

### Overview

The Front Panel of the RAS consists of a keypad and an LCD display. This front panel is common to all models of RAS and can be used for initial set up of the RAS and monitoring its status.



The front panel program has three main functions:

- Configuration (small subset of the Manager configuration features)
- Status (LAN connection, Port Connection, display of Manager configuration)
- Statistics (dynamic data such as traffic flow and utilization)

#### Front Panel Language

When the unit is first powered up the LCD display will cycle through the list of languages that it supports. Wait until the appropriate language is displayed and then press

## Navigational Rules

Use these keys to navigate through the front panel display.

1. Use the ↵ key to:
  - select a menu,
  - select a sub-menu, or
  - select an item for editing.
2. Use the **UP** and **DOWN** arrow keys to view selections within a menu.
3. Press the **ESC** key once to return to the previous screen.  
Press the **ESC** key several times to return to the RAS main screen.

## Editing Fields

Use these keys to edit a selected field and confirm changes.

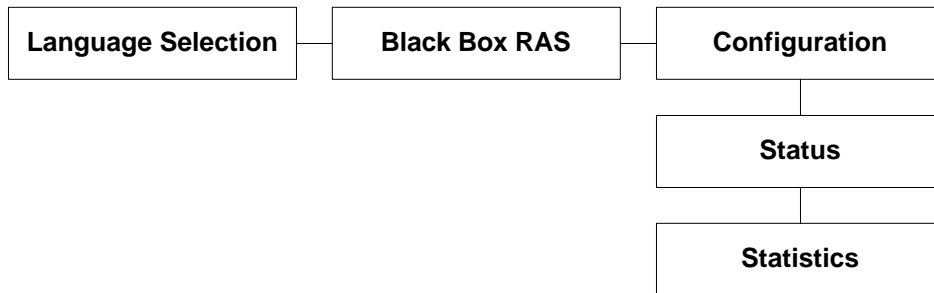
1. Use the **UP** and **DOWN** arrow keys to view selections or change a value.
2. Use the **LEFT** and **RIGHT** arrow keys to position the cursor on the correct editing position.
3. Press the ↵ key to accept changes.
4. Press **ESC** to cancel changes.



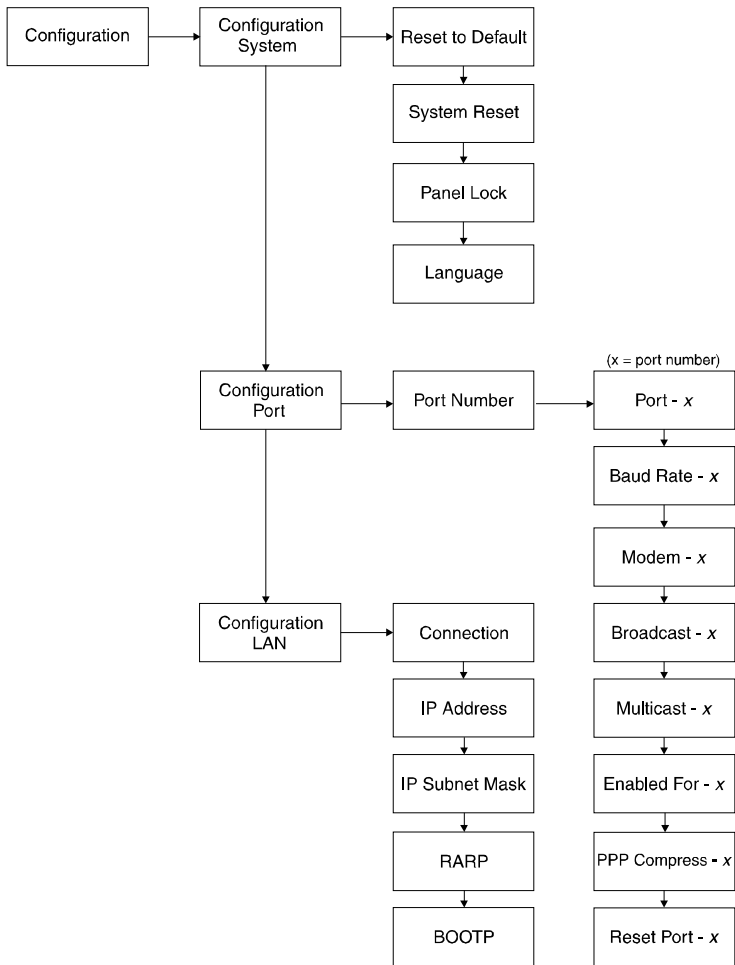
## Menu Structure

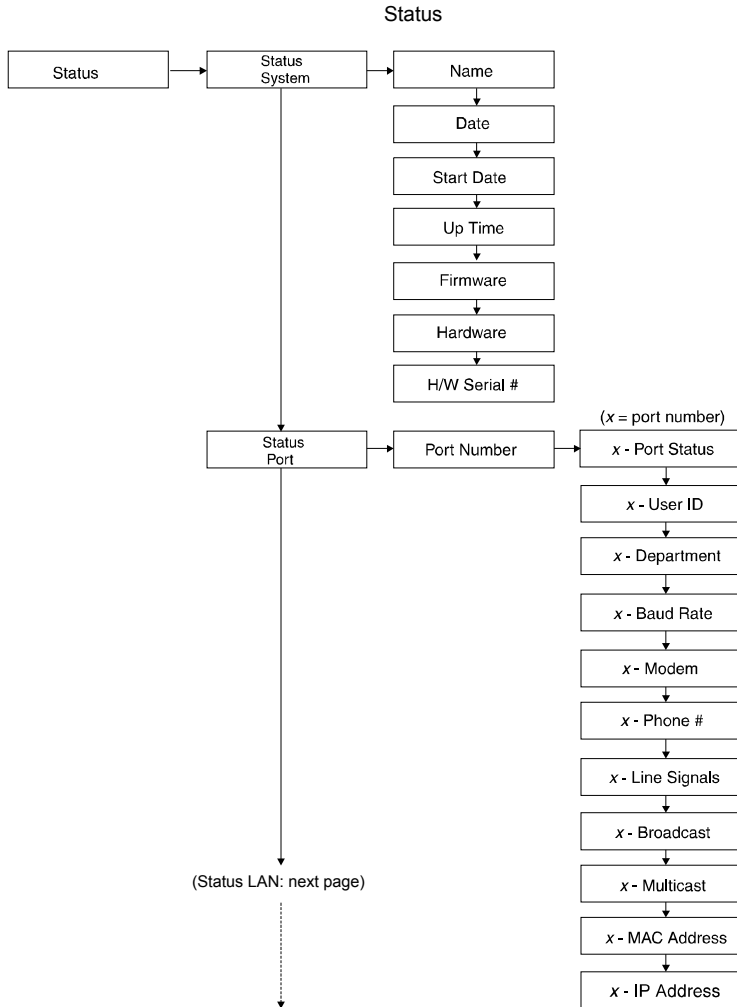
The following diagrams illustrate the flow of options that are available through the front panel LCD.

### Front Panel Main Screen

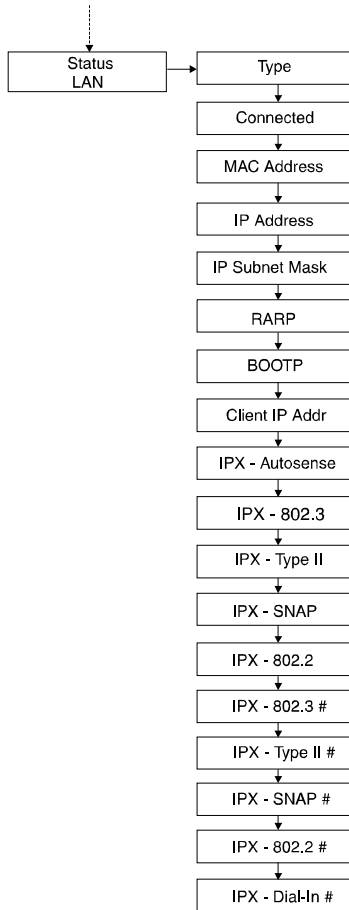


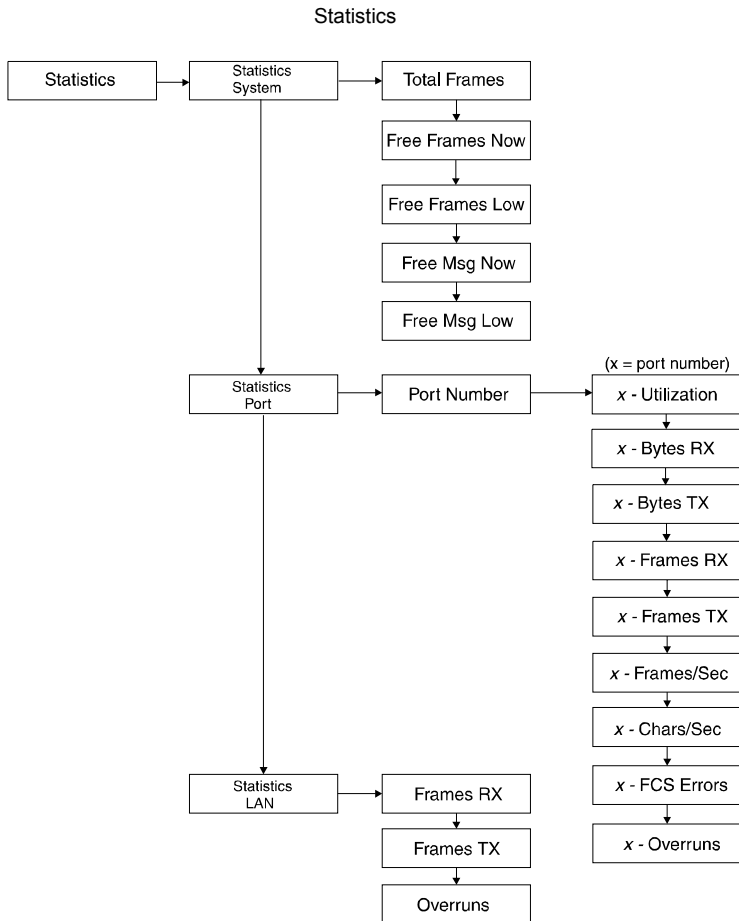
### Configuration





Status Cont.





## Menu Descriptions

<b>Menu Name</b>	<b>Description</b>
<b>RAS/<i>ne</i> or RAS/<i>nt</i></b>	<b>RAS front panel main menu</b> , where <i>n</i> is the number of ports, <i>e</i> is Ethernet, and <i>t</i> is Token-Ring.
Configuration	Sets values used by the server.
Status	Reflects the current values for the server.
Statistics	Supplies server, port and LAN data for diagnostics.
<b>Configuration System</b>	<b>Edits parameters that configure the server.</b>
Reset to Default	Resets the configuration of the server to factory defaults.
System Reset	Performs a system reset; required to implement changes to the server configuration.
Panel Lock	Prevents access by anyone to the front panel by locking it.
Language	Allows you to change the language used by the front panel display.
<b>Configuration Port</b>	<b>Set values for various parameters for each port on the RAS.</b>
Port Number	Chooses the port to which the port configuration will be applied.
Port - <i>x</i>	Enables or disables the port, where <i>x</i> is the port number.
Baud Rate - <i>x</i>	Sets the line speed for this port, where <i>x</i> is the port number.
Modem - <i>x</i>	Specifies the type of modem attached to the port. You can also choose <b>direct</b> for a Null Modem connection, where <i>x</i> is the port number.
Broadcast - <i>x</i>	Enables or disables network broadcasts from getting past the port to dial-in clients, where <i>x</i> is the port number.
Multicast - <i>x</i>	Enables or disables network multicasts from getting past the port to the dial-in clients, where <i>x</i> is the port number.

<b>Menu Name</b>	<b>Description</b>
Enabled For - <i>x</i>	Specifies the type of operation this port can be used for: Dial-In                      Dial Out Dial In/Dial Out   None. <i>x</i> is the port number.
PPP Compress - <i>x</i>	Specifies the type of PPP compression: Header & Addr Address Only Header Only None. <i>x</i> is the port number.
Reset Port - <i>x</i>	Resets the port to implement new settings, where <i>x</i> is the port number.
<b>Configuration LAN</b>	<b>To configure the LAN configuration area of Server configuration.</b>
Connection	Identifies the LAN port to which the LAN is attached.
IP Address	Allows the entry of the IP address for the server.
IP Subnet Mask	Allows the entry of the IP subnet mask.
RARP	Indicates whether RARP is enabled or disabled.
BOOTP	Indicates whether BOOTP is enabled or disabled.
<b>Status System</b>	<b>Gives the status of the settings used by the system.</b>
Name	Gives the name of the server.
Date	Indicates the current date in yyyy/mm/dd hh:mm format.
Start Date	Indicates the date of the last restart in yyyy/mm/dd hh:mm format.
Up Time	Indicates the amount of time since the last restart in dddd hh:mm format.
Firmware	Provides the firmware revision number.
Hardware	Provides the hardware version level.
H/W Serial #	Lists the 833 hardware serial number.

<b>Menu Name</b>	<b>Description</b>
<b>Status Port</b>	<b>Gives the status of the selected port.</b>
Port Number	Allows you to select the desired port.
<i>x</i> - Port Status	Indicates if a port is: Disabled: port is disabled. Idle: port is enabled but not currently being used. Dial-In: port is enabled as being used for dial-in. Dial-Out: port is enabled as being used for dial-out. <i>x</i> is the port number.
<i>x</i> - User ID	Indicates the ID of the connected user, where <i>x</i> is the port number.
<i>x</i> - Department	Gives the department name of the currently connected user, where <i>x</i> is the port number.
<i>x</i> - Baud Rate	Gives the port line speed, where <i>x</i> is the port number.
<i>x</i> - Modem	Lists the currently attached modem name, where <i>x</i> is the port number.
<i>x</i> - Phone #	Provides the call back phone number currently in use, where <i>x</i> is the port number.
<i>x</i> - Line Signals	Gives the port line signals, where <i>x</i> is the port number.
<i>x</i> - Broadcast	Indicates if network broadcasts are enabled or disabled through this port, where <i>x</i> is the port number.
<i>x</i> - Multicast	Indicates if network multicasts are enabled or disabled through this port, where <i>x</i> is the port number.
<i>x</i> - MAC Address	Gives the currently used MAC address for this port, where <i>x</i> is the port number.
<i>x</i> - IP Address	Provides the currently used IP address for this port, where <i>x</i> is the port number.
<b>Status LAN</b>	<b>Provides LAN related status information.</b>
Type	Gives the physical connection type.
Connected	Indicates if the 833 is currently connected to the LAN.
MAC Address	Gives the 833 MAC address.



<b>Menu Name</b>	<b>Description</b>
IP Address	Gives the 833 IP address.
IP Subnet Mask	Gives the 833 IP Subnet Mask.
RARP	Indicates if RARP is enabled or disabled.
BOOTP	Indicates if BOOTP is enabled or disabled.
Client IP Addr	Indicates that dial-in clients are permitted to supply an IP address.
IPX - Autosense	Indicates if IPX autosense is enabled or disabled.
IPX - 802.3	Indicates if the IPX - 802.3 is enabled or disabled.
IPX - Type II	Indicates if the IPX - Type II is enabled or disabled.
IPX - SNAP	Indicates if the IPX - SNAP is enabled or disabled.
IPX - 802.2	Indicates if the IPX - 802.2 is enabled or disabled.
IPX - 802.3 #	Gives the IPX - 802.3 network number (if applicable).
IPX - Type II #	Gives the IPX - Type II network number.
IPX - SNAP #	Gives the IPX - SNAP network number.
IPX - 802.2 #	Gives the 802.2 network number.
IPX - Dial-In #	Gives the IPX dial-in network number.
<b>Statistics System</b>	<b>Provides statistics of the system.</b>
Total Frames	Total frames transmitted and received.
Free Frames Now	Current number of internal free frame buffers.
Free Frames Low	Lowest attained internal free frame buffers.
Free Msg Now	Current number of free message buffers.
Free Msg Low	Lowest number of free message buffers.
<b>Statistics Port</b>	<b>Gives statistics of the selected port.</b>
Port Number	Allows you to select the desired port.

<b>Menu Name</b>	<b>Description</b>
<i>x</i> - Utilization	Gives the line utilization over the last second. <i>x</i> is the port number.
<i>x</i> - Bytes RX	Total bytes received for this port. <i>x</i> is the port number.
<i>x</i> - Bytes TX	Total bytes transmitted for this port. <i>x</i> is the port number.
<i>x</i> - Frames RX	LAN frames received intended for this port. <i>x</i> is the port number.
<i>x</i> - Frames TX	LAN frames transmitted from this port. <i>x</i> is the port number.
<i>x</i> - Frames/Sec	Average frames per second over the last second. <i>x</i> is the port number.
<i>x</i> - Chars/Sec	Average characters per second over the last second. <i>x</i> is the port number.
<i>x</i> - FCS errors	Number of Frame Check Sequence errors. <i>x</i> is the port number.
<i>x</i> - Overruns	Number of frames re-sent due to buffer overruns.
<b>Statistics LAN</b>	<b>Provides statistics for the LAN.</b>
Frames RX	Total LAN frames received.
Frames TX	Total LAN frames transmitted.
Overruns	Frames re-sent due to buffer overruns.

---

## Chapter 12: Custom Server Configuration

This chapter describes some of the configurations that may be required in some environments.

In this chapter you will read about:

- Custom Modem Configurations
- Changing Link Control Parameters
- Changing the Async Control Map

### Creating a Custom Modem Configuration

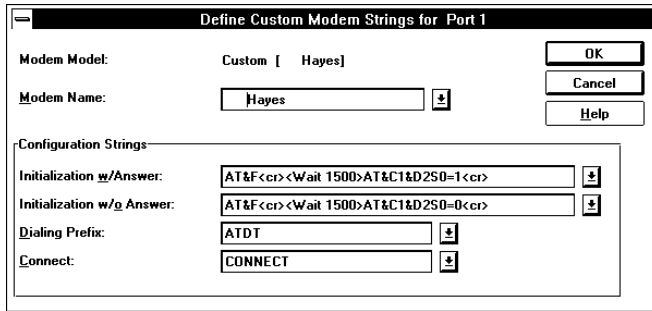
If your particular modem does not appear on the provided modem list, or if you wish to take advantage of some special features of your modem, you can create a custom modem configuration.

1. Open the required configuration file.
2. From the Port section of the **Configuration File** window, select the port to which the modem will be attached and click the **Edit** button.
3. On the **Edit Port** dialog box, click on the **Modem Model** pull down list and select a modem similar to the one you want to create. All custom modem configurations are based on existing configurations.

*Suggestion:* The **Hayes** option is often a good place to start.

4. Click the **Custom Modem...** button. The **Define Custom Modem Strings** dialog box appears.
5. Modify the **Modem Name** field to identify your custom modem.
6. Type in the proper initialization strings (refer to your modem documentation.) Change any other necessary parameters, and click **OK**.

- The custom modem configuration is complete.



## Modem String Commands

The RAS can process commands within any modem string. Each command must be enclosed in angle brackets “<>”. If an angle bracket is required in the string, it is doubled (*i.e.*, “abc<<def>>ghi” would be interpreted as “abc<def>ghi”).

### Commands

All of these commands are optional with one exception. All initialization strings must end with <CR>. Most modems require a carriage return to execute the initialization string.

<NUL>

This command causes a NUL character (0x00) to be sent to the modem.

<CR>

This command causes a carriage return (0x0d) to be sent to the modem.

<^x>

This command causes a control character to be sent to the modem, where **x** is the control character. Note that <^@> is illegal; use <NUL> instead.

<0xhh>

This command causes a hexadecimal character to be sent to the modem, where **hh** is the hexadecimal character. Note that <0x00> is illegal, use <NUL> instead.

## Changing Link Control Protocol Parameters

The Link Control Protocol (LCP) is used to set up the serial link for transferring Point-to-Point Protocol (PPP) frames. IP and IPX traffic is encapsulated within the PPP frames.

You should not be changing these parameters under normal conditions. If you are familiar with PPP and specifically these LCP parameters, then these values can be adjusted to compensate for specific network characteristics.

Follow these steps below to change the Link Control Protocol parameters.

1. Open the required configuration file.
2. From the Port section of the **Configuration File** window, select the appropriate port and click the **Edit** button.
3. On the **Edit Port** dialog box, click the **Link Control Protocol** button. The **Link Control Protocol** dialog box appears.

The screenshot shows the 'Link Control Protocol for Port 1' dialog box. It is divided into several sections:

- Timeouts (Seconds):**
  - Restart: 6
  - Listen Inactivity: 60
  - Call Back Retry: 90
- Compression:**
  - Protocol
  - Address
- Buttons:** OK, Cancel, Help
- Use Magic Number:**
- Challenge Handshake (CHAP):**
  - Maximum Interval: 300 Seconds
  - Minimum Interval: 120 Seconds
  - Retry Timeout: 3 Seconds
  - Retry Count: 10
- Maximum Counts:**
  - Call Back Attempts: 3
  - Terminate Attempts: 3
  - Configuration Attempts: 10
  - NAK Count: 10

4. Change the following parameters as required.

### Timeouts

#### Restart

This field specifies the number of seconds a receiver of a PPP terminate request will wait after receiving the message before disconnecting. This ensures the proper transmission of all messages.

### Listen Inactivity

The specifies the number of seconds of inactivity on the link before PPP will send messages to ensure that the link is still active.

### Call Back Retry

The amount of time to wait between call back retries.

### Use Magic Number

In a PPP environment it is possible to confuse echoed messages as replies from a Peer. The use of magic numbers ensures that this cannot happen by having each side generate a unique number and comparing it to the PPP partner's number.

### Challenge Handshake (CHAP)

#### Maximum Interval

This is the maximum amount of time that PPP will wait before sending out a CHAP challenge.

#### Minimum Interval

This is the minimum amount of time the PPP will wait before sending out a CHAP challenge.

#### Retry Timeout

This is how long CHAP will wait for a response before retrying.

#### Retry Count

This is how many times CHAP will retry before disconnecting the client.

### Compression

PPP can compress data at the Protocol or Address level or both.

### Maximum Counts

#### Call Back Attempts

This is the maximum number of times the server will attempt to call back a user.

#### Terminate Attempts

The maximum number of times that PPP will attempt a "Terminates" request without success before dropping the line.

### Configuration Attempts

Configuration is the process by which server and client negotiate operating parameters. This is the maximum of configuration attempts without reply that the server will attempt before dropping the line.

### NAK Count

During negotiation either side can NAK a configuration message if the options are not acceptable. This number represents the maximum number of NAKs that will be accepted by the server before the line is dropped.

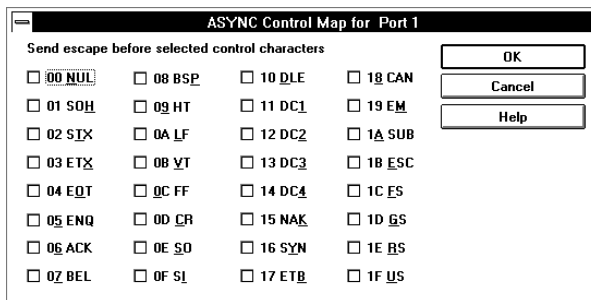
5. Click **OK**.

## Changing the Async Control Map

The Async Control Character Map is an advanced feature of Point-to-Point Protocol (PPP). This map lets you select all of the control characters that you require to be masked in order to have them passed through your network. Whenever a control character appears in the data stream, it is preceded by an escape sequence and changed into non-control characters. The destination end then converts them back to the original value. The two sides of the PPP link must agree on the Character Map.

Follow these steps to change the Async Control Map.

1. Open the required configuration file.
2. From the Port section of the **Configuration File** window, select the appropriate port and click the **Edit** button.
3. On the **Edit Port** dialog box, click the **Async Control Map...** button. The **Async Control Map** dialog box appears.



4. Click the check boxes of the control characters you want hidden.
5. Click **OK**.



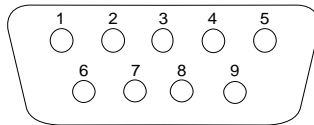
---

# Appendix A: Pinout and Cable Diagram

## Asynchronous Connector Pinout

### Pinout

The pins in the 9-pin D asynchronous connectors on the back panel of the RAS have the following assignments:



Pin	Circuit	Function
1	CD	Carrier Detect
2	RXD	Received Data
3	TXD	Transmitted Data
4	DTR	Data Terminal Ready
5	GND	Signal Ground
6	DSR	Data Set Ready
7	RTS	Ready To Send
8	CTS	Clear To Send
9	RI	Ring Indicator

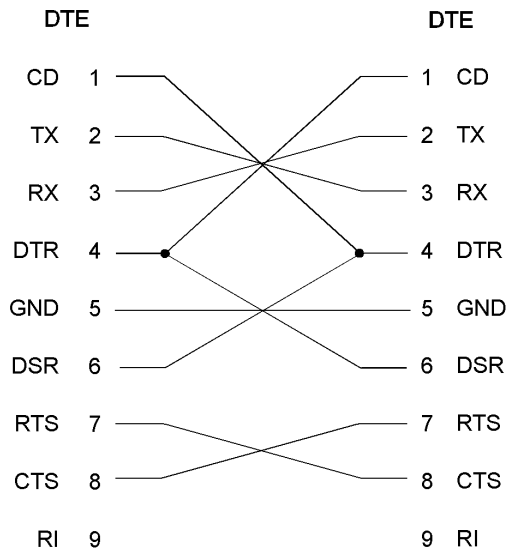
## Null modem cable

### Introduction

A PC can be directly connected to a RAS without using modems. This is called a direct connection. A special cable is provided with the RAS to do this and is called a null modem cable.

### Diagram

The diagram below shows how the null modem cable is constructed.



---

## Appendix B: Hardware Specifications

---

<b>Cabling</b>	<p>Token ring interface</p> <ul style="list-style-type: none"><li>• UTP, Type 3 (RJ-45)</li><li>• STP, Type 1 (DB-9)</li></ul> <p>Ethernet interface</p> <ul style="list-style-type: none"><li>• 10BaseT (RJ-45)</li><li>• Base2 (BNC)</li><li>• 10Base5 (AUI)</li></ul> <p>WAN Interface (2, 4 or 8 ports)</p> <ul style="list-style-type: none"><li>• Asynchronous EIA/TIA-232-E Serial Ports for up to 115 Kbps/port</li><li>• Male DB9 EIA/TIA-574 connectors: vertical spacing is 15.87 mm (0.625 in)</li><li>• Compatible with external ISDN terminal adapters</li></ul>
<b>Processor 32-bit RISC</b>	<ul style="list-style-type: none"><li>• AMD 29200 (2 and 4 port)</li><li>• AMD 29240 (8 port)</li></ul>
<b>Memory</b>	<ul style="list-style-type: none"><li>• 1 Mb Flash ROM</li><li>• 2 Mb RAM</li></ul>
<b>Front and Rear Panel Indicators</b>	<ul style="list-style-type: none"><li>• Power LED</li><li>• System operational LED</li><li>• LAN connect LED</li><li>• 2 x 16 LCD panel</li></ul>

---

<b>Operating Temperature</b>	<ul style="list-style-type: none"><li>• 0°-40° C (32°-104°F)</li></ul>
<b>Humidity</b>	<ul style="list-style-type: none"><li>• 0-90% non-condensing</li></ul>
<b>Operating Voltage</b>	<ul style="list-style-type: none"><li>• 90-230 VAC,(auto-sensing), 50-60 Hz</li><li>• 40 watts</li></ul>
<b>BTU Output</b>	<ul style="list-style-type: none"><li>• 400 BTU/hour max</li></ul>
<b>Approvals</b>	FCC Class A <ul style="list-style-type: none"><li>• TUV</li><li>• UL</li><li>• CSA</li><li>• DOC</li><li>• CE</li></ul>
<b>Dimensions</b>	<ul style="list-style-type: none"><li>• 50 mm x 432 mm x 250 mm</li><li>• 1.97 in.(H) x 17.0 in.(W) x 9.84 in(D)</li><li>• 6.8 kg / 3.1 lbs</li></ul>

---

---

# Glossary

## **activity log**

The activity log records each connection to the RAS with the time, user name, and type of activity. The network administrator can then view the server's use on the network.

## **address**

A number or string that specifies the destination for the data sent across the network.

## **Apple Remote Access Protocol (ARAP)**

Protocol allowing Macintoshes to communicate, either with another Macintosh or with an AppleTalk network over standard telephone lines.

## **AppleTalk**

A network system for Apple computers. An AppleTalk network system consists of devices that support AppleTalk protocols.

## **asynchronous**

When transmission of data communication is not synchronized by a clocking signal. Instead, start and stop bits are used.

## **AUI (Attachment Unit Interface)**

The type of connector used with thick (10Base-5) Ethernet cable.

## **baud rate**

The rate of the signaling speed of a transmission device, usually a modem.

## **bps (bits per second)**

The basic unit used to measure serial transmission capacity. How fast data is being sent.

## **BOOTP (BOOTstrap Protocol)**

A single BOOTP message specifies many of the items used at startup, including the IP address, the address of a gateway, and the address of a server.

**bridge**

A network device that connects two networks so that devices on one network can communicate with devices on the other network.

**broadcast**

A network transaction that sends data to all hosts connected to the network.

**call back**

A security feature where the RAS calls back the user at a predetermined number defined in the user's account.

**client**

A workstation that makes requests to servers.

**COM port**

A port on a communications device to which another device connects.

**configuration file**

The file that contains the configuration information for a RAS.

**data transfer speed**

The speed that data is transmitted across the network.

**dial-in**

The process of attaching to a local network from a remote client that is using dial-in software.

**dial-out**

The process of attaching to a remote server from a local device that is using dial-out software.

**Ethernet**

A high-speed (10Mbps) cable technology that connects devices into a local area network (LAN) using one or more sets of communication protocols.

**gateway**

A gateway has its own processor and memory and is used to connect two or more networks at the upper protocol layers of the OSI reference model. The networks can use different protocols and different physical media.

**initialization**

The process of bringing a hardware device or a software system to a known state.

**internet**

An interconnected group of networks.

**Internet Protocol (IP)**

A protocol that manages the routing of data packets between stations on the same or different networks.

**IP address**

A 32-bit address assigned to every host that wants to use IP to communicate across a network. The address consists of a network and host field.

**IPX (Internet Packet Exchange)**

A network transfer protocol from Novell, Inc.

**LAN (Local Area Network)**

A network system that does not use long-distance carriers. A LAN is usually limited by cable length restrictions.

**Logical Link Control (LLC)**

The IEEE 802.2 standard that corresponds to the ISO model's Data Link layer. LLC covers station-to-station connections, generation of message frames, and error control.

**modem**

Converts digital signals from a computer into analog signals that can then be transmitted over a telephone network.

**modem-pool**

A group of modems that can be used when paired together by a RAS. Perle manager software allows the administrator to group together modems so that if the first modem is unavailable, the call is passed over to another modem in the group.

**NASI (NetWare Asynchronous Services Interface)**

A Novell networking communications protocol.

**NetWare**

Novell's Network Operating System which includes a protocol suite that provides network services and utilities.

**network number**

The number by which an individual network is identified.

**node**

The point at which a device is connected to a network; used to refer to the device itself. A node can be a computer, RAS server, printer, modem, or any other device.

**OSI (Open Systems Interconnection model)**

A model developed by the ISO used to define a network architecture.

**packet**

A unit of data transmitted on a network.

**peer-to-peer**

A networking system architecture in which connected workstations use and provide services such as file sharing.

**protocol**

A set of rules for exchanging data across a network.



**RARP (Reverse Address Resolution Protocol)**

A protocol that supplies a low-level address determination scheme by which a device obtains its IP address from a server.

**remote access**

Connecting to a network from a remote location using a computer, a modem, and remote access software.

**RIP (Routing Information Protocol)**

A protocol that allows gateways and hosts to exchange information about various routes to different networks.

**router**

An intelligent device that links networks together to form an internetwork. Routers know how to send data to any node in the internetwork.

**SAP (Service Advertising Protocol)**

A protocol used by Novell NetWare devices to broadcast their names, addresses, and current state on the network.

**server**

A network device that provides file sharing services to multiple computers on a network.

**SNMP (Simple Network Management Protocol)**

A protocol for managing network devices.

**subnet mask**

The IP network mask. Identifies the device's IP address, which portion constitutes the network address and which portion constitutes the host address.

**TCP (Transmission Control Protocol)**

A protocol that organizes packets, manages their transmission, and ensures their accurate delivery to the receiving station.

### **TCP/IP**

A protocol suite developed by the U.S. Department of Defense. Used to connect different types of computers while providing data correction, security, and reliability.

### **time-out**

The process by which a network device is unable to make a connection and, therefore, terminate a session.

### **Token Ring**

A LAN that conforms to the IEEE 802.5 Token Ring Access Method standard.

### **WAN (Wide Area Network)**

A communications network that connects geographically separated areas.

<b>A</b>	
Add / Edit IP Filter Definition .....	58
addresses	
fixed MAC addresses.....	73
addressing	
MAC addresses for COM ports .....	65
Apple remote access .....	84
AppleTalk .....	69
AssureNet.....	112
Async Control Map.....	137
Async Map	
Server.....	133, 137
<b>B</b>	
back panel	
Ethernet.....	10
LED.....	9
Token-Ring.....	12
BOOTP .....	47
<b>C</b>	
cables .....	4, 7
Call Back	
Server.....	106
call back .....	83, 106, 118
centralized billing .....	76
security.....	76
centralized billing .....	76
CHAP see security .....	105
COM port	
MAC address conventions.....	65
pinout diagram .....	139
communication parameters .....	87
communities	
adding .....	96
deleting .....	96
editing .....	96
configuration	
Manager, detailed steps .....	31
methods of.....	3
server .....	31
configuration file	
creating.....	32
downloading.....	41
opening.....	32
saving .....	40
screen description.....	33
configuration:Manager role.....	15
configuring	
call back .....	76
Dial-in .....	81
Dial-Out parameters .....	86
Dial-Out, summary.....	85
Dial-up networking .....	82
IP parameters.....	49
IPX parameters.....	59
modem pools .....	78
network protocols.....	47
serial port.....	37
SNMP.....	94
user records .....	71
configuring modem	
customized .....	133
Connect Time, RAS setting .....	74
connection	
disabling Manager port for dial-in .....	39
Manager, link problems, correcting .....	135
null modem cable diagram.....	140
creating a custom modem configuration .....	133
<b>D</b>	
data forwarding .....	87
date and time, server, setting.....	37
default mode.....	47
default settings	
LAN .....	14
ports.....	14
system.....	14
Dial Out	

trigger characters.....	88
Dial-In	
introduction.....	1
dial-in connection to server, disabling.....	39
Dial-In connection, communicating via.....	6
Dial-Out	
configuration summary.....	85
introduction.....	2
modem pools.....	91
parameters.....	86
server parameters.....	90
direct connect cable, communicating via.....	4
disabling users on RAS.....	72
disconnection unpredictability warning.....	74
downloading firmware.....	102
dynamic routing.....	61
<b>E</b>	
elapsed time limit, setting.....	74
enabling users on RAS.....	72
Ethernet	
installing.....	10
event log.....	101
event log, viewing.....	26
<b>F</b>	
File Menu	
Manager.....	24
firmware, updating.....	22
fixed MAC address	
overview of use.....	73
Fixed MAC Addresses	
configuring number of users.....	65
fixed time limit per user.....	74
Front Panel	
Menu Structure.....	123, 128
Message Codes.....	128
front panel	
description.....	8
functions of.....	121

language.....	121
menu descriptions.....	128
menu structure.....	123
password.....	103
security.....	120
use.....	122

## G

generic user.....	118
-------------------	-----

## H

### Hardware

833/2e.....	8, 12
asynchronous connector.....	139
LEDs.....	9
null modem cable diagram.....	140

### hardware

connector.....	139
front panel.....	8
installing Ethernet.....	10
installing Token-Ring.....	12
items included.....	7
null modem.....	140
specifications.....	141

### Help

Manager.....	28
help index, locating.....	28
hour/minute, setting on server.....	37

## I

### install

Token-Ring hardware.....	12
--------------------------	----

### IP

address.....	47
configuring.....	49
requirements.....	48

IP Filter Definition.....	57
---------------------------	----

### IPX

configuration.....	59
--------------------	----

parameters.....	59
requirements .....	59
IPX Filter Definition.....	67

## L

LAN status fields, server front panel .....	129
LAN, communicating over .....	3
LCD	
front panel.....	8
LCP see Link Control Protocol	
LED	
front and back panel.....	9
link control parameters, setting.....	135
Link Control Protocol .....	135
lock server front panel .....	26
log filter, adjusting.....	27

## M

MAC Addresses	
Fixed Addresses.....	65, 73
Manager	
files included with installation.....	16
link problems, correcting.....	135
main screen .....	23
option summaries.....	23
Manager software	
configuration of PC.....	3
installing .....	17
main screen .....	23
menu descriptions .....	24
overview .....	15
Menu Bar .....	23
modem configuration	
customized.....	133
modem pools	
overview .....	78, 91
Modem Strings	
Commands .....	134
modems	
commands .....	134

configuration .....	133
Dial-in .....	78
Dial-Out .....	91
installing.....	14
null modem .....	140
recommended speed.....	7
serial connection .....	17
monitoring server events .....	26

## N

Netware Bindery .....	104, 108
network access.....	107
NT Domain.....	117
Null Modem Cable .....	140
null modem cable diagram .....	140

## P

PAP see security.....	105
RAS	
configuring ports .....	40
customizing the event log .....	27
fixed MAC address .....	73
locking front panel .....	26
system statistics.....	26

## Port

RAS, configuring.....	40
port status fields, server front panel .....	129
protocols, supported .....	1

## Q

Quick Buttons.....	23
--------------------	----

## R

RADIUS .....	104, 109
RARP .....	48

## S

Security.....	106
security	

administrative privileges.....	103, 107
AssureNet.....	112
call back .....	76, 106
communities, community tables .....	95
configuration .....	107
external hardware.....	105, 111
front panel .....	103, 120
Netware Bindery .....	104, 108
network access .....	104, 107
PAP and CHAP.....	105
RADIUS.....	104, 109
server access.....	103
serial port, configuring.....	37
server	
configuration .....	31, 133
connecting to.....	15, 18
parameters .....	34
security.....	103
server list.....	20
setting time and date .....	37
SNMP	
communities.....	95
community tables.....	95
configuration .....	94
description.....	93
trap host.....	95
trap messages .....	95
static routing.....	61
statistics fields, server front panel.....	129
statistics, getting from server .....	26

statistics, viewing .....	97
Status Bar .....	23
string .....	38
subnet mask .....	47
system requirements .....	16

## T

Token-Ring	
hardware installation .....	12
Token-Ring, installing.....	12
Tool Bar descriptions, Manager .....	28
trap host .....	95
trap messages, SNMP .....	95
Trigger Characters .....	88

## U

Update Menu .....	25
user	
assigning fixed MAC address, overview.....	65
User Enabled, setting for server .....	72
User Filter Assignment.....	77

## V

View Menu .....	25
-----------------	----

## W

WAN Connector.....	139
Window Menu .....	27