

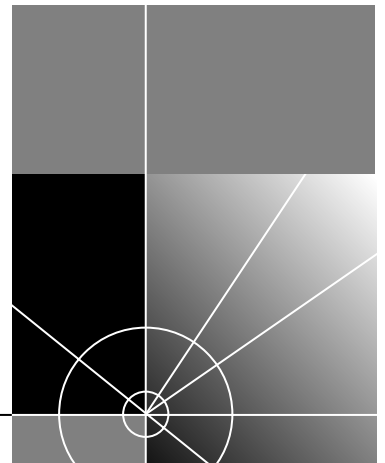


# SuperStack® II Remote Access System 1500 System Management Guide

Release 2.0

<http://www.3com.com/>

Part No. 1.024.1797 Rev 2.00  
December, 1999



**3Com Corporation**  
**5400 Bayfront Plaza**  
**Santa Clara, California**  
**95052-8145**

Copyright © 1999, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

**UNITED STATES GOVERNMENT LEGENDS:**

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

**United States Government Legend:** All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

[Portions of this documentation are reproduced in whole or in part with permission from (as appropriate).]

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, and SuperStack are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. AIX, AT, IBM, NetView, and OS/2 are registered trademarks and Warp is a trademark of International Business Machines Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

# CONTENTS

---

## ABOUT THIS GUIDE

Finding Specific Information in This Guide	13
Conventions	14
Related Documentation	15
Year 2000 Compliance	16

---

## 1 OVERVIEW

Overview	18
Basic Configuration	18
Port Expansion Module Configuration	18
Primary Access Unit	18
Applications	18
Dial-In	18
Shared ISP	19
LAN-to-LAN	19
Individual Dial-Out	19
Comprehensive Security Options	20
Configuration Options	20
Web Configuration Interface	20
Command Line Interface	20

---

## 2 USING THE COMMAND LINE INTERFACE

CLI Overview	22
Viewing Command Line Interface Help	22
Navigating the Command Line Interface	22
Obtaining Registered IP Addresses	23
Accessing the CLI	23
IBM Computer-compatible Computers	24
Macintosh Computers	24
UNIX-based Computers	24
Using CLI Quick Setup	24

Configuration with the CLI	25
Step One: Power On the RAS 1500	25
Step Two: Configure the RAS 1500 Basics	25
Step Three: Configure IP	26
Step Four: Configure IPX	27
Step Five: Configure DNS - <i>Optional</i>	30
Step Six: Configure SNMP - <i>Optional</i>	31
Step Seven: Save Your Work	31
64 Character Limit	32
Configuring a Manage User	32
Configuring Specific Modems	33
Configuring Modems in the Router Unit	33
Configuring Modems in the Port Expansion Unit	33
Configuring Modems in the Primary Access Unit	33
Configuring Expansion Units	34
Reconfiguring the Private IP Network	34
Replacing I/O Modules in the Port Expansion Unit	35
Disconnecting Expansion Units	35
Expansion Unit Configuration after Rebooting	35
Configuring the WAN Interface	36
Configuring Static Routes	36
IP Routes	36
IPX Routes	37

---

### **3 WEB-BASED CONFIGURATION OF THE RAS 1500**

Overview	39
Preparing the RAS 1500 for Web-based Management	41
Accessing the RAS 1500 for Web-based Management	43
Web-based Management of the RAS 1500	43
Basic Navigation	43
Setup Wizard	45
Configuration Pages	46
Accessing Help	48
Advanced Configuration	48

---

### **4 CONFIGURING DIALOUT/IP**

Overview	49
----------	----

Dialout IP Verses Telnet	49
Before You Begin	50
Required Information	50
Optional Information	50
Configuring Your System For DialOut/IP Software	50
Configure the RAS 1500	51
Configure Client Workstations	54

---

## **5 CONFIGURING TELNET NETWORK DIAL-OUT**

Overview	58
Using Telnet Network Dial-out	58
DialOut/IP Versus Telnet	59
Configuring and Using Telnet Network Dial-out	59
Before You Begin	59
Required Information	59
Optional Information	60
RAS 1500 Configuration	60
Computers on the Network	60
Configuring the RAS 1500	61
Step One: Add a System Name	61
Step Two: Add an IP Network	62
Step Three: Add a Modem Group (optional)	62
Step Four: Add the Dial-out Service	63
Step Five: Add Users	65
Step Six: Save Your Work	66
Configuring Network Computers	66
Dialing Out From a Network Computer	67
Case Study	67

---

## **6 CONFIGURING NETWORK DIAL-IN**

Overview	70
Using Network Dial-In	70
Before You Begin	71
Required Information	71
Configuring the Remote Computer	71

Requirements	71
Communications Software	71
Communication Parameters	71
IP Addresses	72
Configuring RAS 1500	72
IP Address Pool Overview	72
Step One: Configure an IP Address Pool	73
Step Two: Configure IP Network Users	74
Step Three: Configure PPP Parameters	76
Step Four: Configure Additional Parameters	78
Using Callback and Roaming Callback	79
Overview	79
Configuring Callback Users	79
Calling Line Identification Callback	80
Overview	80
Call Handling	82
Configuring CLID Callback	84
Step One:	
Add a CLID User	84
Step Two:	
Configure the User CLID-callback Settings	84
Step Three:	
Configure	
CLID Security	86
Troubleshooting CLID Callback	87
Case Study	88
Network Callback User Case Study	88
Assumptions	88
How to Configure this User	88
How it Works	89
Network User Case Study	89
Assumptions	89
How to Configure this User	90
How it Works	90

---

## **7 LAN-TO-LAN ROUTING**

Overview	92
The Difference Between Bridging and Routing	92

Routing Overview	93
IP Routing Overview	94
Dynamic, Static, and Default Routes	95
How the RAS 1500 Routes Packets	95
Establishing Connections to Remote Gateways	96
Spoofing	96
Authentication	96
Before you Begin	97
Required Information	97
Configuring LAN-to-LAN Routing	98
Step One: Add the LAN-to-LAN User	98
Step Two: Configure the User Network Parameters	99
Step Three: Configure the User Dial-out Parameters	100
Step Four: Configure the User Routing Parameters	102
Step Five: Configure the User PPP Parameters	103
Step Six: Configure Phone Numbers	104
Step Seven: Configure Authentication	105
Step Eight: Save Your Work.	105
LAN-to-LAN Routing Case Study	105
Goals	105
Assumptions	105
Strategies	106
Configuring IP on Demand	110

---

## **8 BRIDGING WITH THE RAS 1500**

Overview	112
How the RAS 1500 Acts as a Bridge	112
When to Use Bridging	112
113	
Bridging Tips	113
Enabling Bridging Over the LAN	113
Using FCP to Bridge with OfficeConnect Routers	114
Using Fast Connect Protocol	114

---

## **9 CONFIGURING AN IP TERMINAL SERVER**

Overview	119
Before You Begin	119

Configuring Remote Computers	119
Setting Communication Parameters	120
Configuring the RAS 1500 Login Hosts	120
Host Name	120
Address	120
Preference	120
Rlogin, Telnet and ClearTCP Ports	121
Configuring Login Users	121
Case Studies	124
Case Study A	124
Case Study B	126

---

## **10 ADVANCED MODEM CONFIGURATION WITH CLI/AT COMMANDS**

Overview	130
Before You Begin	130
Connecting to the RAS 1500	130
Accessing the Console Interface	130
AT Commands	130
Sending AT Command	130
Obtaining AT Command Help	131
Commonly Used AT Commands	131
Disconnecting with AT Commands	133
Configuring Data Compression Settings	134
Configuring Error Control Options	136
Using Error Control	137
Configuring Carrier Delay Times	138
Modifying Carrier Receive Delay	139
Configuring Link Option Settings	140
Link Speed Index	140
Obtaining Modem Call Information	144
Modem Query Commands	144
Working with Modem Memory	147
Viewing Settings	147
Saving a Phone Number to Flash Memory	148
Working with the Flash Memory Template	148
Configuring Modem Call Control Settings	149



Configuring 56 Kbps Technology	151
Factory-enabled Protocol	151
Controlling Server x2	151
Disabling V.34 Connections	152
Configuring ISDN	152
Enabling X.75	152
Frame Size	152
Window Size	152
Selecting Frame and Window Size	152
Relationships Between Frames and Windows	153
Viewing Current Frame and Window Size Settings	153
Best Possible Connection	153
Universal Connect Call Flow	154
Answering and Originating Calls	154
Setting the Originate Call Type	154

---

## **11 CONFIGURING THE RAS 1500 ROUTER**

Reconfiguring Your System	157
Customizing CLI Parameters	157
Discarding and Renaming Files	161
Communicating with Remote and Local Sites	161
Dial, Disconnect, and Hangup Commands	161
Exiting the CLI	162
Network Services	163
Troubleshooting Commands	168
Viewing Facility Errors	168
Terminating an Active Process	168
Resolving Addresses	169
Resolving Host Names	169
Using Ping	169
Viewing RAS 1500 System Information	172
Viewing Interface Status, Settings	172
Monitor PPP Activity	172
Displaying System Information	173
List Commands	173
Show Commands	173

---

## 12 USING SECURITY AND ACCOUNTING

- Authentication Overview 177
- Local Authentication 178
- RADIUS Authentication 178
  - Overview 178
  - RADIUS Authentication Process 179
  - Configuring RADIUS Authentication on the RAS 1500 180
- NOS Authentication 182
  - Overview 182
  - NOS Authentication Process 183
  - Installation Overview 183
  - Installing and Configuring NOS Authentication Software (Novell NetWare) 183
  - Installing and Configuring NOS Authentication Software (Windows NT) 189
  - Changing Encryption Key 191
  - Configuring NOS Authentication on the RAS 1500 192
  - Troubleshooting NOS Authentication 195
- RADIUS Accounting 195
  - Configuring RADIUS Accounting 196
  - Enabling and Disabling RADIUS Accounting 198

---

## 13 USING FRAME RELAY

- Overview 202
  - What is Frame Relay? 202
  - Permanent and Switched Virtual Circuits 202
  - Data Link Connection Identifier 202
  - Committed Information Rate 203
  - Forward and Backward Explicit Congestion Notifications 203
  - Local Management Interface 203
  - Supporting Frame Relay 203
  - Congestion Control 203
- Before You Begin 206
- Basic Frame Relay Configuration Using the Command Line Interface 206
  - Frame Relay User Configuration 206
- Frame Relay Data Link Configuration 208
- Frame Relay PVC Configuration 209

Monitoring and Troubleshooting	211
Show the Settings at the Interface Level	211
Show the Settings at the PVC Level	211
List PVC Statistics	211
List the Status of all Frame Relay PVCs	211
Case Study	211
Goal	211
Assumptions	211
Strategies	211

---

## **14 HANDLING PACKET FILTERS**

Filtering Overview	218
Filtering Capabilities	218
Filter Types	219
Data Filters	219
Advertisement Filters	219
Call Filters	220
Generic Filters	220
Creating Filters	220
Filter File Components	220
Creating Filter Files	224
Configuring Filters	226
Setting Filter Access	226
Interface Filters	227
User Filters	228
Assigning a Filter to an Interface	229
Assigning a Filter to a User	229
Managing Filters	230
Displaying the Managed Filter List	230
Adding Filters to the Managed List	230
Removing a Filter from an Interface	231
Removing a Filter from a User Profile	231
Deleting a Packet Filter	232
Verifying Filter File Syntax	232
Showing Filter File Contents	232
Generating SYSLOG Messages for Filtered Packets	232
General Filter Setup	233

Filter Examples	234
IP Packet Filter Rule Examples	234
RAS 1500 Global Filtering	241
Keywords	242

---

## **15 CONFIGURING DYNAMIC HOST CONFIGURATION PROTOCOL**

Overview	245
Scenario 1	246
Scenario 2	247
Scenario 3	247
Scenario 4	248
Scenario 5	249
Configuring the RAS 1500 for Dynamic Host Configuration Protocol	250
DHCP Server	250
DHCP Proxy Server	251
User Datagram Protocol Broadcast Forwarding	251
Configuring UDP Broadcast Forwarding	252
Displaying UDP Broadcast Forwarding Parameters	252

---

## **16 USING NETWORK ADDRESS TRANSLATION AND PORT ADDRESS TRANSLATION**

Overview	253
Network Address Translation	253
Port Address Translation	255
Configuring NAT and PAT	257
Configuring Network Address Translation	257
Configuring Port Address Translation	258
Case Studies	260
NAT Case Study	260
PAT Case Study	262

---

## **17 PPP OVER SERIAL WAN PORT**

Overview	265
Case Study	266
Before You Begin	266
PPP Over Serial WAN Port Case Study	267

Goals	267
Assumptions	267
Process	267
Disabling Leased-line PPP on the RAS 1500	270
Viewing the Status of the Connection	270
Troubleshooting	270

---

## **A GMT TIME ZONES**

---

## **B TECHNICAL SPECIFICATIONS**

Certification	279
United States	279
For More Information	280
Analog V.34 Model: FCC Part 68 Compliance Statement	280
Canadian Installations	280
Physical Dimensions	281
Interfaces	281
Power Requirements	283

---

## **C TECHNICAL SUPPORT**

Online Technical Services	285
World Wide Web Site	285
3Com FTP Site	285
3Com Bulletin Board Service	286
3ComFacts Automated Fax Service	287
Support from Your Network Supplier	287
Support from 3Com	287
Returning Products for Repair	289

---

## **INDEX**

---

## **3COM LIMITED WARRANTY**



# ABOUT THIS GUIDE

This guide describes how to configure the SuperStack® II Remote Access System (RAS) 1500 with AT commands and router commands.

You can also configure the RAS 1500 with the Web Configuration Interface. See Chapter 3 or Web configuration online help for more information.



*If the information in the release notes shipped with your product differs from the information in this guide, follow the instructions in the release notes.*

---

## Finding Specific Information in This Guide




This table shows the location of specific information in this guide.

Information Required	Reference
Command Line Interface basics	Using the Command Line Interface
Web-based Configuration	Web-based Configuration of the RAS 1500
Configuring NOS or RADIUS security	Using Security and Accounting
Enhancing security with packet filters	Handling Packet Filters
How to configure outgoing calls via DialOut/IP	Configuring DialOut/IP
How to configure outgoing calls via Telnet	Configuring Telnet Network Dial-Out
How to configure incoming calls	Configuring Network Dial-In
LAN to LAN routing configuration	LAN-to-LAN Routing
Bridging configuration	Bridging with the RAS 1500
IP terminal server configuration	Configuring an IP Terminal Server
Frame Relay configuration	Using Frame Relay
Warranty Information	3Com Limited Warranty


## Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

**Table 1** Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

**Table 2** Text Conventions

Convention	Description
Syntax	<p>The word “syntax” means you must evaluate the syntax provided and supply the appropriate values. Placeholders for values you must supply appear in angle brackets. Example:</p> <pre>Set callback user's primary dial-back number Set user &lt;name&gt; phone_number &lt;number&gt;</pre> <p>In this example, you must supply the user's name for &lt;name&gt; and phone number for &lt;number&gt;.</p>
<b>Commands</b>	<p>The word “command” means you must enter the command exactly as shown in text and press the Return or Enter key. Example:</p> <p>To list the current IP routes, enter the following command:</p> <pre><b>list IP routes</b></pre> <p> <i>This guide always gives the full form of a command in uppercase and lowercase letters. However, you can abbreviate commands by entering only the uppercase letters and the appropriate value. Commands are not case-sensitive.</i></p>
Screen displays	This typeface represents information as it appears on the screen.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”

(continued)



**Table 2** Text Conventions (continued)

Convention	Description
[Key] names	<p>Key names appear in text in one of two ways:</p> <ul style="list-style-type: none"> <li>■ Referred to by their labels, such as “the Return key” or “the Escape key”</li> <li>■ Written with brackets, such as [Return] or [Esc]</li> </ul> <p>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:</p> <p style="padding-left: 40px;">Press [Ctrl]+[Alt]+[Del]</p>
<i>Menu commands and buttons</i>	<p>Menu commands or button names appear in italics. Example:</p> <p style="padding-left: 40px;">From the <i>Help</i> menu, select <i>Contents</i></p>
Words in <i>italicized</i> type	<p>Italics emphasize a point or denote new terms at the place where they are defined in the text.</p>
Words in <b>bold-face</b> type	<p>Bold text denotes key features.</p>

## Related Documentation

The RAS 1500 documentation set includes the following documents. All 3Com documentation is available on the 3Com web site:

<http://www.3Com.com>

- *Base Unit Memory Upgrade SuperStack® II Remote Access System 1500*

This document describes how to perform the memory upgrade for the SuperStack II Remote Access System 1500.
- *Firmware Upgrade SuperStack® II Remote Access System 1500*

This document describes how to perform the upgrade procedures for the SuperStack II Remote Access (RAS) 1500 Base Unit and RAS 1500 Port Expansion Unit.
- *I/O Module Installation Guide SuperStack® II Remote Access System 1500*

This document describes how to install an I/O module in a Router Module or Port Expansion Module.
- *Release Notes SuperStack® II Remote Access System 1500*

This document provides information about the system software release, including new features and bug fixes. It also provides information about any changes to the RAS 1500 system

documentation. The Release Notes are enclosed in the RAS 1500 package and are available at <http://www.3com.com/ras1500.htm>.

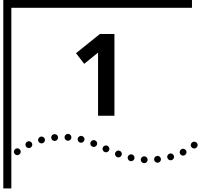
- *SuperStack® II Remote Access System 1500 Quick Setup Guide*  
This guide describes the installation and initial configuration of the RAS 1500 system.
- *SuperStack® II Remote Access System 1500 System Reference Guide*  
This guide describes how to configure the software for the SuperStack II Remote Access System 1500.

---

## **Year 2000 Compliance**

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

<http://www.3com.com/products/yr2000.html>



# OVERVIEW

This chapter contains the following information:

- Overview
- Applications
- Configuration Options

This guide provides the most commonly used command line interface (CLI) parameters.

---

**Overview**

The SuperStack® II Remote Access System (RAS) 1500 is a powerful data communications platform that supports a broad variety of applications.

**Basic Configuration**

The basic configuration of a RAS 1500 consists of one Router Unit with the following options:

- Two Basic Rate Interface (BRI) line connections, expandable to four
- Four analog lines, expandable to eight

**Port Expansion  
Module  
Configuration**

The RAS 1500 allows you to add two Port Expansion Units to your stack. The addition of the expansion units allows your RAS 1500 stack to support up to 12 Integrated Services Digital Network (ISDN) BRI lines or 24 analog lines.

**Primary Access Unit**

The RAS 1500 maybe be configured with a Router Unit and a Primary Access Unit as follows:

- T1 (North America) Primary Access Unit with 23 Primary Rate Interface (PRI)-ISDN channels
- E1 (European) Primary Access Unit with 30 PRI-ISDN channels

---

**Applications**

The RAS 1500 is a multiprotocol, dial-up router and terminal server commonly described as a remote access server. The RAS 1500 performs the following four basic applications:

- Dial-In
- Shared ISP
- LAN-to-LAN
- Individual Dial-Out

**Dial-In**

The RAS 1500 provides dial-in network access for remote users. Remote Internet Protocol (IP), Internetwork packet eXchange (IPX), and AppleTalk network users can dial in and attach to the local network as if they were on local nodes.

Packets transmitted over the dial-in connection are encapsulated using the following protocols:

- Point-to-Point Protocol (PPP)

- Serial Line IP Protocol (SLIP)
- 3Com Fast Connect Protocol (FCP)

The RAS 1500 offers access extensive security, dial-back, and substantial configurability for dial-in network connections.

**Shared ISP** The RAS 1500 can be configured for shared Internet Service Provider (ISP) access. This allows dial users and users on the Ethernet network to simultaneously share a single ISP dial-up connection/account.

**LAN-to-LAN** The RAS 1500 performs dial-up routing over a PPP connection between two local area networks (LANs), enabling users to share access or resources between a local LAN and a remote LAN. Routing occurs when one device dials up another device and logs in as a user.

There are several types of LAN-to-LAN connections:

- Manual
- On-demand
- Timed
- Continuous

The RAS 1500 supports many routing and protocol configurations. It is capable of establishing additional connections to increase bandwidth automatically when network traffic increases.

**Individual Dial-Out** Dial-Out is used to configure individual stations on the LAN to access a modem on the RAS 1500 as if the modem was virtually connected to the COM port on the PC. This allows network users to connect to a Bulletin Board System (BBS) or information services such as CompuServe, or to access the Internet over a dial-up PPP connection. LAN users require a dial-out IP application to access RAS 1500 modems.

## Comprehensive Security Options

RAS 1500 supports the following security options:

Firewall protection in the form of IP packet filtering in both the inbound and the outbound directions of ports, users, and dial-out locations.

- Remote Authentication Dial-In User Service (RADIUS)
- Network Operating System (NOS)-based authentication (Windows NT, Novell)
- Dial-back, fixed and roaming
- Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP)
- Local password authentication

---

## Configuration Options

The RAS 1500 supports the following configuration options:

- Web Configuration Interface
- Command Line Interface

## Web Configuration Interface

You can configure the RAS 1500 by accessing the RAS 1500 Web Configuration Interface. The Web Configuration Interface consists of a series of Web pages that are embedded on the RAS 1500 and viewed through a Web browser.

## Command Line Interface

The RAS 1500 command line interface (CLI) provides the most extensive set of commands available. It includes an assortment of utilities for troubleshooting connections including:

- The ability to manually dial a location to test connectivity
- The ability to use Telnet, Rlogin, or ClearTCP to establish a session with another host from the RAS 1500 command line
- UNIX-like troubleshooting commands, such as **ping**, to debug IP connections

# 2

## USING THE COMMAND LINE INTERFACE

This chapter contains the following information:

- CLI Overview
- Obtaining Registered IP Addresses
- Accessing the CLI
- Using CLI Quick Setup
- Configuration with the CLI
- Configuring a Manage User
- Configuration with the CLI
- Configuring Expansion Units
- Configuring the WAN Interface
- Configuring Static Routes

## CLI Overview

Although 3Com recommends using Web Configuration Interface to configure the SuperStack II Remote Access System (RAS) 1500, you can use the RAS 1500 command line interface (CLI) to configure all RAS 1500 parameters.



*You can also manage the RAS 1500 through the Web Management Interface, the Windows-based graphic user interface (GUI) provided in your package.*

## Viewing Command Line Interface Help

Any time you need help in the CLI, type a question mark (?) and press the Return key to view a list of possible options.

## Navigating the Command Line Interface

In addition to CLI commands required to configure the RAS 1500, the CLI has several additional commands to help make navigation through the CLI easier.

**Table 3** General CLI Editing Functions

Action	Command
Move to the beginning of the command line	Ctrl-A
Move to the end of the command line	Ctrl-E
Go left one character	Ctrl-B or left arrow
Go right one character	Ctrl-F or right arrow
Delete a character	Ctrl-D
Recall the next command in history	Ctrl-N
Recall the previous command in history	Ctrl-P
Go left one word	Esc-B
Go right one word	Esc-F
Display a full command or parameter	Tab Key
Display a list of possible parameters for your situation	<command>?
Display help for a command	help <command>



---

## Obtaining Registered IP Addresses

Each computer or network that attaches to the Internet must have a registered IP address.

Obtain registered addresses from the Internet Network Information Center (InterNIC) for IP machines and networks that are attached to the Internet. The InterNIC Web site is:

`http://ds.internic.net`

If you only need a small number of IP addresses, your Internet access providers should be able to provide them.

---

## Accessing the CLI

This section explains how to access the CLI through the console port using a communications program that supports VT100 terminal emulation (for example, HyperTerminal).

Use the following steps to access the CLI from the Windows 95 or Windows NT desktop:

- 1 Connect the provided serial cable to the RAS 1500 console port and your computer serial port.
- 2 Click *Start*, then *Programs*, then *Accessories*, then click *Hyperterminal*.
- 3 Select *hypertrm.exe*.

HyperTerminal starts and displays the Connection Description dialog box.

- 4 In the Connection Description dialog box, type a name and select an icon for your connection.
- 5 Click *OK*. The Connect To dialog box appears.
- 6 From the *Connect Using* drop-down list, select the communications port from which you are connected to the RAS 1500, for example, COM1.
- 7 Click *OK*. The Properties dialog box for the port you selected appears.
- 8 View the *Port Settings* tab. Modify settings to display these options:
  - Bits per second: 38400
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: Hardware

- 9 On the *Port Settings* tab, click *OK* to return to the CLI.
- 10 Press Enter.

The RAS 1500 displays the `RAS 1500>` prompt.

### **IBM Computer-compatible Computers**

Windows Terminal (included with Microsoft Windows) and ProComm Plus are popular communications packages that also support VT100 terminal emulation for IBM-computer compatible computers.

### **Macintosh Computers**

ProComm, MicroPhone, White Knight, Kermit, Red Ryder, VersaTerm, and ZTerm (a shareware application available on the Internet and many on-line services) are popular communications programs that carry VT100 terminal emulation service for Macintosh computers. If you do not have a communications package or your program does not support VT100 emulation, use ZTerm.

### **UNIX-based Computers**

Kermit, minicom, and tip are typical terminal emulation programs for UNIX-based computers. Depending on the platform you use, you may need to modify a configuration file for VT100 settings.

---

## **Using CLI Quick Setup**

The RAS 1500 automated Quick Setup program provides initial configuration through the CLI. It starts automatically after the boot process of an unconfigured device (or when you type **reboot** at the CLI prompt).

3Com recommends using the CLI Quick Setup to configure the RAS 1500 and access the GUI. The Quick Setup will let you set up simple configuration for your whole system or different portions of the system. For more information about the CLI Quick Setup, refer to the *Getting Started Guide*. Use the steps in the following section to perform basic CLI configuration.

---

## Configuration with the CLI

This section describes how to set up your RAS 1500 with the full CLI. To configure the RAS 1500 with CLI Quick Setup, see “Using CLI Quick Setup”.

### Step One: Power On the RAS 1500

To begin manual configuration, power on your RAS 1500. After a few moments when your screen has registered system initialization. The `RAS 1500>` prompt appears. When prompted by the Quick Setup Program to continue, enter the following: `no`

### Step Two: Configure the RAS 1500 Basics

Use the following steps to configure a basic setup on the RAS 1500:

- 1 Name your RAS 1500 and specify additional system information. The name you enter serves as the RAS 1500 DNS name and SNMP system name. The name is also the name that the RAS 1500 advertises in SAP broadcasts.

The name must be unique; no other device on your network can share it.

- a Set system information. Use the following command:

```
set system name <"RAS 1500 name" (up to 64 characters)>  
location ["system site"]  
contact ["contact information"]
```

You can enter the command all at once or in separate commands.

Example:

```
set system name superstack location boston contact "Bob  
@508 555-4567 666x"
```

Or, you can enter the following:

```
set system name superstack  
set system location boston  
set system contact "Bob @ 508 555-4567 666x"
```

- b Set the system date and time. Use the following command:

```
set date <dd-mon-yyyy> time <hh:mm:ss>
```

Example:

```
set date 01-jan-2001 time 01:01:01
```

**Step Three: Configure IP** Use the following steps to configure the RAS 1500 interface (rm0/eth:1) for IP networks. The IP network information is required for proper operation.

- 1 Enter IP network information. The network address consists of the station address and a subnet mask using this format:

```
nnn.nnn.nnn.nnn/A, B, C, H, 8-30 or nnn.nnn.nnn.nnn
```

The first four octets describe the IP station address, followed by the subnet mask (contiguous) designator. You can specify the subnet by class, numerical designation or in the IP address format. If you specify a Class C mask, for example, this command generates a 255.255.255.0 subnet value for you. If you specify the number of 1 bits in the mask, the acceptable range is 8-30 (32 if a host).

The network address is considered invalid if the portion of the station address not covered by the mask is 0, or if the station address plus the mask is -1 (all 1s). Defining a numerical subnet is useful when your classification falls in between classes.

To enter the IP network information, enter the following command:

```
add ip network <network name>  
interface rm0/eth:1  
address <station address/mask>  
frame [ethernet_II | snap]
```

For example, to enter IP network information with the traditional subnet mask format, use the following command:

```
add ip network backbone address 192.75.202.99/C interface  
rm0/eth:1 frame ethernet_II
```

To enter IP network information in a numerical mask format, use the following command:

```
add ip network backbone address 192.75.202.99/24 interface  
rm0/eth:1 frame ethernet_II
```



*To verify network settings, use the list networks command and check the connection by using the ping <ip address> command.*

- 2 Set a default gateway. Default gateways must be on the same subnet.

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

To add the default gateway, use the following command:

```
add ip defaultroute gateway <default route gateway ip address> metric <integer>
```

Example:

```
add ip defaultroute gateway 192.75.202.40 metric 1
```



*Check the default route setting with the list ip routes command.*

#### **Step Four: Configure IPX**

To configure the RAS 1500 LAN interface on an IPX network, you must:

- Determine the IPX network number
- Set the RAS 1500 IPX parameters
- Specify Frame Type



*Even if your network uses only the IPX protocol, you must still set up an IP address for the RAS 1500, if you want to use the Web Management Interface later.*

#### **Determining the IPX Network Number**

If your network uses the IPX protocol, you must first enter the IPX network number of the segment connected to the RAS 1500 LAN port. You can find this network number using the Novell CONFIG utility.

#### **For File Servers Running Novell Version 3.xx**

- 1 Go to the console of a file server that is on the same network segment as the RAS 1500.
- 2 From the Novell Console program press **C-E**, then **E**, until the colon (:) prompt appears. Select *System Console* and press the Return key.

**3** Type the following:**config**

A display similar to the one shown below appears:

```
File server name:  USR_SERVER_ONE
IPX internal network number: 0000000A
Western Digital Star EtherCard PLUS Driver v2.05 (910424)
Hardware setting: I/O Port 300h to 31Fh, Memory CC000h to
Cffffh, Interrupt Ah
Node address: 0000C0488D28
  Frame type: ETHERNET_802.3
  Board name: TENBASE_802.3
  LAN protocol:  IPX network 00000255
Western Digital Star EtherCard PLUS Driver v2.05 (910424)
Hardware setting: I/O Port 300h to 31Fh, Memory CC000h to
Cffffh, Interrupt Ah
Node address: 0000C0488D28
  Frame type: ETHERNET_802.2
  Board name: TENBASE_802.2
  LAN protocol:  RPL
  LAN protocol:  IPX network 00000684
```

This is an example of the information returned for one version 3.xx card that has two different frame types. The card has one port address, but two LAN protocol network addresses, one for each frame type. The network number for 802.3 is 00000255, and for 802.2 it is 00000684.

**4** Write down the LAN protocol IPX network number for the frame type you want to use.**For File Servers Running Novell Version 2.xx**

Use the following steps to configure file servers running Novell version 2.xx:

- 1** Go to the console of a file server that is on the same network segment as the RAS 1500.
- 2** Press C-E until the colon (:) prompt appears.

- 3 Type the following:

```
config
```

The RAS 1500 displays information similar to the display below:

```
LAN A Configuration Information:
Network Address:  [0788] [002608C0D53F4z]
Hardware Type:   [3Com 3C505 EtherLink Plus (Assy 2012 only)
V2.30EC (880813)]
Hardware Setting:  IRQ=5, IO=300h, DMA 5
```

The above example only has one frame type, so the network address is 0788.

- 4 Write down the network address for the frame type you will use.

### Setting IPX Parameters

To configure the RAS 1500 LAN interface for an IPX network:

- 1 Specify IPX network information including the network name, address, interface and frame type of the network segment connected to the RAS 1500 LAN port. The same physical network segment has a different network number for each frame type used. Be sure to enter the network number associated with the chosen frame type. Use the following command:

```
add ipx network <network name>
address [ipx address]
interface rm0/eth:1
frame [dsap | ethernet_ii | novell_8023 | snap]
```

Example (abbr.):

```
add ipx network segment2 add 00000576 interface rm0/eth:1
frame ethernet_ii
```



*You can omit preceding zeros. The RAS 1500 accepts "576" as the correct IPX network number.*

- 2 Set the IPX default gateway with the format xxxxxxxx.xx:xx:xx:xx:xx:xx where xxxxxxxx is the IPX network address and xx:xx:xx:xx:xx:xx is a MAC address.

```
set ipx system default_gateway <network number.mac address>
```

Example:

```
set ipx system default_ gateway ABCD.011:11:01:11:00:11
```



*To verify network settings, use the **list networks** command.*

- 3 Save your work.

```
save all
```

**Step Five: Configure  
DNS - Optional**

This section sets a Domain Name Server (DNS). If you do not wish to use DNS, skip to “Step Six: Configure SNMP - Optional”.

- 1 Specify the IP address of the server you want to function as the DNS server, which, when queried, translates host names into their corresponding IP addresses and saves that information in a local Hosts Table.

You can name up to 10 DNS servers using the command shown on the next page. You must specify the order in which they are to be chosen (highest priority: 1). This value is the *preference* number.



*The RAS 1500 tries to reach each configured host three times in round-robin fashion before issuing an error message. For instance, in the case of three offline servers - A, B, and C, the RAS 1500 admits failure only after trying to reach them one after the other, three times.*

Use the following command:

```
add dns server <ip_address> preference <number> name  
<server_name>
```

Example:

```
add dns server 192.75.222.182 preference 1 name farley
```



*The DNS server is only consulted to resolve host names not found in the Hosts Table. If you are using a name service, the Hosts Table may be left empty. Also, issue `list dns server` and `show dns settings` commands to verify your action. You may use the `resolve name` command to learn DNS host names or numbers.*

- 2 Specify your default domain, the Ethernet segment where your system resides and your default. Adding this entry to the Hosts Table eliminates the task of always specifying the domain. Use the following command:

```
set dns domain_name <string>
```

Example:

```
set dns domain_name 3com.com
```



### Step Six: Configure SNMP - *Optional*

The following section configures SNMP service. If you do not wish to set up SNMP, skip to “Step Seven: Save Your Work”.

If you plan to use an SNMP application to configure and manage the RAS 1500, you must specify SNMP community values. SNMP community names segregate administrative management groups and should match the community settings of your generic SNMP software.

You must set the following SNMP community values:

- **name** — community name
- **address** — IP address of the Windows SNMP manager
- **access** — either read-only, read-write or administrator (read and write) access



*For a public community with read-only privileges, assign the address to any station (0.0.0.0).*

To add the SNMP community values, enter the following:

```
add snmp community <name>\  
address <IP address>  
access [RO | RW | ADM]
```

Example:

```
add snmp com mis add 192.77.202.30 acc adm
```



*Command keywords can be abbreviated, as long as they are unique to the command.*

### Step Seven: Save Your Work

Save your work.

```
save all
```

## 64 Character Limit

The CLI has a 64 character limitation for each field. When you attempt to add more than three interfaces with the interface command, 3Com recommends the following:

- 1 Assign the first three interfaces.

```
add modem_group test interface <3 interface names>
```

Example:

```
add modem_group test interface
rm0/slot:1/mod:1,rm0/slot:1/mod:2, rm0/slot:1/mod:3
```

- 2 Assign the additional interfaces.

```
assign interface <3 interface names> modem_group test
```

Example:

```
assign interface
rm0/slot:2/mod:3,rm0/slot:2/mod:4,pem0/slot:1/mod:1 mod test
```

## Configuring a Manage User

This section describes how to create an administrative user with *manage* privileges to establish a secure, centrally administered router through the CLI. You can configure a remote login user, or, if you prefer to dial in, you can create a manage user locally through the console port. You cannot do so via Telnet at this point in the configuration.



*Only manage users can access the CLI.*

- 1 Create a manage user:

- If you want the manage user to login, use the command below, set the type to *manage*, *login* and login service (Telnet is the default; otherwise choose Rlogin or ClearTCP).
- If you want a manage user to access the device via a dial-in (network) connection, use the command below. The network service default is PPP; otherwise select SLIP.

```
add user <"username">
network_service [ppp, slip, arap, fcp, fr_1490]
password [password]
type [login, network, callback, dial_out, manage]
```



*Passwords are optional. You may add a null password with the keyword password and string: ""*

Network example:

```
add user predator type manage,network
```

Login example:

```
add user predator type manage,login
```

2 Save your work.

```
save all
```

## Configuring Specific Modems

When connected to the Router Unit Console Port, you can configure all devices in your stack with the CLI. Each modem is identified by slice (rm0, pem0, pem1, and pem2), slot (slot1 or slot2), and modem number (mod:1, mod:2, mod:3, mod:4).

### Configuring Modems in the Router Unit

To configure specific modems on your Router Unit, use the following rule:

```
set imodem interface rm0/slot<1-2>/mod:<1-4> at_command
[command]
```

For example, to view the configuration of the first I-modem in the left slot of your Router Unit, use the following command:

```
set imodem interface rm0/slot1/mod:1 at_command ati12
```

### Configuring Modems in the Port Expansion Unit

To configure specific modems on your Port Expansion Unit, use the following rule:

```
set imodem interface pem<0-2>/slot<1-2>/mod:<1-4>
```

For example, to view the configuration of the first I-modem in the left slot of the first Port Expansion Unit in your stack, use the following command:

```
set imodem interface pem0/slot1/mod:1 at_command ati12
```

### Configuring Modems in the Primary Access Unit

To configure specific modems on your T1 Primary Access Unit, use the following rule:

```
set imodem interface pau0/slot1/mod:<1-23>
```



*The T1 PAU has 23 modems while the E1 has 30.*

For example, to view the configuration of the first I-modem in the Primary Access Unit in your stack, use the following command:

```
set imodem interface pau0/slot1/mod:1 at_command ati12
```

## Configuring Expansion Units

The RAS 1500 requires minimal configuration. However, several unique situations require additional Port Expansion Unit or Primary Access Unit configuration.

### Reconfiguring the Private IP Network

The Router Unit that supports the expansion units uses a private IP network over the IEEE1394 bus (FireWire) to communicate with the expansion units. Because the Router Unit communicates with the expansion units using IP, configure a private IP subnet address to the FireWire interfaces.

The Router Unit configuration software selects the IP address/subnet pair 192.168.128.0/255.255.255.0 for this private network. This is defined as a private Class C subnet, is not to be transmitted onto the public Internet, and need not be registered with the IETF. Although it is private, it may possibly conflict with other private IP networks defined in an office or enterprise. If there is a conflict, unpredictable problems with routing those private IP addresses through the RAS 1500 and unpredictable problems with booting expansion units could occur. Therefore, the RAS 1500 supports reconfiguration of this private network.

Use the following steps to reconfigure the RAS 1500 private IP network:

- 1 Select a private IP network/subnet pair that does not conflict with any other private addresses inside of your internet gateway.



*Contact your Network Administrator for more information.*

- 2 Disable the IP network associated with the FireWire.

```
disable ip network ip_fwire
```

- 3 Reconfigure the IP network associated with the FireWire with the unique IP network/subnet mask selected in step 1 (where x.x.x.x/x.x.x.x is the address mask, subnet pair).

```
reconfigure ip network ip_fwire address x.x.x.x/x.x.x.x
```

- 4 Re-enable the IP network associated with the FireWire.

```
enable ip network ip_fwire
```

- 5 Save your changes.

```
save all
```

### Replacing I/O Modules in the Port Expansion Unit

The slot in each Port Expansion Unit retains configurations of specific I/O modules that are installed. As a result, the Port Expansion Unit uses the following rules when you replace I/O modules (analog modems, U interface ISDN, or S/T interface ISDN):

- If you remove an I/O module from a Port Expansion Unit and replace it with the same type of module into the same slot, the Port Expansion Unit retains the configuration of that module.
- If you remove an I/O module from a Port Expansion Unit and replace it with different type of I/O module in the same slot, the Port Expansion Unit may not recognize the new I/O module.

To verify if the Port Expansion Unit recognizes the correct I/O modules, use the `show pem <pem name>` command in the CLI.

After you install a new I/O module, if the Port Expansion Unit does not correctly recognize it, complete the following steps:

- 1 Disconnect the FireWire cable to the Router Unit.
- 2 Delete the Port Expansion Unit:  
`delete pem <pem-name>`
- 3 Save the configuration:  
`save all`
- 4 Reconnect the FireWire cable.
- 5 Reset the Port Expansion Unit (via the front panel).
- 6 After the boot procedure is complete (blinking green on the Port Expansion Unit), save the configuration:  
`save all`

### Disconnecting Expansion Units

After an expansion unit is physically disconnected from a stack, the `list stack` command still recognizes the removed expansion unit. To permanently remove the expansion unit from the list, issue the `delete unit type (pem, pau)` command, then the `save all` command.

To list available ports, use the `list interfaces` command. This command lists ports on physically connected expansion units.

### Expansion Unit Configuration after Rebooting

When you add an expansion unit to a stack, issue the `save all` command in the CLI; otherwise, the expansion unit configuration will not be saved after a reboot.

---

## Configuring the WAN Interface

Protocols are set up over the WAN by creating and editing a user profile. A user profile specifies the call type, protocols, addresses, and bandwidth management parameters that determine how you connect and communicate to that user (remote site) over the WAN.

When you save user profiles you've just created, you are finished configuring the RAS 1500 side of the link. Configuration of the router on the remote side of the WAN link varies, but setup includes the local IP address. See your product manual for more information.

---

## Configuring Static Routes

The RAS 1500 provides the ability to dynamically learn remote IP routes via the IP RIP protocol. The `add ip route` or `add ipx route` commands set the destination IP/IPX address, the gateway used to access the remote destination, and a metric value or distance in hops to reach the destination from the RAS 1500.



*The RAS 1500 also allows you to configure a static route when you know the destination you want to connect with.*

### IP Routes

The command below adds an IP static route entry to the IP Routing Table:

```
add ip route <ip_network_address>  
gateway [gateway_address]  
metric [hop_count]
```

The IP address of the remote destination is written in the format *nnn.nnn.nnn.nnn*, entered with or without a mask specifier. The mask specifier can be designated either 'A', 'B', 'C', or 'H' (host), or with a numeric value from 8 to 30 (32 if a host) that describes the number of one bits in the mask. You can also specify the netmask in the *xxx.xxx.xxx.xxx* format. If you do not specify a mask, the system generates it (based on the network address) for all routes (*ip\_net\_addresses*) except host routes, for which you must specify a mask.

Example:

```
add ip route 145.122.231.43/h gateway 145.122.232.28 metric 1
```

The `list ip routes` command displays all currently defined routes including the route just configured but only if you have specified a gateway.



*Static routes are installed but not visible via the `list ip routes` command until the interface to the gateway is active (entered in the IP/IPX Forwarding Tables).*

## IPX Routes

The command below adds an IPX static route entry to the IPX Routing Table:

```
add ipx route <ipx_network_address>  
gateway [gateway_address]  
metric [hop_count]  
ticks [number]
```

The IPX network address of the remote destination is written in the hexadecimal format `xxxxxxx` where addresses `fffffff` or `ffffffe` are invalid. The gateway is expressed in the hex format `xxxxxxx.xx:xx:xx:xx:xx:xx` where `xxxxxxx` is the IPX network address and `xx:xx:xx:xx:xx:xx` is a MAC (Ethernet) address. Metric and tick values are also required. Ticks specify the interval between transmission and delivery of a packet to the remote network.

Example:

```
add ipx route fffff111 gateway fffff101.ff:ff:ff:00:00:ff  
metric 1 ticks 1
```

The `list ipx routes` command displays all currently defined routes including the route just configured but only if you have specified a gateway.



*Static routes are installed but not visible via the `list ipx routes` command until the interface to the gateway is active (entered in the IP/IPX Forwarding Tables).*





# 3

## WEB-BASED CONFIGURATION OF THE RAS 1500

This chapter contains the following information about Web-based configuration of the RAS 1500:

- Overview
- Preparing the RAS 1500 for Web-based Management
- Accessing the RAS 1500 for Web-based Management
- Web-based Management of the RAS 1500

---

### Overview

You can remotely configure the RAS 1500 by accessing the RAS 1500 Web Configuration Interface. The Web Configuration Interface consists of a series of Web pages that are embedded on the RAS 1500 and viewed through a remote Internet browser, such as Netscape Navigator or Microsoft Internet Explorer (4.x or greater).

Initially, use the Web Configuration Interface Setup Wizard to perform basic configuration of the RAS 1500. The Setup Wizard guides you through the setup of the modem configuration, dial-in, dial-out, LAN-to-LAN, and shared ISP applications.

After you set up the RAS 1500 using the Setup Wizard, use other Web pages in the Web Configuration Interface to configure the following:

- Basic system information, such as the RAS 1500 name and location
- Date and time settings, including daylight savings time
- Domain name server (DNS) settings
- IP and IPX settings, such as addresses and framing methods and address pools
- Dynamic host configuration protocol (DHCP) settings
- Network address translation (NAT) and port address translation (PAT) settings
- Authentication Remote Authentication Dial-In User Service (RADIUS) and network operating system (NOS) and accounting settings
- Login host, Simple Network Management Protocol (SNMP) community, and Trivial File Transfer Protocol (TFTP) client settings
- System log settings
- Modem group settings
- User settings
- Network services, such as Telnet
- Calling line identification (CLID) callback settings

Other Web pages in the Web Configuration Interface let you perform the following:

- Access the RAS 1500 console through a Telnet connection
- Reboot the RAS 1500
- Save, backup, and restore the RAS 1500 configuration
- Restore the RAS 1500 to its factory-default settings

## Preparing the RAS 1500 for Web-based Management

Before you can manage a RAS 1500 using the Web Management Interface, the RAS 1500 must have an IP address assigned to it. Out of the box, the RAS 1500 does not have an IP address.

This procedure lets you assign an IP address, network mask, and community string to the RAS 1500.

To assign an IP address to a device:



*Before you start this procedure, confirm the RAS 1500 is connected to the same LAN segment as the workstation on which you are running the IP Wizard.*

- 1 Insert the SuperStack II Remote Access System 1500 Resource CD into the CD-ROM drive. The RAS 1500 Setup Screen appears.



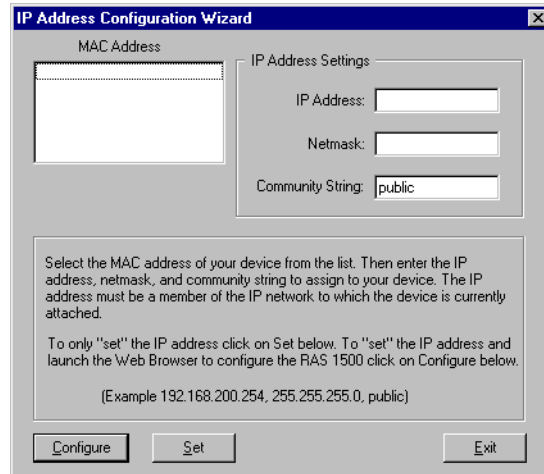
*If your PC does not automatically run the CD, perform the following steps:*

- a At the Windows 95 or NT desktop, click Start, then click Run.
- b In the Run dialog box, type the following: `<your CD drive letter>:\setup`
- c Click OK. The RAS 1500 Resource CD Splash Screen displays as shown in Figure 1.



**Figure 1** RAS 1500 Resource CD Splash Screen

- 2 At the RAS 1500 Setup screen, click Configure RAS 1500. The IP address Configuration Wizard appears as shown in Figure 2.



**Figure 2** IP Address Configuration Wizard

- 3 In the Discovered MAC Address list, select the RAS 1500 to which you want to assign an IP address. This list contains devices that are connected to the same LAN segment as the IP Wizard workstation but do not have an IP address.



*The RAS 1500 MAC address is printed on a sticker on the rear of the unit.*

- 4 In the IP Address text box, type the IP address (in dotted-decimal notation) you want to assign to the RAS 1500. The IP address you assign must be a part of the IP network to which the RAS 1500 is attached.
- 5 In the Netmask text box, type the network mask (in dotted-decimal notation) you want to assign to the device. For example, a class C network with no subnetting is 255.255.255.0.
- 6 Click Configure. The settings are assigned to the RAS 1500. The RAS 1500 is ready to be accessed over the Internet.

---

**Accessing the RAS 1500 for Web-based Management**

To access the RAS 1500 Web Management Interface, perform the following steps:

- 1 Launch your preferred Internet browser.

To properly view the Web Management Interface, your browser must meet the following criteria:

- HTML Version 4 or greater
  - Java script supported and enabled
  - Style sheets supported and enabled
  - Frames supported
  - 800 x 600 resolution on a 15" monitor
- 2 In the location or address field at the top of the browser, type the RAS 1500 IP address. The Web Management Interface appears.

---

**Web-based Management of the RAS 1500**

This section provides an overview of the RAS 1500 Web Configuration Interface.

**Basic Navigation**

Figure 3 highlights important aspects of the initial screen of the RAS 1500 Web Configuration Interface. See Table 4 for a detailed description.

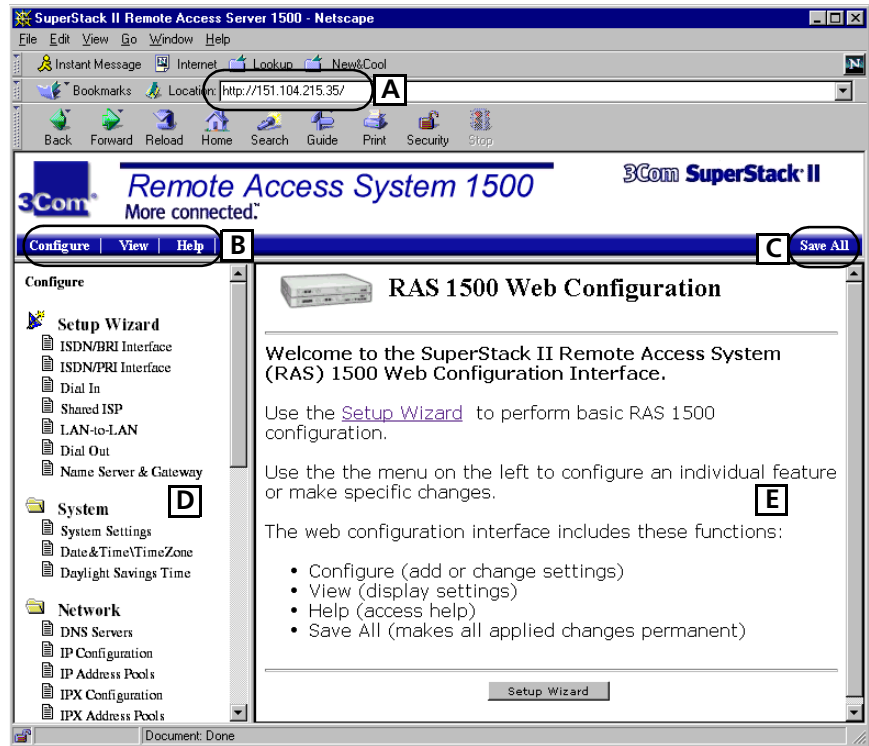


Figure 3 Web Configuration Interface, Initial Screen

**Table 4** Web Configuration Interface, Initial Screen

Callout	Description
A	Uniform resource locator (URL) of the RAS 1500.
B	Available views. Each of these views displays a different tree of folders and Web pages in the left frame of the window. The "Configure" view displays Web pages in which you change the RAS 1500 settings. The "View" view displays Web pages in which you view the RAS 1500 settings. The "Help" view displays Web pages that offer help for each configuration page.
C	"Save All" button. Click this button to save all of the changes you have made to memory.
D	Navigation frame. Click on a Web page in this frame to configure settings, view settings, or receive help about a Web page. This frame is in either "Configure," "View," or "Help" mode (see callout B, above, for more information).
E	Work frame. This frame displays the configuration, view, or help Web pages.

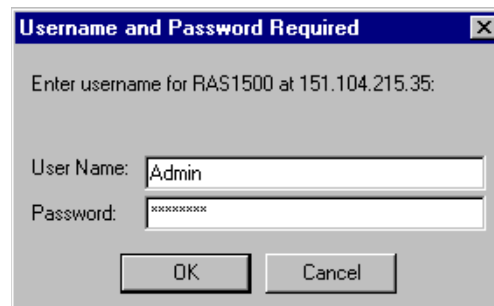
## Setup Wizard

The Web Configuration Interface Setup Wizard allows you to quickly configure the RAS 1500 for basic functionality.

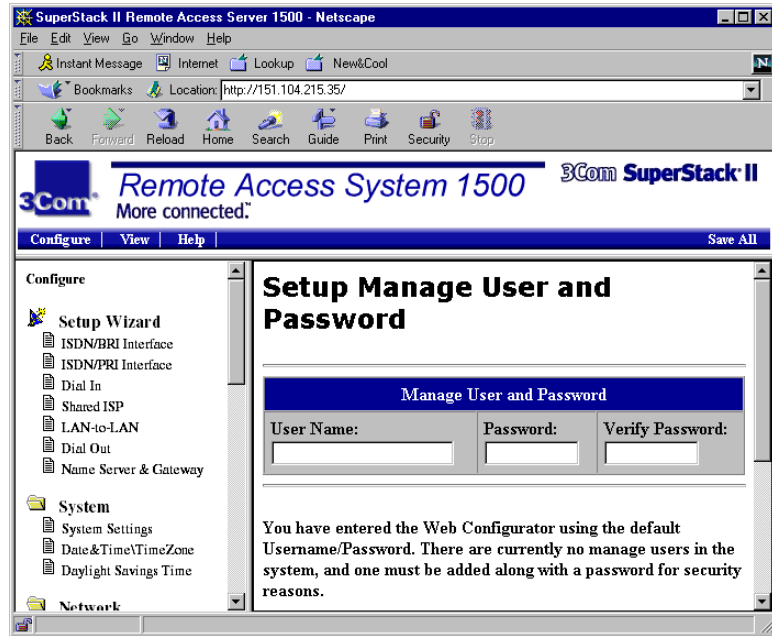
To launch the Setup Wizard, either click the "Setup Wizard" link in the text of the initial screen or click the "Setup Wizard" icon at the top of the left frame. Once you launch the Setup Wizard, follow the instructions on the screen.



*Before you can make configuration changes or selections, you are prompted to enter a Username and Password as shown in Figure 4. The default Username and Password is **Admin** and **Password**.*

**Figure 4** Web Configuration Interface, Username and Password Screen

After entering **Admin** and **Password**, you are prompted to setup a manager user as shown in Figure 5. Once this is done you may setup the RAS 1500.

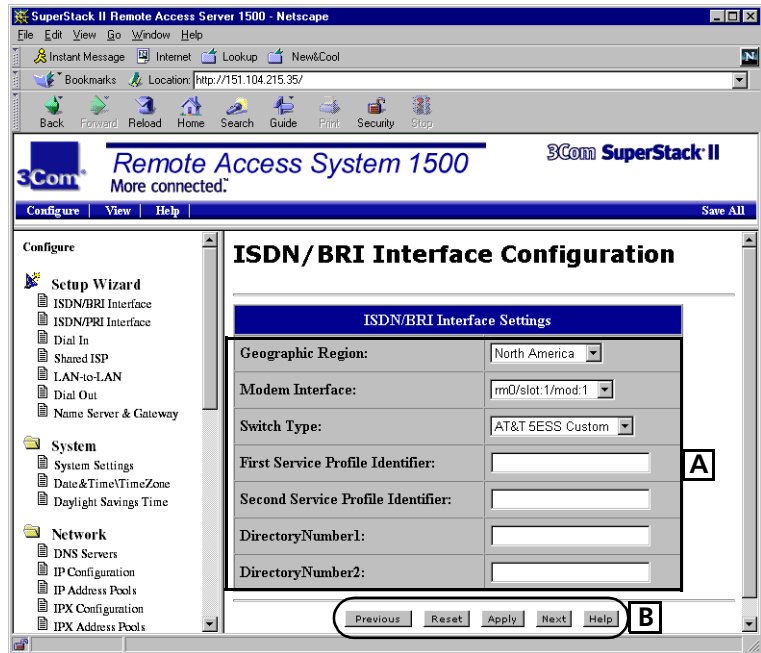


**Figure 5** Setting Manager User Username and Password

### Configuration Pages

Figure 6 shows a configuration page in the Web Management Interface. See Table 5 for a detailed description.





**Figure 6** Web Configuration Interface, Configuration Page

**Table 5** Web Management Interface, Configuration Page

Callout	Description
A	Configuration fields.
B	Navigation buttons.

**Accessing Help** The Web Configuration Interface offers three types of help:

- **Status bar help.** In a configuration page, place the cursor over a field label. Help text appears in the status bar of the browser.
- **Field-specific help.** In a configuration page, click on a field label. A new window appears and displays help text for the selected field.
- **Page-specific help.** In a configuration page, click the Help button at the bottom of the page, or, in the “Help” view, click the configuration page for which you want help. A new window appears and displays help text for the page.

**Advanced Configuration** After initial configuration using the setup wizard, you use the Navigation frame (Figure 3) to configure the following functions:

- System
- Network
- Administration
- Dial-In
- Dial-Out
- Management

# 4

## CONFIGURING DIALOUT/IP

This chapter contains the following information:

- Overview
- Before You Begin
- Configuring Your System For DialOut/IP Software

---

### Overview

DialOut/IP™ allows computers connected to the local area network to access modems on the SuperStack II Remote Access System (RAS) 1500, as though the modems were directly connected to the computers. Once connected to a modem, a network user can dial out to the Internet, electronic bulletin board systems (BBSs), information services (such as CompuServe), ftp sites, and e-mail sites—anything that you could access with a modem directly connected to the computer.

### Dialout IP Verses Telnet

Network computers communicate with the RAS 1500 over the LAN using either DialOut/IP or Telnet. A difference between DialOut/IP and Telnet network dial-out is that DialOut/IP supports Windows Dial-Up Networking, and Telnet does not. So, if you need access to the Internet over a dial-up PPP connection or any software that supports PPP negotiation, which Windows Dial-Up Networking provides, choose DialOut/IP.

If you do not need to use Windows Dial-Up Networking, either method is acceptable, although Telnet is easier to set up.

This chapter details DialOut/IP. For details about Telnet dial-out, refer to Chapter 5, “Configuring Telnet Network Dial-Out”

---

**Before You Begin**

Before you configure DialOut/IP, you need to obtain some system information and confirm some basic configuration of the RAS 1500 and the network computers.

**Required Information**

The following information is required:

- System name of the RAS 1500
- MAC address of the RAS 1500
- IP address of the RAS 1500
- IP network name
- Network service name

**Optional Information**

The following information is optional:

- Modem group name
- Modems to include in the modem group

---

**Configuring Your System For DialOut/IP Software**

The RAS 1500 includes DialOut/IP software for Windows® 95/98/NT computers. DialOut/IP allows the RAS 1500 modems to be shared for dialing out. However, the RAS 1500 is not configured “out of the box” to support dial-out.

Setting up your system for dial-out through the RAS 1500 using DialOut/IP software requires two general steps:

- 1 Configure the RAS 1500.
- 2 Configure client workstations.

These steps are detailed below.

## Configure the RAS 1500

Complete the following steps to enable dial-out through the RAS 1500.



*Unless otherwise noted, all of the commands in these steps are issued through the command-line interface (CLI) of the RAS 1500. Press the Enter key to issue the command. Items in brackets (<...>) require specific information from the user.*

### Step 1: Define a Modem Group

The modem group you define contains the modems that are used for dial-out. Issue the following commands:

```
add modem_group <modem group name> interface <list of modems>
set modem_group <modem group name> access two_way
```

The <modem group name> is the name to assign the modem group, for example, dialout\_modems.

The <list of modems> is a comma-separated list of modem device names. It cannot contain spaces.

Example: rm0/slot:1/mod:1,rm0/slot:1/mod:2

The RAS 1500 includes a default modem group named "all" that contains all of the modems on the RAS 1500. If you want dial-out available from all of the modems on the RAS 1500, skip the "add" command and use the "all" modem group in the "set" command.



*Use the "all" modem group only if every modem port on the 1500 is connected to a telephone switch, central office, or PBX.*

### Step 2: Define a Network Service

The network service you define provides access to the modem group at a specified TCP port number. Issue the following command (line breaks added for readability):

```
add network service <service name> server_type telnetd socket
<socket number> data auth=off,service_type=dialout,
modem_group="<modem group name>"
```

The <service name> is the name to assign the network service, for example, dialout-service.

The <socket number> is the TCP port number where the service is accessible. DialOut/IP expects the TCP port number for the RAS 1500 to be 6000 (and above). Therefore, 6000 is a logical value to use.

The <modem group name> is the name of the modem group created in Step 1. The parameters following the "data" keyword cannot include spaces.

### Step 3: Turn off Security for Dial-out

DialOut/IP does not support authentication through the RAS 1500, therefore a "login" prompt must not appear when the network service is first contacted. To ensure security is off, issue the following command:

```
set dial_out security no
```

### Step 4: Save the Configuration

Save the configuration using the following command:

```
save all
```

### Step 5: Test the Configuration

To test that the configuration was successful, complete the following steps **from a workstation on the same LAN as the RAS 1500**:

- 1 From the Windows desktop, select Start, then Run. The Run dialog box appears.
- 2 In the Open text box, enter the following:

```
telnet <RAS1500's IP address> <network service's port number>
```

Example:

```
telnet 192.168.1.1 6000
```

- 3 Click OK. A Telnet session starts.
- 4 In the Telnet window, type **AT**, then press Enter.
  - If the response is "OK," the port is configured correctly for dial-out using DialOut/IP.
  - If the connection is unsuccessful, or if a "login" prompt appears, the port is configured incorrectly for dial-out using DialOut/IP. Review the previous steps and try again.

### Example 1: Dial out using all modems

To enable dial-out on all modems in the RAS1500, using the default modem group "all," issue the following commands (line breaks added for readability):



*Use the "all" modem group only if every modem port on the 1500 is connected to a telephone switch, central office, or PBX.*

```
set modem_group all access two_way

add network service dialout_service server_type telnetd
socket 6000 data
auth=off,service_type=dialout,modem_group="all"

set dial_out security no

save all
```

### Example 2: Dial out using the first four modems

To enable dial-out for the first four modems on the RAS 1500, issue the following commands (line breaks added for readability):

```
add modem_group dialout_modems interface rm0/slot:1/mod:[1-4]

set modem_group dialout_modems access two_way

add network service dialout_service server_type telnetd
socket 6000 data
auth=off,service_type=dialout,modem_group="dialout_modems"

set dial_out security no

save all
```

**Configure Client Workstations**

Complete the following steps to install and configure DialOut/IP software on **each** of the client workstations from which you plan to dial out.

**Step 1: Install DialOut/IP Software**

- 1 Insert the Resource CD into the workstation.
- 2 Navigate to the ClientSoftware\Dial-out\Tactical directory.
- 3 Double-click Setup.exe. After a few seconds, the readme file appears.
- 4 Review the readme file.
- 5 Close the NotePad application. The License Agreement dialog box appears.
- 6 Review the license agreement, then click I Agree. The “Welcome” dialog box appears.
- 7 Follow the instructions on the screen. After several steps, the “Installation Completed” dialog box appears.
- 8 Click Finish. The Select Ports dialog box appears.

**Step 2: Create DialOut/IP COM Ports**

- 1 In the Select Ports dialog box, select the COM ports you want DialOut/IP to create. The list does not include COM ports that are in use.
- 2 Click OK. The COM ports are created. A dialog box appears.
- 3 Click Reboot Now. The workstation reboots.

**Step 3: Run the Configuration Wizard**

- 1 After the workstation reboots, a DialOut/IP icon appears in the lower-right corner of the Windows desktop.
- 2 Double-click the DialOut/IP icon. (To determine which icon is the DialOut/IP icon, hold the mouse pointer over each icon until you see “DialOut/IP...” in the pop-up window.) The Configuration dialog box appears; a list of the COM ports you selected before the reboot is on the left side of the dialog box.
- 3 In the list of COM ports, select the port you want to configure. You can configure only one port at a time.
- 4 Click Configuration Wizard. The Configuration Wizard dialog box appears.



- 5 In the Presets drop-down list, select "3Com RAS-1500." (You might need to scroll down the list.) The default TCP port number for the RAS 1500, 6000, is entered in the Port Number text box.
- 6 In the IP Address of Server text box, type the IP address of the RAS 1500.
- 7 If necessary, in the Port Number text box, type the TCP port number of the RAS 1500.
- 8 Click Start. DialOut/IP determines the correct settings for the COM port.
  - If the process finishes with no errors, click Use Settings to configure the selected COM port.
  - If the process finishes with errors, you must investigate and correct them before proceeding.
- 9 Repeat steps 3 through 8 for each COM port you want to configure.
- 10 Close the dialog box.

#### **Step 4: Add a Windows Dial-up Networking Connection**

- 1 Set up a Windows Dial-Up Networking connection using the DialOut/IP port you just configured.
- 2 Dial out through the connection.





# CONFIGURING TELNET NETWORK DIAL-OUT

This chapter contains the following information:

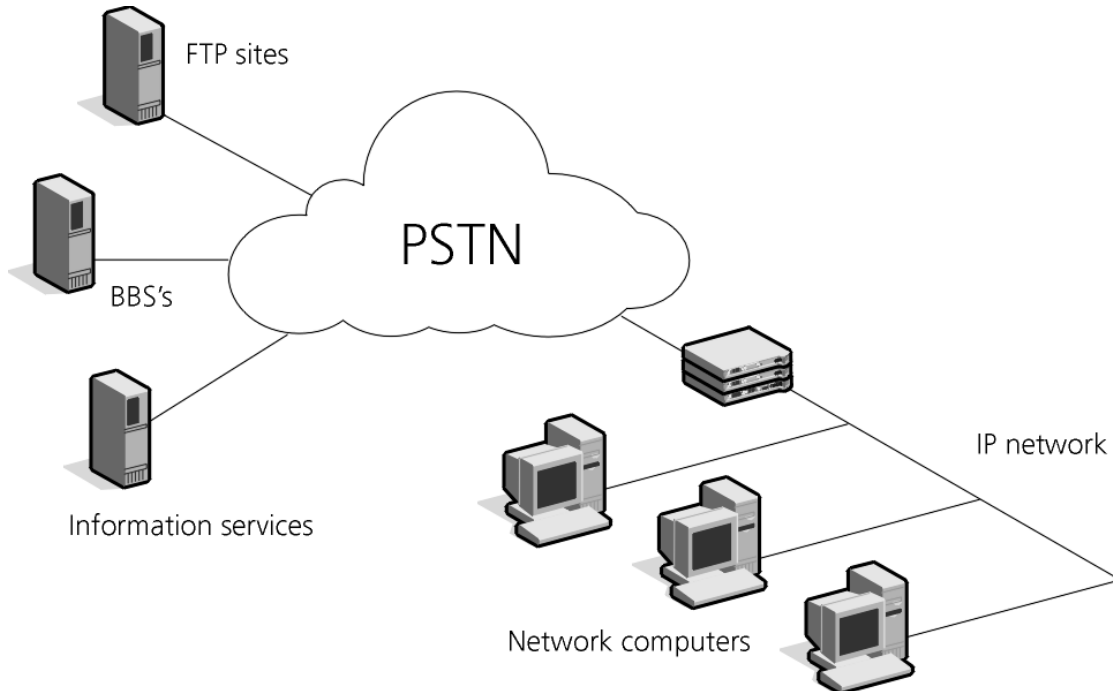
- Overview
- Before You Begin
- Configuring the RAS 1500
- Configuring Network Computers
- Dialing Out From a Network Computer
- Case Study

**Overview**

You can access modem ports on the SuperStack II Remote Access System (RAS) 1500 from computers on the network to provide dial-out services.

**Using Telnet Network Dial-out**

Network dial-out allows computers connected to the local area network (LAN) to access modems on the RAS 1500, as though the modems were directly connected to the computers. Once connected to a modem, a network user can dial out to the Internet, electronic bulletin board systems (BBSs), information services (such as CompuServe), ftp sites, and e-mail sites—anything that you could access with a modem directly connected to the computer. See Figure 7 for a diagram of Network dial-out over Telnet.



**Figure 7** Network Dial-out over Telnet

**DialOut/IP Versus  
Telnet**

Network computers communicate with the RAS 1500 over the LAN using either DialOut/IP or Telnet. A difference between DialOut/IP network dial-out and Telnet network dial-out is that DialOut/IP supports Windows Dial-Up Networking, and Telnet does not. So, if you need access to the Internet over a dial-up PPP connection, which Windows Dial-Up Networking provides, choose DialOut/IP network dial-out.

If you do not need to use Windows Dial-Up Networking, either method is acceptable, although Telnet is easier to set up.

This chapter details Telnet network dial-out. For details about DialOut/IP, refer to Chapter 4, "Configuring DialOut/IP".

**Configuring and  
Using Telnet Network  
Dial-out**

Complete the following steps to dial out from a network computer through a RAS 1500. Each of these steps is detailed later in this chapter.

- 1 Configure the RAS 1500.
- 2 Configure computers on the network.
- 3 Dial out from a computer on the network.

---

**Before You Begin**

Before you configure Telnet network dial-out, you need to obtain required information and optional information, based on your dial-out needs.

**Required Information**

The following information is required:

- System name of the RAS 1500
- Network service name
- IP address of the RAS 1500
- Network name
- At least one username and password

**Optional Information** The following information is optional:

- Modem group name
- Modems to include in the modem group
- Idle timeout
- Recovery timeout
- Login banner
- Login prompt

**RAS 1500  
Configuration**

Before you begin, confirm the following steps are complete, as detailed in the Getting Started Guide:

- The RAS 1500 hardware is successfully installed.
- An IP address is assigned to the RAS 1500.
- If necessary, the RAS 1500 ISDN ports are configured, including SPIDs, directory numbers, and switch type.

**Computers on the  
Network**

- Must have Telnet.

---

## Configuring the RAS 1500

To configure the RAS 1500 for Telnet network dial-out service, follow these steps. Each of these steps is detailed in this section.

- Step One: Add a System Name
- Step Two: Add an IP Network
- Step Three: Add a Modem Group (optional)
- Step Four: Add the Dial-out Service
- Step Five: Add Users
- Step Six: Save Your Work

### Notes about the procedures

The commands below are performed in the RAS 1500 command line interface (CLI). If you need assistance with accessing the CLI, refer to the *Getting Started Guide*.

You must press Enter to issue a command in the CLI. This step is not included in the procedures below.

### Step One: Add a System Name

The system name helps you identify the RAS 1500 during subsequent configuration. Use the following command to add a system name:

```
set system name <name>
```

**Table 6** RAS 1500 System Parameters

Parameter	Description
system name	Designation of the RAS 1500. This parameter cannot include spaces, and its maximum length is 64 characters.

Example:

```
set system name ras1500_lab
```

### Step Two: Add an IP Network

Essentially, this step gives an IP address to the RAS 1500, so it can be found on the LAN. Use the following command:

```
add ip network <IP network name>
      address <IP address>
```

**Table 7** IP Network Parameters

Parameter	Description
network name	Name of IP network. Unique ASCII string of up to 64 characters.
address	Address of the IP network. The RAS 1500 and the network computers must be on the same subnet of the LAN.

Example:

```
add ip network ipnet address 192.112.227.115
```

### Step Three: Add a Modem Group (optional)

By default, all modem ports on your RAS 1500 belong to a modem group named "all." But, you can create your own modem groups and assign modems to them. Modems can belong to more than one modem group.

When a network user requests the use of a modem group on the RAS 1500, the user is assigned the first available modem from that group. If all modems in the group are being used, the RAS 1500 sends a message to alert the user. Users can either re-submit the request for a modem or select another modem group.

Configure modem groups by specifying the interfaces that you want to belong to the group:

```
add modem_group <group_name>
      interface <modem slot/modem port>
```

**Table 8** Modem Group Parameters

Parameter	Description
modem group name	Name of the modem group. You should limit the length of this name to eight characters. That ensures the name always displays completely in list and show commands. The maximum length is 64 ASCII characters.
modem slot/port	List of interfaces to be assigned to the modem group. The format is module/slot/modem. A comma separates each interface.



For example, to add a modem group called `Telnet_users` with three modems assigned to it:

```
add modem_group telnet_users interface
rm0/slot:1/mod:1,rm0/slot:1/mod:2,rm0/slot:1/mod:3
```



*After you create the modem group, you assign it to the dial-out service (in step four). The modem group you assign in that step must match exactly (case-sensitive) with the modem group you create in this step.*

### Step Four: Add the Dial-out Service

- 1 Add the Telnet dial-out service. Use the following command:

```
add network service <service name>
    server_type <server type>
    socket <socket number>
    data <ancillary data>
```

**Table 9** Network Service Parameters

Parameter	Description
<code>network service name</code>	Name of the service. Limit: 64 ASCII characters.
<code>server type</code>	Designates the type of service, which in this case is <b>telnetd</b> .
<code>socket number</code>	Port on which the server monitors for activity. This parameter should be higher than 1024 to avoid conflicts with existing socket numbers.

**Table 9** Network Service Parameters

Parameter	Description
ancillary data	<p>This field contains server-specific configuration data. You can set the following:</p> <p><code>service_type &lt;service type&gt;</code>, which in this case is <b>dialout</b>. This parameter is required.</p> <p><code>modem_group &lt;modem group&gt;</code>, which defines the modem group this service uses. This parameter is optional. For example, <b>modem_group telnet_users</b></p> <p>If you do not enter this command, the network service uses the default modem group, <i>all</i>, which includes all of the modems on the RAS 1500.</p> <p>Important: You cannot assign more than one modem group to a DialOut/IP network service.</p> <p><code>auth=&lt;on/off&gt;</code>, which indicates whether a dial-out user is required to login. This parameter is optional.</p> <p>If you do not want dial-out callers seeking authentication, add <code>auth=off</code> to the DATA value of the network service (<code>auth=on</code> is the default). In this case, do not add a user when setting <code>auth=off</code>.</p> <p><code>login_banner="string,"</code> which is sent to a client when a connection is made. This parameter is optional.</p> <p><code>login_prompt="string,"</code> which is sent during authentication. This parameter is optional.</p> <p>Note: Adding control characters <code>\r\n</code> to banners or prompts puts a carriage return after the string.</p>

Example:

```
add network service telnet_lab server_type telnetd socket
6666 data "service_type=dialout
```

This example makes available modem ports assigned to the modem group `telnet_users` (modems 1-3).

- 2 Confirm the dial-out service is enabled. Use the following command:

```
list network services
```

A list of network services appears. Confirm Admin Status is enabled for the dial-out service you added. If it is disabled, repeat step 1.

## Changing a dial-out service

To change dial-out service settings:

- 1 Disable the dial-out service.

```
disable network service <service_name>
```

- 2 Make the changes to the dial-out service.

```
set network service <service name>  
  data <ancillary data>
```



*All DATA parameters are lost when you issue the set network service command. So you must re-enter all options in the DATA field.*

- 3 Enable the network dial-out service

```
enable network service <service_name>
```

Example:

```
enable network service telnet_lab
```



*You cannot change the service name using the set network service command. To change the service name, you must delete the network service using the delete network service command and add it again using the add network service command.*

## Step Five: Add Users

Create at least one dial-out user. Use the following commands to add a username, type (passwords optional), and modem group. Remember to specify a modem group *exactly* matching the modem group you specified earlier.

```
add user <name>  
  password <password>  
  type dialout
```

**Table 10** User Parameters

Parameter	Description
<code>username</code>	Name of user, up to 64 ASCII characters.
<code>user password</code>	Password of the user.
<code>user type</code>	Type of user. A user can be more than one type, but for Telnet dial-out, these types must include dial-out. <ul style="list-style-type: none"> <li>■ Login</li> <li>■ Network</li> <li>■ Callback</li> <li>■ Dial-out</li> <li>■ Manage</li> </ul>
<code>modem group name</code>	Name of modem group used to make the dial-out connection. This parameter is optional.

Example:

```
add user gil password fish type dial_out
set user gil modem_group telnet_users
```

### Step Six: Save Your Work

Use the following command:

```
save all
```

## Configuring Network Computers

Confirm Telnet is installed on each of the network computers (as noted in “Before You Begin” on page 59).

---

## Dialing Out From a Network Computer

- 1 From the Windows 95 or NT desktop, click *Start*, then *Run*. The Run dialog box appears.
- 2 In the Open text box, enter the following:  

```
telnet <ip address of the RAS 1500> <socket number>
```

Example:  

```
telnet 192.112.227.115 6666
```
- 3 Click *OK*. The Telnet application is launched.
- 4 At the login prompt, type the user name, then press *Enter*.
- 5 At the password prompt, type the user password, then press *Enter*. The RAS 1500 authenticates the user.
- 6 At the command prompt, issue **AT** commands to the modem.

---

## Case Study

This section provides a step-by-step example of configuring the RAS 1500 and network computers for Telnet dial-out.

A user on the network, Eddie, wants to dial out through the RAS 1500 using Telnet.

This example assumes the following:

- Eddie uses a Windows 95 computer.
- Analog I/O cards are installed in the RAS 1500.
- All basic system and network configuration is complete.

To configure network dial-out service, follow these steps:

- 1 Access the RAS 1500 CLI.
- 2 Name the system "ras1500\_north." Use the following command:  

```
set system name ras1500_north
```
- 3 Specify an IP network named "ipnetwork" with an IP address of 149.112.152.195. Use the following command:  

```
add ip network ipnetwork address 192.112.227.110
```
- 4 Add a modem group named "telnet\_lan" that uses modems 1 and 2 on slot 0. Use the following command:

```
add modem_group telnet_lan interface
rm0/slot:1/mod:1,rm0/slot:1/mod:2
```

- 5 Add a dial-out user named "eddie" with a password "panama." Use the following command:

```
add user eddie password panama type dial_out
```

- 6 Add a Telnet network dial-out service named "telnet" with these characteristics: socket number 6666 and a modem group "telnet\_users." Use the following command:

```
add network service telnet server_type telnetd socket 6666
data service_type=dialout,modem_group=telnet_users
```

- 7 Save your work. Use the following command:

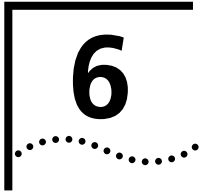
```
save all
```

- 8 On the network computer, launch Telnet and access the RAS 1500. From the Windows 95 desktop, click *Start*, then *Run*. In the Run dialog box, enter the following: **telnet 192.112.227.110 6666**. Click *OK*.

- 9 Log in to the RAS 1500. At the login prompt, enter the following: **eddie**  
At the password prompt, enter the following: **panama**

- 10 Issue an AT command to dial. Use the following command:

```
atdt918475551212
```



# 6

## CONFIGURING NETWORK DIAL-IN

This chapter contains the following information:

- Overview
- Before You Begin
- Configuring the Remote Computer
- Configuring RAS 1500
- Using Callback and Roaming Callback
- Calling Line Identification Callback
- Network Callback User Case Study
- Network User Case Study

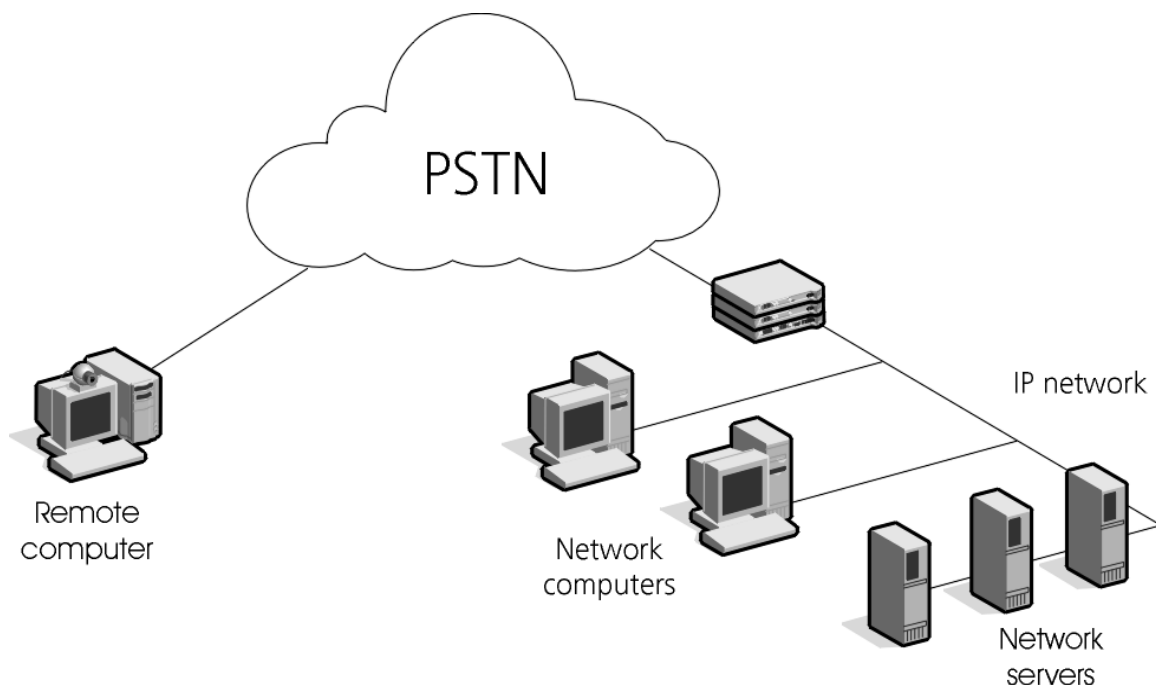
## Overview

SuperStack II Remote Access System (RAS) 1500 allows remote computer and Macintosh users to dial in over ISDN or analog lines and connect to the local network via Novell IPX, Internet Protocol (IP), or AppleTalk.

### Using Network Dial-In

Use network dial-in (Figure 8) if you want to configure a RAS 1500 to allow dial-in users to do the following:

- Access network servers (such as e-mail)
- Access the Internet
- Access bulletin board systems
- Access UNIX hosts
- Remotely access your RAS 1500



**Figure 8** How Network Dial-In Works



---

**Before You Begin**

Before you begin configuring RAS 1500 for Network Dial-in, follow all the configuration steps in the *SuperStack II Remote Access System Getting Started Guide*.

**Required Information**

Obtain the following information for network dial-in:

- Dial-in phone numbers
- Usernames and passwords
- The number of IP addresses needed
- How you want RAS 1500 to assign IP addresses

---

**Configuring the Remote Computer**

Remote users must have a modem supporting the remote access protocol used (Point-to-Point Protocol [PPP] or Serial Line Internet Protocol [SLIP]).

**Requirements**

Provide the remote RAS 1500 dial-in user with the following:

- Username and password
- Telephone number to access RAS 1500

**Communications Software**

Provide the remote computers with the correct communications software:

- Dial-up Adapter to connect to PPP and RAS 1500
- TCP/IP Dial-up Adapter to connect to the Internet and Wide Area Networks (WANs)
- Client for Microsoft Networks to connect to other Windows computers and servers

**Communication Parameters**

Provide the remote computer with the correct communications parameters:

- 8 bits, no parity, and 1 stop bit
- Hardware (RTS/CTS) flow control
- Normal Carrier Detect



*These are default communication parameters. If you change the RAS 1500 communications settings, you must provide the remote user with the appropriate settings.*

**IP Addresses** You may specify an IP address for your remote computer during the session. If RAS 1500 is configured to negotiate an IP address with the remote computer, RAS 1500 automatically detects this address.



*If the remote computer does not have an IP address configured and the address selection type is negotiate, RAS 1500 terminates the call.*

---

## Configuring RAS 1500

You need to perform the following actions to configure RAS 1500 for network dial-in:

### Required Steps

- 1 Configure IP address pools.
- 2 Configure IP network users.

### Optional Steps

- 3 Configure PPP parameters for network users.
- 4 Configure additional dial-up parameters.

## IP Address Pool Overview

RAS 1500 has an option to dynamically assign IP addresses to dial in network users from a pool each time they connect. This is done on RAS 1500 by configuring IP address pools.

RAS 1500 bundles several IP addresses into one to limit Routing Information Protocol (RIP) advertisements. The IP pool is created as a range, starting from an initial address. As PPP users dial in, IP allocates addresses from this pool and assigns them to users.



*Users assigned to more than one pool receive an address from the last assigned pool in round-robin fashion. As a safeguard, if the administrator reduces the size of the pool, users who are deleted will not be denied access until after their calls have terminated.*

## Step One: Configure an IP Address Pool

Use the following steps to configure an IP address pool:

- 1 Designate an IP address pool name and initial pool address. Use the following command:

```
add ip pool <name> initial_pool_address
<initial_pool_address>
```

Example:

```
add ip pool kurtspool initial_pool_address 172.32.142.2
```



*Do not overlap the ip addresses of the IP address pool and DHCP pool.*

- 2 Configure the size of the IP address pool. Use the following command:

```
set ip pool <name> size [1-4096]
```

Example:

```
set ip pool kurtspool size 24
```

- 3 Configure the state of the IP address pool. Use the following command:

```
set ip pool <name> [public |private]
```

**Table 11** IP Pool Access

User Type	Parameter
All users	public
Specific users	private

Example:

```
set ip pool kurtspool public
```

- 4 Configure the IP address pool route.

**Table 12** RAS 1500 Routing Table Actions

RAS 1500 Action	Parameter
Add a network route to the Routing Table immediately, and advertise it as a single network route.	aggregate
Add a network route to the Routing Table only when a user dials into that IP address pool. (default)	no_aggregate

Use the following command:

```
set ip pool <name> route [aggregate | no_aggregate]
```

Example:

```
set ip pool kurtspool route aggregate
```

## Step Two: Configure IP Network Users

A remote access user is as a network user. When you create a network user, the software builds a user profile that includes many default parameters. These defaults reflect most common types of user configurations. As a result, you may only need to change a few parameters from the default settings.



*When you add a network user, RAS 1500 enables the IP protocol by default.*

Use the following steps to configure an IP user:

- 1 Add a standard network user, specifying the user's name, user type, and network service type.



*Callback and dial\_out user types are mutually exclusive.*

**Table 13** Network User Types and Parameters

User Access Type	Parameter
CLI with full administrative privileges	manage
Login or network services	network, login
Login or network services (calls user back)	network, login, callback
Network services (calls user back)	network, callback
Network services at a remote site	network, dialout
Network services	network

Use the following command:

```
add user <name> password <password>
    type [network | login | callback | dialout | manage]
    network_service [slip | ppp | fcp | arap | fr_1490]
```

Example:

```
add user kurt password chicago type network,login
network_service ppp
```



*IP users can use SLIP or PPP as their remote access protocol, but SLIP is not supported for network users using the negotiate address selection method.*

For example, to add a network/manage user using PPP over IP, use the following command:

```
add user gina type network,manage network_service ppp
```

- 2 Specify a Remote Address. If you want the remote IP address to be selected from a pool or negotiated, go to step 3. When adding a remote IP address, RAS 1500 automatically chooses the specified address selection method, so you do not need to configure the parameter in the command.

Use the following command:

```
set network user <name> remote_ip_address <ip_address>
```

Example:

```
set network user gina remote_ip_address 195.114.123.16
```

- 3 Set the Address Selection Method. If the network user's address is not specified, define whether the RAS 1500 assigns or negotiates remote IP addresses.

**Table 14** IP Address Selection

Selection Method	RAS 1500 Action
assign	Configures an IP address based on the configured IP address pools.
negotiate	Attempts to learn the remote computer IP address using IPCP address negotiation. If the remote computer does not have a configured IP address, RAS 1500 disconnects the user.  This works with PPP connections only.
specified	Provides a fixed address.



*SLIP is not supported for network users employing this method.*

Use the following command:

```
set network user <name> address_selection [assign | negotiate  
| specified]
```

Example:

```
set network user gina address_selection negotiate
```

- 4 Save your work.

```
save all
```



*For most configurations, additional setup is not required. If you are an advanced user, read steps three and four and determine if you need to perform advanced configuration or PPP configuration.*

### Step Three: Configure PPP Parameters

If your remote users connect using PPP, you can also define several optional PPP parameters that control how RAS 1500 handles the remote access session.



*This section describes parameters that are applicable for network dial-in users. Many of the configurable PPP parameters are more often used for LAN to LAN routing users only. However, channel decrement, channel expansion, and max channels parameters can all be configured for callback users to employ bandwidth allocation.*

- 1 Configure PPP compression algorithm type. Use the following command:

```
set network user <name> ppp compression_algorithm [ascend |
auto | microsoft | none | stac]
```

Example:

```
set network user tom ppp compression_algorithm stac
```

- 2 Configure the PPP expansion algorithm type.

**Table 15** PPP Bandwidth Measurements and Parameters

Measurement	Parameter
Long-term bandwidth changes.	constant
More current, higher weight traffic when allocating bandwidth.	linear

Use the following command:

```
set network user <name> ppp expansion_algorithm [constant |
linear]
```

Example:

```
set network user tom ppp expansion_algorithm constant
```

- 3 Configure the PPP minimum size compression value. Use the following command:

```
set network user <name> ppp min_size_compression [value from
0-2048]
```

Example:

```
set network user tom ppp min_size_compression 256
```

- 4 Configure if RAS 1500 uses the asynchronous control character map to filter incoming data. Use the following command:

```
set network user <name> ppp receive_acc_map [hex_number -
array of 4 bits]
```

Example:

```
set network user tom ppp receive_acc_map 0
```

- 5 Configure if RAS 1500 uses the asynchronous control character map to filter outgoing data. Use the following command:

```
set network user <name> ppp transmit_acc_map [hex_number -
array of 4 bits]
```

Example:

```
set network user tom ppp transmit_acc_map 0
```

- 6 Configure how often PPP should examine packets to decide when to renegotiate the optimum compression algorithm.

**Table 16** PPP Packet Actions and Parameters

PPP Action	Parameter
Renegotiate the entire PPP session if RAS 1500 does not negotiate a PPP session	auto
Examine every packet	every_packet
Examine a packet every time PPP detects an error	every_error

Use the following command:

```
set network user <name> ppp reset_mode_co [auto |
every_packet | every_error]
```

Example:

```
set network user tom ppp reset_mode_co auto
```

- 7 Configure the ML-PPP channel values. Use the following commands:

```
set network user <name> ppp channel_decrement [0-100]
set network user <name> ppp channel_expansion [0-100]
set network user <name> ppp max_channels [0-8]
```

Example:

```
set network user tom ppp channel_decrement 20
set network user tom ppp channel_expansion 60
set network user tom ppp max_channels 1
```

- 8 Save your work.

```
save all
```

#### Step Four: Configure Additional Parameters

You can configure several additional network user parameters. Use the following steps to configure additional parameters:

- 1 Configure the Maximum Transmission Unit (MTU).



*MTU is the largest packet size (in bytes) RAS 1500 accepts. The default setting is 1514 for PPP and SLIP, although the maximum MTU SLIP accepts is 1006. PPP connections negotiate the MTU while SLIP connections do not.*

Use the following command:

```
set network user <name> mtu <number>
```

Example:

```
set network user tom mtu 1006
```

- 2 Configure PAP/CHAP authentication.

By default, RAS 1500 is configured globally to use either the Password Authentication Protocol (PAP), or Challenge-Handshake Authentication Protocol (CHAP) for PPP connections.

The default setting is *either*. When a user dials in, RAS 1500 first tries to authenticate the user using CHAP. If the remote computer does not respond, RAS 1500 attempts to use PAP. If the remote computer doesn't respond, the connection is dropped. Change the authentication setting by typing:

```
set ppp receive_authentication [chap | pap | either | none]
```

Example:

```
set ppp receive_authentication chap
```

- 3 Configure callback phone numbers. Callback phone numbers only work when a user is configured as a callback user.



*These phone numbers do not apply to other dial-in users.*

```
set user <name> phone_number <number>
```

```
set user <name> alternate_phone_number <number>
```

Example:

```
set user tom phone_number 555-1234
```

```
set user tom alternate_phone_number 555-5678
```



- 4 Configure idle and session timeouts to limit a user's time on the line or end a call after a specified idle period:

```
set user <name> idle_timeout <0-86400 seconds>
session_timeout <0-86400 seconds>
```

Example:

```
set user tom idle_timeout 60000 session_timeout 60000
```

- 5 Save your work.

```
save all
```

---

## Using Callback and Roaming Callback

**Overview** There are two types of callback: normal and dynamic.

### Normal Callback

Normal callback allows your users to dial-in to RAS 1500, hangup, and have the RAS 1500 call you back at a preconfigured phone number.

### Dynamic callback

Dynamic callback or Roaming callback allows your users to dial into your SuperStack II Remote Access 1500, prompts for the callback number, hangs up, and negotiates the number to be called back.

## Configuring Callback Users

You can use the SuperStack II Remote Access 1500 to call back users.

### Configuring a Normal Callback User

Use the following steps to configure a normal callback user:

- 1 Add a callback user:

```
add user [username] password [password] type network, callback
set user [username] callback_type normal
```

- 2 Set the callback user phone number:

```
set user [username] phone [phone number]
set user [username] alt_phone [phone number]
```

- 3 Save your work.

```
save all
```

### Configuring a Roaming Callback User (Dynamic)

Use the following steps to configure a roaming callback user:

- 1 Add the roaming callback user.

```
add user [username] password [password] type network, callback
```

- 2 Set the roaming callback user as “dynamic.”

```
set user [username] callback_type dynamic
```

- 3 Save your work.

```
save all
```

---

## Calling Line Identification Callback

This section contains the following information:

- Overview
- Configuring CLID Callback
- Troubleshooting CLID Callback
- Case Study

### Overview

Using Calling Line Identification (CLID) callback, the RAS 1500 dials back a remote dial-in user based on the user's Automatic Number Identification (ANI).

Benefits of callback over dial-in:

- Cheaper (in certain cases). Provides lower-cost connections when the calling party's tariffs are higher than the service provider's tariffs.
- More secure. Provides additional security because remote users must be contacted at a phone number maintained at the service provider.

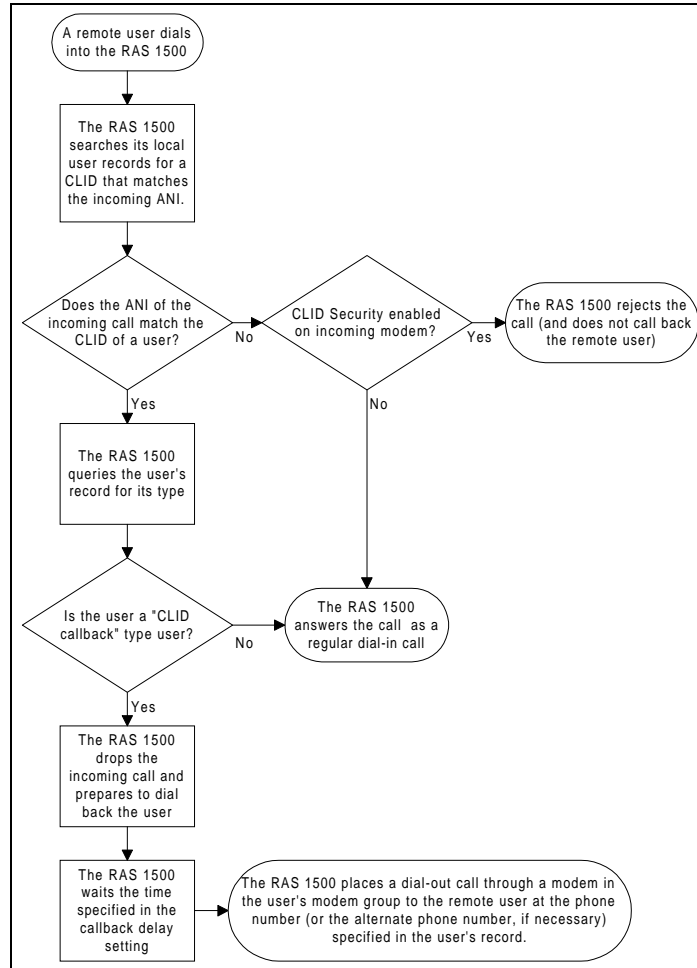
Benefits of CLID callback over PPP callback:

- Cheaper. The remote user is not charged for initiating the CLID callback because the remote user ANI information is transmitted before a connection is established (via the D channel). To initiate a PPP callback, the remote user must connect and, therefore, be charged.
- Easier. It is easier for remote users to use because the callback number is provided by the network, not the remote user.

Restrictions of CLID callback:

- CLID callback only works with the RAS 1500 for LAN-to-LAN connections.
- CLID callback does not provide “roaming” callback; PPP callback does.
- The RAS 1500 supports only CLID callback for ISDN users, not analog users.
- The RAS 1500 supports only CLID callback for local users, not Network Operating System (NOS) and Remote Authentication Dial-In User Service (RADIUS) users.
- Microsoft Windows Dial-Up Networking does not support the RAS 1500's implementation of CLID callback, in which the remote user does not initially connect to the RAS 1500 and is not charged.

**Call Handling** Figure 9 details the CLID callback/security process.



**Figure 9** CLID Callback Process

After the system determines whether the incoming call ANI matches a user CLID, the handling of an incoming call is determined by two settings: the status of CLID security (a modem-level setting) and the incoming user type (a user-level setting). These two settings are configured independently. Use the following table to decide which combination best suits your situation.



*Because CLID security is “per modem” and user type is “per user,” more than one of these options may be used simultaneously on one RAS 1500.*

**Table 17** Combinations of CLID Security and User Type

Option 1 (Only CLID callback is possible)	CLID security ENABLED User type “CLID_callback”	If the ANI of the incoming call matches the CLID of the user, the user is called back  If the ANI of the incoming call does not match the CLID of the user, the call is rejected.
Option 2 (CLID callback <u>and</u> other types of calls are possible)	CLID security DISABLED User type “CLID_callback”	If the ANI of the incoming call matches the CLID of the user, the user is called back  If the ANI of the incoming call does not match the CLID of the user, the call is answered as a regular dial-in call.
Option 3 (CLID callback are not possible; other types of calls are possible)	CLID security ENABLED User type NOT “CLID_callback”	If the ANI of the incoming call matches the CLID of the user, call is answered as a regular dial-in call.  If the ANI of the incoming call does not match the CLID of the user, the call is rejected.
Option 4 (CLID callback is not possible; other types of calls are possible)	CLID security DISABLED User type NOT “CLID_callback”	The call is answered as a regular dial-in call.

For examples of these options, refer to the “Case Studies” section at the end of this chapter.

## Configuring CLID Callback

For most CLID-callback setups, three general steps must be completed to prepare the RAS 1500:

Step One: Add a CLID user.

Step Two: Configure the user CLID-callback settings.

Step Three: Configure CLID security.

Each of these steps is shown in detail below. In some cases, not all of the steps are necessary. See the “Case Studies” section for more specific examples.

### Step One: Add a CLID User

To add a new CLID callback user, use the following command:

```
add user [name] type clid_callback,[network and/or login]
```

For example,

```
add user schmidt type clid_callback,network
```

When issuing the **add** command for a `clid_callback` user, the **type** parameter must also include either “network” or “login” or both.

To modify an existing user to be a CLID user, use the following command:

```
set user [name] type clid_callback,[network and/or login]
```

For example,

```
set user johnson type clid_callback,network
```

When issuing the **set** command for a `clid_callback` user, the **type** parameter must also include either “network” or “login” or both.

### Step Two: Configure the User CLID-callback Settings

To configure a user for CLID callback, perform the following steps:

- 1 Set the user CLID numbers. Use the following command:

```
set user [name] caller_id1 [number 1] caller_id2 [number 2]
```

For example,

```
set user schmidt caller_id1 8475552100 caller_id2 8475552101
```

The parameter **caller\_id2** is optional.

Each CLID number must be unique, otherwise the RAS 1500 cannot determine which user to call back.

For CLID callback to function correctly, one of the CLID values must exactly match the value of the automatic number identification (ANI) of the incoming call. If CLID callback does not function correctly, refer to the “Troubleshooting CLID Callback” section, later in this chapter.

- 2 Specify the phone numbers at which the RAS 1500 calls back the remote user. The RAS 1500 attempts the alternate number if the primary number is unavailable. Use the following command:

```
set user [name] phone_number [primary phone number]
set user [name] alternate_phone_number [alternate phone number]
```

For example,

```
set user schmidt phone_number 8475552100
set user schmidt alternate_phone_number 8475552101
```



*CLID callback and PPP callback use the same dial-back phone numbers.*

- 3 Set the length of time, in seconds, the RAS 1500 waits to call back the user. Use the following command:

```
set user [name] callback_delay [seconds of delay]
```

For example,

```
set user schmidt callback_delay 10
```

The default setting, which is pulled from the user named “default,” is 30 seconds. To change the **callback\_delay** parameter for the user named “default,” which changes the **callback\_delay** default for CLID users you add in the future, issue the following command:

```
set user default callback_delay [seconds of delay]
```



*CLID callback and PPP callback use the same callback delay.*

### **Step Three: Configure CLID Security**

CLID security provides an additional layer of security by rejecting calls from remote users whose ANI does not match the CLID of any user on the RAS 1500. The default setting is “off.”

CLID security is a modem-level setting. You can apply the setting to modems or modem groups.

To set CLID security for a modem:



*You can only configure modems one at a time. To configure multiple modems at the same time, use modem groups, below.*

```
set switched interface [interface name] clid_security [on | off]
```

For example,

```
set switched interface rm0/slot:1/mod:1 clid_security on
```

To set CLID security for a modem group:

```
set modem_group [modem group name] clid_security [on | off]
```

For example,

```
set modem_group callback clid_security on
```

To show the settings of a particular modem:

```
show interface [interface name]
```

The status of “CLID Security” is at the end of the list.

For example,

```
show interface rm0/slot:1/mod:1
```



## Troubleshooting CLID Callback

Follow this procedure to obtain more information from the RAS 1500 about the CLID-callback process:

- 1 Set the log level of the RAS 1500:  
**set facility "Call Initiation Process" loglevel verbose**
- 2 Enable CLID security for one of the interfaces (for example, rm0/slot:1/mod:1):  
**set switched interface rm0/slot:1/mod:1 clid\_security on**
- 3 Dial from the remote user into the interface (in this case, rm0/slot:1/mod:1).
- 4 View the console (or syslog, if enabled). This displays a message that describes the incoming ANI and interface, which user, if any, matches the ANI, and the disposition of the call. If callback is enabled for the user, the call initiation messages begin after the callback delay expires.
- 5 Set the log level of the RAS 1500 back to its original setting:  
**set facility "Call Initiation Process" loglevel critical**

```
ras1500> add user fred type manage,clid_callback
ras1500> set user fred phone_number 384010 modem_group onest
ras1500> set user fred callback_delay 5
ras1500> set fac "Call Initiation Process" log verb
ras1500> set switched inter rm0/slot:2/mod:1 clid_security
off
ras1500> AT 05:42:41: Facility "Call Initiation Process"
Severity "VERBOSE": CIP: Call arrived request, id 2, was
accepted on interface rm0/slot:2/mod:1
```

```
ras1500> set switched inter rm0/slot:2/mod:1 clid_security on
ras1500> AT 05:44:23: Facility "Call Initiation Process"
Severity "VERBOSE": CIP: Caller ID 384010 on interface
rm0/slot:2/mod:1: No matching user. Call rejected.
```

```
ras1500> set user fred caller_id1 384010
ras1500> AT 05:45:00: Facility "Call Initiation Process"
Severity "VERBOSE": CIP: Caller ID 384010 on interface
rm0/slot:2/mod:1: User fred scheduled for callback.
AT 05:45:05: Facility "Call Initiation Process"
Severity "VERBOSE": CIP: Sent a dial request to the driver
for user fred @ 384010 on interface rm0/slot:2/mod:1
AT 05:45:29: Facility "Call Initiation Process"
Severity "VERBOSE": CIP: Login succeeded for
call id 0 on interface rm0/slot:2/mod:1 for user fred
```

**Case Study** A small office satellite provides dial-up connections to its at-home workers using the RAS1500. All the modems have CLID security enabled, and the user records have the caller ID fields set. This ensures the workers can dial in only from home. Additionally, on-demand networking is set up to call the main office's RAS1500. The main office user profile for the SOS has CLID callback set so that the main office calls the SOS back to reduce tariff charges for the LAN-to-LAN connection.

---

## Network Callback User Case Study

In this case study, a *network/callback* user is configured for the IP protocol. This user's IP address is *negotiated*, *phone* and *alternate phone numbers* provided, and *session* and *idle timeouts* specified.

**Assumptions** This case study assumes the following:

- A *Windows 95 Dial-Up Networking* connection was created, and *Network* settings were configured for the client.
- RAS 1500 uses the correct IP address and netmask.
- The IP network is configured.
- All other settings remain at factory defaults.

## How to Configure this User

Use the following steps to configure the user:

- 1 Add a user "Gina" of the *network/callback* type.

```
add user gina password 1234 type network,callback
```



*Because the default network service for network users is PPP, do not set the value.*

- 2 Enter phone and alternate phone numbers at which RAS 1500 calls Gina back.

```
set user gina phone 5085524438 alter 5085527867
```

- 3 Gina's home computer has an IP address configured on it. RAS 1500 detects this address by setting the address selection method to *negotiate*.

```
set network user gina address_selection negotiate
```

- 4 Add idle and session timeouts to limit Gina's time on the line.

```
set user gina idle_timeout 40000 session_timeout 40000
```

## 5 Save your work.

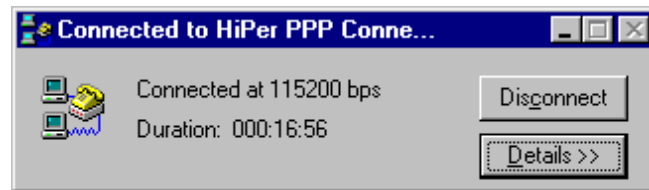
**save all**

**How it Works** Gina dials in to RAS 1500 using PPP (Dial-Up Networking) with the username and phone number supplied by the administrator. After Gina is authenticated, the call is disconnected and RAS 1500 dials Gina back at the phone or alternate phone number. Once reconnected, RAS 1500 attaches the user to the host or gateway specified in the Windows 95 Network dialog box from the Control Panel under Settings. If Gina exceeds the timeout periods, the call is disconnected.



*By default, RAS 1500 autodetects the authentication method the remote computer is using (CHAP or PAP). RAS 1500 first attempts CHAP, then PAP authentication. If the remote computer does not support one of these methods, RAS 1500 drops the call.*

If the PPP link to RAS 1500 succeeds, the message appears on Gina's screen as shown in Figure 10.



**Figure 10** Connection Message

---

## Network User Case Study

In this case study, a network user is configured for the IP protocol. This user's IP address is assigned by RAS 1500, and session and idle timeouts are specified.

**Assumptions** This case study assumes the following:

- A Windows 95 Dial-Up Networking session was made, and the client Network settings were configured.
- RAS 1500 uses the correct IP address and netmask.
- The IP network is configured.

- All other settings remain at factory defaults.

### How to Configure this User

Use the following commands to configure the user:

- 1 Create a network user “Bridgett” of the network user type. Use the following command:

```
add user bridgett password 1234 type network
```

- 2 Bridgett's home computer has no IP address configured on it. RAS 1500 assigns the IP address to authenticate. Since the address selection method is assign by default from an IP address pool, you need not configure the value. But you need to create an IP pool with an initial pool address.

```
add ip pool redsox initial_pool_address 177.143.045.9
```

- 3 Now that you have added the address pool, set its size, state, and route.

Example:

```
set ip pool redsox size 24 state public route no_aggregate
```

- `no_aggregate` (default) — IP addresses are not broadcast.
- `aggregate` — IP addresses are broadcast.

- 4 Add idle and session timeouts to limit Bridgett's time on the line.

```
set user bridgett idle_timeout 90 session_timeout 1800
```

- 5 Save your work.

```
save all
```

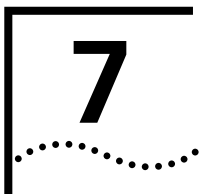
### How it Works

Bridgett dials into RAS 1500 using PPP (Dial-Up Networking) with the username and phone number supplied by the administrator. Bridgett is authenticated by PAP, and Windows prompts for a network login and the password. If approved, the user is connected to the host or gateway specified in the Windows 95 Network dialog box from the Control Panel under Settings. If Bridgett exceeds the timeout periods, the call is disconnected.



*By default, RAS 1500 autodetects the authentication method the remote computer is using (CHAP or PAP). RAS 1500 first attempts CHAP, then PAP authentication. If the remote computer does not support one of these methods, RAS 1500 drops the call.*

If the PPP link to RAS 1500 succeeds, the message appears on Bridgett's screen as shown in Figure 10.



# LAN-TO-LAN ROUTING

This chapter contains the following information:

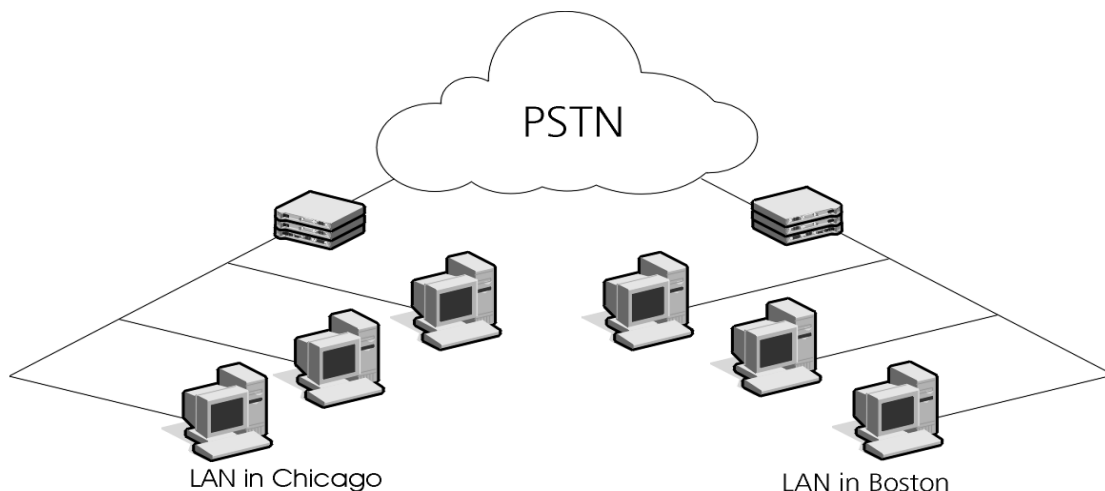
- Overview
- Before you Begin
- Configuring LAN-to-LAN Routing
- LAN-to-LAN Routing Case Study
- Configuring IP on Demand



*This chapter assumes that all routing devices have been installed and that both local area networks (LANs) have been properly configured.*

## Overview

The SuperStack II Remote Access System (RAS) 1500 can perform IP routing with a remote RAS 1500 or third-party router over analog or Integrated Services Digital Network (ISDN) digital lines (Figure 11).



**Figure 11** LAN-to-LAN Routing with the RAS 1500

### The Difference Between Bridging and Routing

Routing and bridging are very similar: they move packets between networks. When a packet arrives at a bridge or a router, the device uses tables to determine where the packet belongs.

A major difference between routing and bridging is the layer at which each works.

- Bridges use hardware address (Data Link layer) to determine the destination of the packet.
- Routers use network address (Network layer) to determine the destination of the packet.

This chapter discusses configuring the RAS 1500 for routing. For a discussion of bridging, refer to Chapter 8, "Bridging with the RAS 1500."

When a packet arrives at a router, the router analyzes the packet for the network address, such as an IP, IPX, or AppleTalk address.

## Routing Overview

Configuring a LAN-to-LAN routing connection is very similar to configuring a network user, with some additional dial-out and routing parameters such as:

- Types of LAN-to-LAN connection
- Routing configuration
- Dial-out scripts used to connect to the remote location
- Bandwidth (can be increased or decreased automatically)

The following sections give an overview of each parameter.

### LAN-to-LAN Connection Types

Table 18 shows the types of LAN-to-LAN connections you can establish.

**Table 18** Types of LAN-to-LAN Connections

Type	Status
On-Demand	This connection is established when a user attempts to access an address that is located at a remote site. The connection is closed after it has been idle for a specified interval.
Timed	The connection is opened and closed at a preset time.
Continuous	This connection is established by the system administrator and is always open, as long as the RAS 1500 is on-line.
Manual	This connection is established by the system administrator using a dial command.



*If system time is changed when timed connection user is enabled, the user must be disabled and re-enabled.*

### Routing Configuration

When the RAS 1500 connects to another router, periodic router updates, called RIP messages, allow routers to identify which networks are accessible. You can configure the RAS 1500 to send and receive these RIP messages on a per "user" (router) basis for the IP protocol. Enable routing if you want to use dynamic routing; the default value is *none*.

### Dial-Out Scripts

All dial-out users can have dial-out scripts defined in the user profile. The dial-out script can consist of up to six send/receive pairs. The script can contain AT commands and other login commands needed to access the remote location.



*The command providing this function (`set dial_out user`) overrides the phone number and alternate phone number values specified in the `set user` command.*

### Bandwidth Allocation with MLPPP

The RAS 1500 can provide variable bandwidth automatically, depending on the amount of traffic, with Multilink Point-to-Point Protocol (MLPPP).

Every five seconds, MLPPP samples network traffic. From these samples, the RAS 1500 calculates the percentage of channel utilization. If the percentage is higher than the expansion value you specify, the RAS 1500 brings up an additional B-channel. If, on a second sample, line usage drops below the decrement value you set, the RAS 1500 drops the additional B-channel. The sampling interval cannot be modified, but you can configure expansion and decrement thresholds to meet your system needs.

## IP Routing Overview

### Numbered and Unnumbered Interfaces

Either a numbered or an unnumbered interface can be used when setting up a wide area network (WAN) link. Using an unnumbered link helps conserve IP addresses. Using a numbered link requires unique IP addresses assigned to each side of the WAN link.

For an unnumbered link, the unnumbered interface may be associated with the IP address of, for example, the Ethernet interface of the router.

**Table 19** Interface Types and Defaults

Type	Default
unnumbered	the <code>rm0/eth:1</code> IP address of the RAS 1500. Using this interface saves IP addresses
numbered	the specification of an address for each end of the link



## **Dynamic, Static, and Default Routes**

You can configure the RAS 1500 to use constantly updated routing tables (dynamic routes that use protocols such as IP RIPv1 or RIPv2) or to use only your pre-configured routing tables (static routes).

### **Dynamic Routes**

Network devices running RIPv1 or RIPv2 broadcast the destination addresses to which they can forward packets. Other routers build routing tables by listening to the broadcasts of other devices that they are directly connected to.

If the RAS 1500 does not periodically hear a broadcast for a given route, the RAS 1500 assumes the route is unavailable and deletes it from the routing table.

### **Static Routes**

Static routes are user-defined. By adding entries to the Routes Table, you tell the RAS 1500 how to forward packets bound for specific networks rather than relying on RIP to dynamically learn the routes. If you have defined a static route to a given location, the RAS 1500 assumes you want to use that route and ignores dynamic routing broadcasts pointing to the same location. Static routes remain in the table until removed by the administrator.

### **Default Routes**

A default route is used to route to networks not specifically listed in the routing table. It can be used on routers that have just one connection to remote sites. It can be used as an alternative to using a dynamic routing protocol across a WAN link, if that is appropriate for the network topology.

## **How the RAS 1500 Routes Packets**

When the RAS 1500 receives a packet, it looks up the packet destination in the routing table. If a static route is found, the RAS 1500 send the packet to the gateway listed in the routing table. If the RAS 1500 does not find a static route, it uses a dynamic route that it learned from other routers. If the routing table contains no dynamic routes to the destination, it sends the packet to the specified default route gateway. If no such gateway has been defined, the RAS 1500 discards the packet.

### **Establishing Connections to Remote Gateways**

The RAS 1500 forwards a packet to a gateway for which there is an established connection, such as a gateway on the same segment of the local LAN or at the other end of an active dial-up connection. All the RAS 1500 does in these situations is send the packet out the correct interface.

However, when there is no existing connection, the RAS 1500 has to do more work. When you define a dial-out user in the RAS 1500 that is intended to connect to another routing device, the entry contains a list of remote gateways that the RAS 1500 can dial into. When the RAS 1500 does not have a connection to a packet's next hop, it looks up the address of the gateway in the user table. Dial scripts are most useful for on-demand routing sessions. In these situations, the RAS 1500 connects to a remote gateway only when it has packets queued for that location.

You can also create a default route gateway to reach a remote network your RAS 1500 is not aware of by manually specifying it.

### **Spoofing**

The RAS 1500 supports spoofing between another RAS 1500 or Total Control products. Spoofing is an inexpensive way to make two sides of a disconnected circuit believe that the connection still exists in order to limit network traffic and maintain the advantages of on-demand service. The RAS 1500 spoofs RIP broadcasts.

### **Authentication**

The RAS 1500 auto-detects Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) login authentication on Point-to-Point Protocol (PPP) links.



*The RAS 1500 also provides Remote Authentication Dial-In User Service (RADIUS) and network operating system (NOS) authentication support for PPP connections.*

#### **PAP Authentication**

PAP supplies a clear text password sought by the authenticating system. Although the RAS 1500 does not initiate dial-out PAP authentication, you can accomplish the same effect by creating a dial script containing the expected prompts and the required responses.

The RAS 1500 responds to a dial-in PAP authentication request, though. All you need is a User Table entry for the remote device.

## CHAP Authentication

Instead of actually sending a clear text password over the link, CHAP relies on a “shared secret,” a password that both sides of the connection know, but never send. When a remote system requests CHAP authentication, the authenticating host replies with a challenge packet. The challenge packet contains important information, including the following:

- Username for the host
- Challenge value

The challenged system needs the username for the host to look up the correct “shared secret” password. The “challenge value” is a randomly generated character string. The challenged system then concatenates the challenge value with the shared secret and passes the new string through a hashing algorithm. When the hashing algorithm has formed a response based on this string, the challenged system replies with a packet containing both the response value and a username.

The authenticating host looks up the correct password for the username received and then performs the same calculations the client performed, comparing the result to the response value received. If the results match, the RAS 1500 allows the challenged system to pass through. However, the authenticating host can issue additional CHAP challenges at any time during the connection.



*Both ends of the connection must be using the same hashing algorithm for the connection to succeed. The RAS 1500 uses the MD5 or MD4 Microsoft (Windows 95) algorithm.*

---

### Before you Begin

Before you configure the RAS 1500 for LAN-to-LAN routing, follow all the configuration steps in the RAS 1500 Getting Started Guide.

### Required Information

Obtain the following information:

- IP addresses and network masks
  - Local RAS1500 Ethernet port
  - Remote device Ethernet port
  - WAN link ports between the two devices
- Routing settings

- Local and remote LAN
- WAN link between the two devices
- Telephone numbers of each side of the connection
- Usernames and passwords used to identify each side to the other

---

## Configuring LAN-to-LAN Routing

Connecting to a remote LAN is similar to connecting to a remote user station (with the addition of a few more parameters); remote LANs are defined as users.

Use the following steps to configure a LAN-to-LAN routing connection:

- Step One: Add a LAN-to-LAN user
- Step Two: Configure the user network parameters
- Step Three: Configure the user dial\_out parameters
- Step Four: Configure the user routing parameters
- Step Five: Configure the user PPP parameters
- Step Six: Configure phone numbers
- Step Seven: Configure authentication
- Step Eight: Save your work

### Step One: Add the LAN-to-LAN User

To add a LAN-to-LAN user, use the following command:

#### 1 Add a user.

Add the user, password, user type "dial\_out,network," and enable the user.

Example:

```
add user main_office password boston type dial_out,network
enable yes
show user <username>
```

#### 2 (Optional) Set the idle timeout interval. Idle timeout specifies the time interval a dial-out connection can remain idle before the RAS 1500 disconnects the connection. RIP (with spoofing enabled) and keep-alive packets do not reset the idle timeout.

## Step Two: Configure the User Network Parameters

Configure network user with the following commands:

```
set network user <name>
    address_selection [specified | assign | negotiate]
    remote_ip_address <ip address>
    ip [enable | disable]
    ipx [enable | disable]
    appletalk [enable | disable]
    bridging [enable | disable]
    send_password <password>
    default_route_option [enable|disable]
    mtu <mtu size>
    spoofing [enable|disable]
```

- 1 Specify the type of address selection and remote IP address.

```
set network user <name>
    address_selection [specified | assign | negotiate]
    remote_ip_address <ip address>
```

**Table 20** address\_selection parameter

Configurable Address Type	Parameter
A specific remote IP address.	specified
When configuring a remote IP address, the RAS 1500 automatically sets address selection to specified.	
the RAS1500 to assign the remote link an IP address from a locally defined address pool.	assign
the RAS 1500 to automatically select the LAN address to be negotiated by IPCP.	negotiate

The `remote_ip_address` for a numbered link is the IP address of the dial-up port on the remote device. The `remote_ip_address` for an unnumbered link is the IP address associated with the unnumbered interface on the remote device to which this link is being configured (for example, the Ethernet port of the remote device).

Example:

```
set network user main_office address_selection specified
remote_ip_address 123.123.123.2
```

- 2 Specify the settings for ip, ipx, appletalk, and bridging.

```
set network user <name> ip [enable | disable] ipx [enable |
disable]
appletalk [enable | disable] bridging [enable | disable]
```

Disable the protocols that are not used across the dial-up link.

Example:

```
set network user main_office ip enable ipx disable appletalk
disable bridging disable
```

- 3 Specify the user send password, default route setting, MTU (maximum transmission unit) size, and spoofing status.

```
set network user <name>
    send_password <password>
    default_route_option [enable|disable]
    mtu <mtu size>
    spoofing [enable|disable]
```

The `send_password` is the password that is supplied by the RAS1500 when it is prompted for a password by a remote router that is authenticating it. It should match the password defined on the remote router for that identity.

When the default route option is enabled, a default route is added to the routing table with the gateway set to the user remote ip address as set on the local RAS 1500.

Example:

```
set network user main_office send_password mexico
default_route_option enable
mtu 1514 spoofing enable
```

### Step Three: Configure the User Dial-out Parameters

Use the following command to configure the user dial-out parameters:

```
set dial_out user <username>
    local_ip_address <ip address>
    site type <type of connection>
    site start_time <time 1>
    site end_time <time 2>
```

- 1 Configure the IP address and site type.

```
set dial_out user <username> local_ip_address <ip address>
site type <type of connection>
```

**Table 21**

Connection Type	Action
on demand	Initiation is automatic when valid/interesting data requires to traverse the link.
timed	Initiated and terminated automatically at preconfigured times.
manual	Initiated with the command "dial <username>".
continuous	Maintained constantly, as long as the RAS1500 remains powered on.

Example:

```
set dial_out user main_office local_ip_address 123.123.123.5
site type on demand
```



*Configure the local IP address if a you are going to use a numbered IP link. If you are using an unnumbered IP link, do not configure the local IP address.*

- 2 (Optional) Set the start and end time of a dial-out user session. These settings are only necessary if the connection type is timed.

```
set dial_out user <username> site start_time <hh:mm:ss>
end_time <hh:mm:ss>
```

Example:

```
set dial_out user main_office site start_time 13:00:00
end_time 14:00:00
```

### Step Four: Configure the User Routing Parameters

Use the following command to configure the user routing parameters:

```
set network user <username>
    ip_routing <level of routing>
    rip <rip version>
```

- Set general IP routing parameters.

```
set network user <username> ip_routing <level of routing> rip
<rip version>
```

**Table 22** IP Routing Levels

Command	RAS 1500 Action
Listen	Listens to RIP updates from the user and updates the local routing table
Send	Sends RIP updates to the user
Both	Listens to and sends RIP updates
None	Does not listen to or send RIP updates

Example:

```
set network user main_office ip_routing both rip ripv2
```

### Framed Routes

An alternative to using dynamic routing is to use framed routes. A framed route is a static route configured for the PPP user. A framed route is added to the routing table after the user connection is active. Until then, it is not visible in the routing table.

```
add framed_route user <username>
    ip_route <ip hostname/ip network address>
    gateway <hostname/station address>
    metric <value>
```

- Configure a framed route for a user.

```
add framed_route user <username> ip_route <ip hostname/ip
network address> gateway <hostname/station address> metric
<value>
```

Example:

```
add framed_route user main_office ip_route 123.123.123.15
gateway 123.123.125.12 metric 3
```



### Step Five: Configure the User PPP Parameters

Use the following command to configure the user PPP parameters:

```
set network user <username> ppp
    compression_algorithm <algorithm>
    max_channels <maximum number of channels>
    channel_expansion <at x percent load on current link>
    channel_decrement <at y percent load on current link>
    expansion_algorithm <linear or constant>
    min_size_compression <0-2047 bytes>
    reset_mode_compression <when to reset>
    receive_acc_map <accm>
    transmit_acc_map <accm>
```

#### 1 Configure basic PPP parameters.

```
set network user <username> ppp
compression_algorithm <algorithm>
max_channels <maximum number of channels>
channel_expansion <at x percent load on current link>
channel_decrement <at y percent load on current link>
```

**Table 23** User Types and Recommended Algorithms

User Type	Recommended Algorithm
Dial-in	AUTO (default)
Dial-out	Ascend, Microsoft, or STAC

The recommended compression algorithm for dial-in users is AUTO, which is the default value. The recommended compression algorithm for dial-out users is Ascend, Microsoft, or STAC.

PPP max\_channel value is "1" by default, which provides single-link PPP operation. If you want MLPPP operation (bandwidth on demand), increase this value.

The PPP `channel_expansion` and `channel_decrement` parameters are associated with MLPPP operation. When the utilization of the link reaches these values, either more links are made available (channel expansion) or links are removed (channel decrement).



*When MLPPP brings up additional links, the RAS 1500 uses the same number it brought up for the first link. Therefore, the destination to which the MLPPP connection is to be established should have its phone lines in a hunt group.*

Example:

```
set network user main_office ppp
compression_algorithm stac
max_channels 2
channel_expansion 60
channel_decrement 20
```

## 2 Configure optional PPP parameters.

```
set network user <username> ppp
expansion_algorithm <linear or constant>
min_size_compression <0-2047 bytes>
reset_mode_compression <when to reset>
receive_acc_map <accm>
transmit_acc_map <accm>
```

Example:

```
set network user main_office ppp
min_size_compression 256
reset_mode_compression auto
receive_acc_map 00000000
transmit_acc_map 00000000
```

### Step Six: Configure Phone Numbers

Use the following command to configure primary and alternate phone numbers:

```
set user <username>
    phone_number <number 1>
    alternate_phone_number <number 2>
```

The RAS 1500 attempts to dial the phone number when a connection is required. If the RAS1500 is unable to establish a link on this number, it attempts to dial the alternate phone number.

Example:

```
set user main_office phone_number 8715552020
alternate_phone_number 5088712022
```

### Step Seven: Configure Authentication

Use the following command to configure authentication settings:

```
set ppp receive_authentications <chap|either|none|pap >
set system transmit_authentication_name <remote_router_name>
```

The PPP receive\_authentication parameter determines how dial-in users are authenticated.

The system transmit\_authentication\_name is the name the RAS 1500 uses to identify itself to the remote router while setting up a dial-up LAN-to-LAN connection.

Example:

```
set ppp receive_authentications chap
set system transmit_authentication_name main_office
```

### Step Eight: Save Your Work.

Save your work.

```
save all
```

---

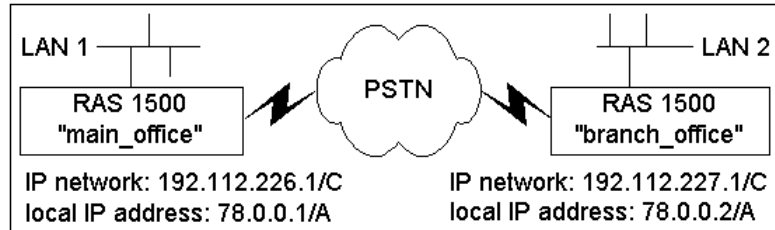
## LAN-to-LAN Routing Case Study

- Goals**
- Connect the "main\_office," the RAS 1500 that is on LAN 1, to the "branch\_office," the RAS 1500 that is on LAN 2. Use a LAN-to-LAN connection over a dial-up, on-demand, PPP link.
  - Increase the bandwidth when the load on the links increases.
  - Decrease the bandwidth when the load on the link decreases.
  - Authenticate using PAP.
  - Idle timeout should be 300 seconds.

- Assumptions**
- Each office has a functioning RAS 1500.
  - Each office has a separate IP network. The main office has 192.112.226.0/C; the branch office has 192.112.227.0/C.
  - Use the RIPv1 routing protocol.

**Strategies** The goals can be achieved in two ways: either a numbered IP link between the sites (see “Strategy 1 (numbered link)”), or an unnumbered IP link between the sites (see “Strategy 2 (unnumbered link)” on page 108).

### Strategy 1 (numbered link)



Configuring the RAS1500 in the Main Office.



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network ipnet-1 address 192.112.226.1/C interface
rm0/eth:1
```

- 2 Add a user.

```
add user branch_office password chicago type network,dial_out
set user branch_office idle_timeout 300
```



*Idle\_timeout must be a minimum of 180.*

- 3 Configure the user network parameters.

```
set network user branch_office address_selection specified
remote_ip_address 78.0.0.2/A
set network user branch_office ipx disable appletalk disable
bridging disable
set network user branch_office send_password boston
```

- 4 Configure the user dial-out parameters.

```
set dial_out user branch_office local_ip_address 78.0.0.1/A
set dial_out user branch_office site type ondemand
```

- 5 Configure the user routing parameters.

```
set network user branch_office ip_routing both rip ripv1
```

- 6 Configure the user PPP parameters.

```
set network user branch_office ppp max_channels 2
set network user branch_office ppp channel_expansion 60
channel_decrement 20
```

- 7 Configure phone numbers.

```
set user branch_office phone_number 5085555555
```

- 8 Configure authentication.

```
set ppp receive_authentication pap
set system transmit_authentication_name main_office
```

- 9 Save your work.

```
save all
```

Configuring the RAS1500 in the Branch Office:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network ipnet-2 address 192.112.227.1/C interface
rm0/eth:1
```

- 2 Add a user.

```
add user main_office password boston type network,dial_out
set user main_office idle_timeout 300
```

- 3 Configure the user network parameters.

```
set network user main _office address_selection specified
remote_ip_address 78.0.0.1/A
set network user main _office ipx disable appletalk disable
bridging disable
set network user main _office send_password chicago
```

- 4 Configure the user dial-out parameters.

```
set dial_out user main _office local_ip_address 78.0.0.2/A
set dial_out user main _office site type ondemand
```

- 5 Configure the user routing parameters.

```
set network user main _office ip_routing both rip ripv1
```

- 6 Configure the user PPP parameters.

```
set network user main _office ppp max_channels 2
set network user main _office ppp channel_expansion 60
channel_decrement 20
```

- 7 Configure phone numbers.

```
set user main_office phone_number 5085556666
```

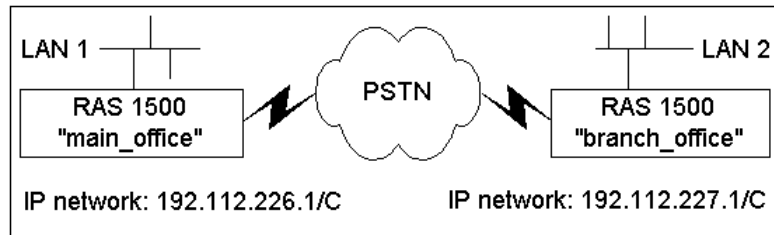
- 8 Configure authentication.

```
set ppp receive_authentication pap
set system transmit_authentication_name branch_office
```

- 9 Save your work.

```
save all
```

### Strategy 2 (unnumbered link)



Configuring the RAS1500 in the Main Office:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network ipnet-1 address 192.112.226.1/C interface
rm0/eth:1
```

- 2 Add a user.

```
add user branch_office password chicago type network,dial_out
set user branch_office idle_timeout 300
```

- 3 Configure the user network parameters.

```
set network user branch_office address_selection specified
remote_ip_address 192.112.227.1/C
set network user branch_office ipx disable appletalk disable
bridging disable
set network user branch_office send_password boston
```

- 4 Configure the user dial-out parameters.

```
set dial_out user branch_office site type ondemand
```

- 5 Configure the user routing parameters.

```
set network user branch_office ip_routing both rip ripv1
```

- 6 Configure the user PPP parameters.

```
set network user branch_office ppp max_channels 2
set network user branch_office ppp channel_expansion 60
channel_decrement 20
```

- 7 Configure phone numbers.

```
set user branch_office phone_number 5085555555
```

- 8 Configure authentication.

```
set ppp receive_authentication pap
set system transmit_authentication_name main_office
```

- 9 Save your work.

```
save all
```

Configuring the RAS1500 in the Branch Office:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network ipnet-2 address 192.112.227.1/C interface
rm0/eth:1
```

- 2 Add a user.

```
add user main_office password chicago type network,dial_out
set user main_office idle_timeout 300
```

- 3 Configure the user network parameters.

```
set network user main _office address_selection specified
remote_ip_address 192.112.226.1/C
set network user main _office ipx disable appletalk disable
bridging disable
set network user main _office send_password chicago
```

- 4 Configure the user dial-out parameters.

```
set dial_out user main _office site type ondemand
```

- 5 Configure the user routing parameters.

```
set network user main _office ip_routing both rip ripv1
```

- 6 Configure the user PPP parameters.

```
set network user main _office ppp max_channels 2
set network user main _office ppp channel_expansion 60
channel_decrement 20
```

- 7 Configure phone numbers.

```
set user main_office phone_number 5085556666
```

**8** Configure authentication.

```
set ppp receive_authentication pap
set system transmit_authentication_name branch_office
```

**9** Save your work.

```
save all
```

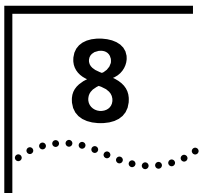
---

## Configuring IP on Demand

Using IP on demand, the RAS 1500 sends IP packets it receives to specified routers. Use the following steps to configure the RAS 1500 for IP on demand:

```
add user [username] password [password] type network,dial_out
network_service ppp enabled no
set network user [username] ip_routing both
set user [username] phone_number [phone number]
set user [username] alternate_phone_number [phone number]
set system transmit_authentication_name [authentication name]
set network user [username] send_password [password]
set network user [username] ppp_max_channels 2
add modem_group [modem group name] interfaces rm0/mod:[5-6]
set user [username] modem_group [modem group name]
set ip network [network name] routing_protocol ripv1
set network user [username] remote_ip_address [ip address]
set dial_out user [username] site type ondemand
set user [username] idle_timeout 60
set dial_out user [username] site spoofing enable
enable user [username]
save all
```





# BRIDGING WITH THE RAS 1500

This chapter contains the following information:

- Overview
- Enabling Bridging Over the LAN
- Using FCP to Bridge with OfficeConnect Routers

## Overview

The SuperStack II Remote Access System (RAS) 1500 uses bridging to allow you to link two separate locations as if they were the same network.

### How the RAS 1500 Acts as a Bridge

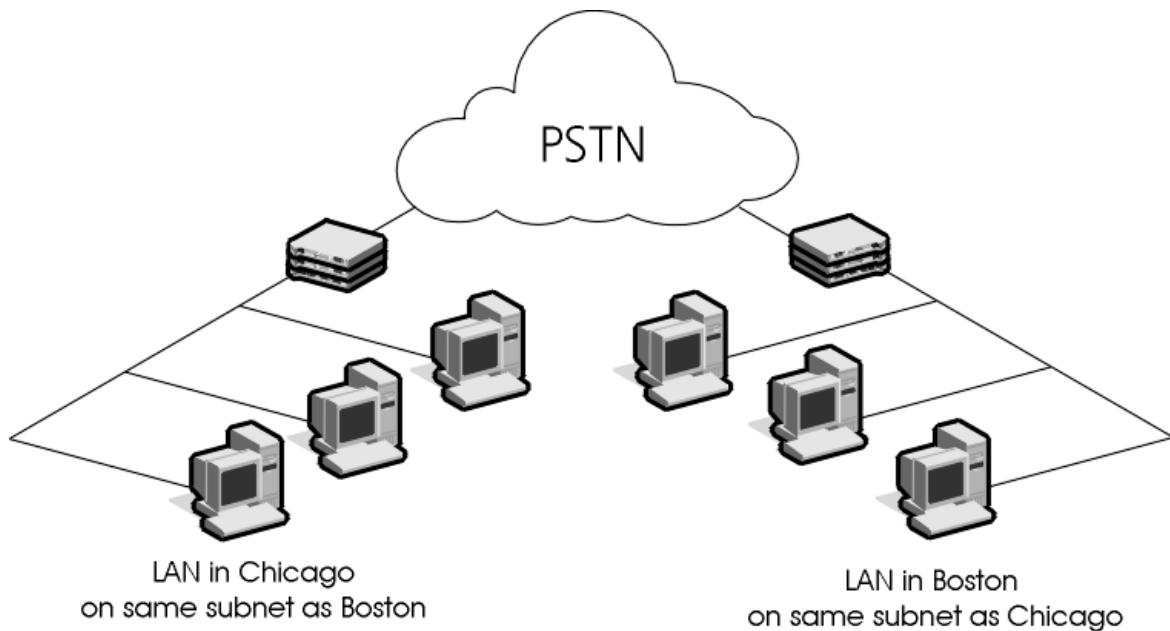
When the RAS 1500 receives a frame, it inspects the frame and determines where the frame belongs by analyzing address information.

**Table 24** Bridge Frames Destined for a Hardware Address

Location	RAS 1500 Action
Remote network	Places a phone call to the RAS 1500 connected to the other network and forwards the packet
Same network	Drops the packet

### When to Use Bridging

When a frame arrives at a bridge, the bridge analyzes the frame for the hardware address. Figure 12 shows an example of the RAS 1500 bridge configuration.



**Figure 12** Bridging with the RAS 1500

If the bridge does not find the destination hardware address in its bridging table, the RAS 1500 transmits the frame across the bridge.

If the bridge finds the destination hardware address in its bridging table, the RAS 1500 transmits the packet across bridge links.

**Bridging Tips** The following sections provide tips to help you understand bridging with the RAS 1500.

### Configuring PPP

To configure a bridge, you need to configure a bridge network, a user, and add Point to Point Protocol (PPP) support for that user.

### Enabling Bridging

The RAS 1500 specifies a protocol to bridge by disabling routing for that protocol. (Routing by default takes precedence over bridging.)

---

## Enabling Bridging Over the LAN

Use the following steps to enable bridging over the local area network (LAN):

- 1 Create a user. Use the following command:

```
add user <name> password <password> type network, dial_out
```

Example:

```
add user Boston password sayhey type network, dialout
```

- 2 Create a bridge network. Parameters for interface are optional because the RAS 1500 will choose the first LAN (rm0/eth:1) it finds in your system. The enable value is selected by default. Use the following command:

```
add bridge network <name> user <name>
```

Example:

```
add bridge network corporatenet user boston
```



*To verify bridge settings, use `show bridge network settings`.*

- 3 Configure network protocols you intend to bridge by editing the earlier created user profile. Because the RAS 1500 defaults to routing, if you want to bridge a particular protocol, disable routing for it. (Internet Protocol [IP], Internetwork Packet Exchange [IPX], AppleTalk, and bridging are enabled by default.)

3Com recommends that you route all protocols and bridge only the protocols that cannot be routed.

Use the command below:

```
set network user <name>
    ip [enable | disable]
    ipx [enable | disable]
    appletalk [enable | disable]
    ip_address [local IP address]
```

For example, to bridge IPX and AppleTalk protocols but route the IP protocol:

```
set network user Boston ipx dis appletalk disabled ip_address
201.191.15.5/c
```

- 4 For dialout specify the phone number and alternate phone number for dial-out using the following two commands:

```
set user <name>
phone_number <number>
alternate_phone_number <second number>
set network user <name>
    ppp channel_decrement <percent>
    ppp channel_expansion <percent>
```

- 5 Save your work.

```
save all
```

---

## Using FCP to Bridge with OfficeConnect Routers

The RAS 1500 gives you a choice of connection protocols: the PPP, ideal for Internet access as well as internetworking in mixed-vendor environments, and FastConnect Protocol (FCP) from 3Com.

FCP runs over LAPB, which is a flavor of High-level Data Link Control (HDLC).

## Using Fast Connect Protocol

FCP, which optimizes Integrated Services Digital Network (ISDN) links between the RAS 1500 and the OfficeConnect® family from 3Com, delivers nearly instantaneous ISDN link establishment.

By connecting more quickly, the RAS 1500 optimizes your performance and reduces your ISDN call charges.

FCP supports the following features:

- Data compression
- Multilink line aggregation (Multilink FCP)

### PPP Versus FCP

PPP is used widely throughout the IP community to connect routers from different manufacturers. It is recognized as the de facto standard protocol for this purpose. PPP can be used over both wide area network (WAN) and ISDN links. When using PPP, both ends of the link must be configured to use PPP.

While PPP is very flexible in terms of configuration, it is not as efficient in terms of speed of connection or throughput as FCP. However, if you need to connect to the Internet or to another manufacturer's router you will need to configure the unit to use PPP.

### How FCP Works

The following steps demonstrate how FCP works:

- 1 The RAS 1500 established the LAPB link as a part of the FCP negotiation.
- 2 Both sides of the link exchange Names and MAC addresses, negotiate compression (STAC), and reset the sequence numbers.
- 3 The RAS 1500 prepends data packets with a 2-byte sequence number.
  - a If you have a routed link, the routed packets are first prepended with a Ethernet MAC Header and then with the 2 byte sequence number.
  - b If you have a bridged link, the bridged packets already carry a MAC Header so only the 2 byte sequence number is prepended.
- 4 The RAS 1500 passes data packets to the LAPB link.



*An FCP link idles out if traffic on the link falls to configured idle threshold for the configured Idle period.*

### Configuring the RAS 1500 for FCP

Use the following steps to configure the RAS 1500 for FCP:

- 1 Define a modem group:

```
add modem_group 12 inter rm0/mod:[1-2]
```

- 2 Define the network settings:

- a Add the FCP user to the network:

```
add user [username] type network,dial_out network fcp
enable no
```

- b** Disable all protocols not used on your network:

```
set network user [username] ipx disable appletalk disable
```



*Bridging IP does not work if you add an IP network to the Ethernet interface.*

- c** Enable bridging for the FCP user:

```
set dial_out user [username] site bridge enable
```

- d** Configure FCP username and password:

```
set network user [username] send password
```

- e** Enable the user on the network:

```
add bridge network [username] interface rm0/eth:1 user  
[username] enable yes
```

- 3** Set dial-out settings for the user:

- a** Associate a user with the modem group:

```
set user [username] modem_group 12
```

- b** Set the user phone number:

```
set user [username] phone [phone number]
```

- c** Set the user alternate phone number:

```
set user [username] alternate [phone number]
```

- d** Add a bridge and associate a user with it:

```
set dial_out user [username] site type ondemand
```

- 4** Enable the user:

```
enable user [username]
```

- 5** Configure MultiLink FCP:

```
set network user [username] fcp max_channels 2
```

- 6** Configure compression settings:

```
set network user [username] fcp compression [STAC | None]
```

- 7** Save your work.

```
save all
```



*Compression is enabled by default in the user profile and no additional command needs to be issued, although there is a command that can be used in case compression is either required to be turned off or later turned on.*

**On-demand Bridging**

When the RAS 1500 receives a frame that needs to be bridged, it checks the learned MAC address table to see if it knows where to send the frame. (Maybe a dial-up link is still available where that can be forwarded.) If it does not know where to send it, it will cycle through the configured dialout bridging users bringing up their dial-up links and bridges the frame over to all these users.

**Configuring OfficeConnect for FCP**

See the documentation that shipped with your OfficeConnect product for configuration information.





# 9

## CONFIGURING AN IP TERMINAL SERVER

This chapter contains the following information:

- Overview
- Before You Begin
- Configuring the RAS 1500 Login Hosts
- Configuring Login Users
- Case Studies

---

### Overview

Remote users can dial in to the SuperStack II Remote Access System (RAS) 1500 to establish a terminal session with a host on the local network using a login service such as Telnet, Rlogin, or ClearTCP.

---

### Before You Begin

Before you begin configuring the RAS 1500 as an IP terminal server, follow all the configuration steps in the RAS 1500 *Getting Started Guide*.

### Configuring Remote Computers

The system administrator should provide the remote login user with the following information:

- A username
- A telephone number to dial into
- Login host address or name



*The RAS 1500 does not need passwords to connect to a network. For more security, add a password.*

### Setting Communication Parameters

The remote computer should be configured for the following communications parameters:

- 8 bits, no parity, and 1 stop bit
- Hardware (RTS/CTS) flow control
- Normal Carrier Detect



*These settings are the defaults. If you change the communications settings, you must provide the remote user with the appropriate settings as well.*

### Configuring the RAS 1500 Login Hosts

For a login host to be available to a login user, define it in the Login Hosts Table.



*To allow the user to access a login host using a host name, you must first configure a DNS server using the `add dns server` command.*

Example:

```
add dns server 7.7.7.7 name boston preference 1
```

To set up login host table entries, perform the following steps:

- 1 Configure the login hosts (up to 10 hosts).

```
add login_host <host_name>
  address <ip_address>
  preference <number>
  rlogin_port <TCP_port_number>
  telnet_port <TCP_port_number>
  clearTCP_port <TCP_port_number>
```

**Host Name** Name of the login host.

**Address** *Optional.* The IP address of the login host. If you do not specify an address, the RAS 1500 consults the DNS server to resolve the address.

**Preference** Priority ranking for the login host, from 1 (highest) to 10. The preference number must be unique for each host entry.

## Rlogin, Telnet and ClearTCP Ports

*Optional.* The Rlogin, Telnet and ClearTCP port numbers of the host.

- 1 To add a login host, use the following command:

```
add login_host detroit address 236.135.221.167 preference 1
```

- 2 Check your work with the following command.

```
list login_hosts
```

- 3 Save your work.

```
save all
```

---

## Configuring Login Users

Remote login users can use login services such as Telnet, Rlogin, or ClearTCP by dialing into the RAS 1500. Login users can connect directly, or be configured as callback users. (The RAS 1500 calls the user back at a phone number specified in their user profile.) You can setup the user for a specific login service to access a specific login host, or you can let the user determine the login service and login host.



*You can also specify login user information in RADIUS. When RADIUS authenticates a user, it can also pass on user configuration information to the RAS 1500.*

To configure a login user:

- 1 Add the user with the following command:

```
add user <name>  
    password [password]  
    login_service [rlogin | telnet | cleartcp | ping]  
    type [login | network | callback | dial-out | manage]
```

### Password

Passwords are optional.

### Login Service

Specifies the default login service. The default is Telnet. This parameter can be one of the following:

**Telnet** — Offered by most TCP/IP computers, Telnet lets users login to supporting hosts.

- **Rlogin** — Although Rlogin was originally a UNIX protocol, it is now supported by some non-UNIX machines as well. Unlike Telnet, Rlogin allows a user logged into a host to access their accounts on other (trusted) hosts without re-entering a password.
- **ClearTCP** — Unlike Telnet and Rlogin, ClearTCP is not actually a login service, it is a direct connection to a given TCP port number. Eight-bit data is exchanged without interpretation.



*The host type setting may override this setting. See step 2 for more information.*

### Type

The following are valid types for a login user:

- login
- login, callback

If you include callback in the user type, you need to specify a phone number at which the user is called back using the following command:

```
set user <name> phone_number <number>
```



*At this point, it may be helpful to use the **show user** command to display the user's default values. This lets you decide which parameters you need to set and which parameters you can leave as defaults.*

- 2 Configure login user parameters with the following command:

```
set login user <name>
  host_type [prompt | select | specified]
  login_host_ip_address <ip_address>
  login_service [rlogin | telnet | cleartcp | ping]
  tcp_port <port_number>
  terminal_type <string>
```

### Host Type

Determines how the user is connected to a login host. The default is *select*.

- **prompt** — If the user is prompted, this setting overrides login service setting. At the prompt, the user can enter the login service (for example, **Telnet**) and the host name or address, or type **connect** and enter host name or address to use the default login service.

- **select** — (*Default*) The user is automatically connected to a host selected from the Login Hosts Table. The method of choosing the host is set using the `set connection <host_select>` command by `random` or `round robin` (default) fashion.
- Example:  

```
set connection host_select random
```
- **specified** — The user is connected to the host specified in the `login_host_ip_address` setting.

### Login Host IP Address

If login user's host type is *specified*, you must enter the IP address for the host to be connected to.

### Login Service

Specifies the default login service. See step 1 for details.

### TCP Port

*Optional.* If the login host uses a TCP port number other than 23 (the default for Telnet), you can set the TCP port number using this command. For ClearTCP connections, make sure that the host's TCP port number matches the TCP port number you enter here.

### Terminal Type

*Optional.* Set the terminal type for the remote connection. The default is VT100.

## 3 Save your work.

```
save all
```

---

## Case Studies

This section provides examples of how to configure a login user to dial-in to the RAS 1500 and establish a Telnet session with hosts on the network.

- In Case Study A, the user is prompted for the login service and host address desired.
- In Case Study B, the user is connected directly to a host you designate.

Jack's home computer uses VT100 terminal emulation software to establish a IP terminal session with any host on the local area network (LAN) that he is authorized to access. In the first example, Jack uses Telnet to access the host named Quartz. In the second example, Jill uses rlogin to access the host name Granite

### Case Study A

This case study assumes the following:

- The user has set up a terminal emulation session such as the Windows HyperTerminal with a phone number and standard communications parameters.
- The IP network is configured.
- All other settings remain at factory defaults.
- A Domain Name System (DNS) server is configured.

Follow these steps to configure the login host and user:

- 1 Add a user "Jack" of the login user type.

```
add user jack type login
```

- 2 Add login hosts "Quartz" and "Granite" for Jack to access. You can prioritize the order these hosts are offered to him by setting the preference of Quartz to 1 and Granite to 2 so if Quartz is unavailable Jack will be able to access Granite. Use the following command:

```
add login_host quartz address 195.112.133.2 pref 1
add login_host granite address 195.112.133.10 pref 2
```

- 3 Configure Jack to be able to choose a login service and host name at the command prompt. Use the following command:

```
set login user Jack host_type prompt
```

- 4 Save your work.

```
save all
```

When Jack dials in, he is prompted for his login name as shown below:

```
Welcome to 3Com RAS 1500 (TM)
login:
```

After Jack is successfully authenticated, the system prompt appears. At this point, Jack can connect to either host by using the following command:

```
telnet quartz
```

or

```
telnet granite
```

Since Jack's default login service is Telnet, he could also enter the following command to connect to either host:

```
connect quartz
```

or

```
connect granite
```

Jack is connected to the host and prompted for a username/password.

```
Trying 195.112.133.2...
Connected to 195.112.133.2.
Hummingbird Communications Ltd., Telnet Daemon V5.1
Username: jack
Password:
```

```
Microsoft(R) Windows 95
(C)Copyright Microsoft Corp 1981-1995.
Quartz:\>
```

When Jack ends his host session, he is returned to the *RAS 1500*: prompt. He can access another login host, or he can exit the RAS 1500 by typing **exit**.

Example:

```
Quartz:\> exit
Connection refused.
RAS1500 exit
NO CARRIER
```

**Case Study B** This case study assumes the following:

- The user has set up a terminal emulation session such as the Windows HyperTerminal with a phone number and standard communications parameters.
- The IP network is configured.
- All other settings remain at factory defaults.
- A DNS server is configured.

Follow these steps to configure the login host and user:

- 1 Add a user "Jill" of user type login, login service of rlogin, and a password. Use the following command:

```
add user jill type login password hill login_service rlogin
```

- 2 Add a login host for Jill to access. Use the following command:

```
add login_host granite address 195.112.133.10 pref 1
```

- 3 Configure Jill to specifically access Granite. Use the following command:

```
set login user Jill host_type specified login_host_ip_address  
195.112.133.10
```

- 4 Save your work.

```
save all
```

When Jill dials in, she is prompted for a login name/password as shown below.

```
Welcome to 3Com RAS 1500 (TM)  
login:  
password:
```

After Jill is successfully authenticated, she is connected to the host and prompted for a username and password.

Example:

```
Trying 195.112.133.10...  
Connected to 195.112.133.10.
```

```
Hummingbird Communications Ltd., Telnet Daemon V5.1  
Username: jill  
Password:
```

```
Microsoft(R) Windows 95  
(C)Copyright Microsoft Corp 1981-1995.  
Granite:\>
```



After system authentication, Jill is up and running on the host.

When Jill logs out of her host session, she exits from the RAS 1500 as well.

Example:

```
Granite:\> logout
NO CARRIER
Microsoft(R) Windows 95
(C)Copyright Microsoft Corp 1981-1995.
Granite:\>
```



# 10

## ADVANCED MODEM CONFIGURATION WITH CLI/AT COMMANDS

This chapter contains the following information:

- Overview
- Configuring Data Compression Settings
- Configuring Error Control Options
- Configuring Link Option Settings
- Obtaining Modem Call Information
- Working with Modem Memory
- Configuring Modem Call Control Settings
- Configuring 56 Kbps Technology
- Configuring ISDN



*3Com recommends using the Web configuration interface to configure the modems on the SuperStack II Remote Access System (RAS) 1500. This chapter explains how to configure modems with the command line interface (CLI). For information about configuring modems with the Web configuration interface, view the online help.*

---

## Overview

**Before You Begin** Before you access the Console Interface, perform the following actions:

- 1 Connect the SuperStack II Remote Access Concentrator (RAS) 1500 console port.
- 2 Access the Console Interface with terminal software.

**Connecting to the RAS 1500** Connect to the RAS 1500 attaching a standard DB-9 connector to the Console Port.

**Accessing the Console Interface** Use a communications program to select terminal software. Select 8 bits, no parity, hardware, and 38.4 Kbps.

After configuring the RAS 1500 Console port, establish a connection from your management station or computer.

You are now ready to use the Console Interface to configure the RAS 1500.

**AT Commands** AT commands are used to communicate directly with the ports within the RAS 1500 module. You can use AT commands to change your modem/port settings at any time.



*Most commercial communications programs send an initialization string to the modem when you start the program. Remove your software initialization string so it does not interfere with the modem power-on defaults.*

**Sending AT Command** To send an AT command to a modem, enter the following information into the CLI:

```
set switched interface rm0/slot1/mod:[modem #] at_command [at command]
```

For example, to view modem settings for the first RAS 1500 modem, use the following command:

```
set switched interface rm0/slot1/mod:1 at_command ATi7
```

## Obtaining AT Command Help

There are five types of AT command help. See the Table 25 for the commands associated with the five types of AT command help.

**Table 25** AT Command Help

Help Type	Command
Basic AT Command Help	AT\$
Ampersand AT Command Help	AT&\$
Percent AT Command Help	AT%\$
Asterisk AT Command Help	AT*\$
S-Register Help	AT\$S

## Commonly Used AT Commands

There are certain AT commands that are used more often than others, such as dial commands, answer mode commands, and others used in modem initialization strings.

### Basic AT Dial Commands

The basic commands needed to dial using an RAS 1500 are listed in the Table 26. Refer to the Issuing AT commands section, earlier in this document, for information on how to send AT commands.

**Table 26** Basic AT Dial Commands

Action	Command
Obtain dial command help	ATD\$
Dial a number and enter Originate Mode	ATD <number>

## Dial Command Options

Include optional dial commands (Table 27) after the D command and before the number to be dialed unless indicated otherwise. To cancel dial command execution, press any key.

**Table 27** Dial Command Options

Action	Command	Example
Tone dial	T	ATDT5551234
Pause for a two second duration, set in S-Register S8	,	ATDT9,5551234
Wait for a second dial tone before dialing the rest of the Dial string. Use this command with result codes X3 or higher.	W	AT9W5551234
Wait for an answer. After the modem detects at least one ring, it waits for five seconds of silence at the other end of the call, and then continues executing the Dial string.  If the modem is set to ATX2 or lower, the @ command is ignored. If set to ATX5 or ATX6, the modem hangs up when it detects a voice answer and send the VOICE result code.  If the correct conditions do not occur (no rings following five seconds of silence), the modem reports NO ANSWER after the time-out period set in S-Register S7.	@	ATDT55512134@089
Reverse frequencies. This command allows calls to an originate-only modem.  The command follows the Dial command, before or after the phone number.	R	ATR5551234

## Using Stored Telephone Numbers

Each modem in an RAS 1500 can store up to four dial strings in NVRAM, store the last dialed number, and do an inquiry of stored phone numbers. A dial string may be up to 40 characters long. The string may include any valid Dial command options (Table 28), but no other commands.

**Table 28** Stored Telephone Numbers

Action	Command	Example
View stored telephone numbers	I5	ATI5
Write the following Dial string(s) to NVRAM at position n (n=0-3).	&Zn=s	AT&Z3=5551234
Write the last dialed number to NVRAM at position n (n=0-3).	&Zn=L	AT3=L
Display the phone number stored in NVRAM at position n (n=0-3).	&Zn?	AT&Z0=5551234
Dial the phone number stored in NVRAM at position n (n=0-3).	DSn	ATDS1
Dial the last-dialed number.	DL	ATDL
Display the last-dialed number.	DL?	ATDL?

## Configuring Answer Mode

Use the commands in Table 29 to configure Answer Mode.

**Table 29** Answer Mode

Action	Command	Example
Force Answer mode when the modem has not received an incoming call.	A	ATA
Set the number of rings before the modem answers.	ATS0=n Where n is the number of rings.	ATS0=3

## Disconnecting with AT Commands

To hang up calls (go on hook), issue the command below.

**H**

Example: ATH hangs up the modem

---

## Configuring Data Compression Settings

Data compression is a method by which the modem sending (transmitting) compresses the data being sent as it transmits, and the receiving modem decompresses the data as it is received. V.42 *bis* and the Microcom Networking Protocol-5 (MNP-5) allows for this compression to take place.

When data compression is enabled and an RAS 1500 makes an outgoing call, and if it successfully establishes a V.42 error control connection with the remote device, it negotiates for V.42 *bis* data compression. If unsuccessful, the module then attempts to use MNP-5 data compression.



*Compression does not occur unless the modems are able to establish an error control (Automatic Repeat Request [ARQ]) connection.*

The type of compression used for a call, if any, is reported through the AT16 command and in the CONNECT message, if &A3 is configured as a default setting.

### V.42 *bis* versus MNP-5 Data Compression

Of the two data compression protocols, V.42 *bis* is considered to be the better of the two in most cases because it dynamically deletes entries that are no longer used.

In addition, it works better with files that are already compressed. These include .ZIP files downloaded from many electronic bulletin board systems and 8-bit binary files, which seem to modems to be compressed. Sometimes the MNP-5 protocol attempts to compress an already compressed file, which causes the file transfer to take longer. V.42 *bis* only compresses data when compression yields an advantage.

To function correctly, V.42 *bis* requires V.42 error control to be enabled. The maximum compression, based on a standard file, that can occur using V.42 *bis* is 4:1. MNP-5 requires the MNP-4 error control protocol to be enabled and can only reach a maximum compression of 2:1.

When transferring compressed files, configure the RAS 1500 modems to &K3 (See Configuring Data Compression Methods below). This allows V.42 *bis* compression to work dynamically with the compressed data, but disables MNP-5.



## Data Compression Tables

A Data Compression Table describes a table of values assigned for each character during a call using data compression techniques. The default values in the table are constantly being changed to ensure the most efficient throughput possible. Each table uses a dictionary to assign these values.

Dictionary size is the amount of memory available for data compression table entries. Entries into the table are codes devised for redundant data. Then data is packed into these shorter data units, called code words, and unpacked by the receiving device. Possible dictionary sizes are in Table 30.

**Table 30** Dictionary Sizes

Bits	Entries
9	512
10	1024
11	2048

The RAS 1500 uses an 11-bit, or 2048-entry dictionary, but can reduce its size to accommodate a remote modem that uses a 9- or 10-bit dictionary. As the dictionary fills, the RAS 1500 deletes the oldest unused strings.

## Configuring Data Compression

The MNP level 5 Disabled setting allows V.42 compression only (for use when transferring compressed files). MNP-5 compression is not useful when transferring files that are already compressed because it tends to add data to the transmission so that throughput over the link degrades.

Table 31 shows the commands used to configure data compression methods:

**Table 31** Data Compression Commands

Action	Command
Disable compression	AT&K0
Auto Enable compression	AT&K1 (Default)
Enable compression	AT&K2
MNP Level 5 Disabled	AT&K3

---

## Configuring Error Control Options

Error control can be accomplished in different ways. Error control is available for calls at 1200 bps and above. It can be disabled, although high speed calls (above 2400 bps) should always be under error control. The operations defined in an error control protocol include the following:

- Establishing compatibility
- Formatting data frames
- Detecting errors using Cyclic Redundancy Checking (CRC)
- Retransmitting corrupt data frames



**CAUTION:** *High speed calls are vulnerable to errors unless the data is protected by error control. The operations described below take place even if the RAS 1500 is not configured for error control. If the modems in an RAS 1500 module connect with a remote device at high speed, but without error control, and if you are not using an error control protocol for your call, you may lose data.*

### Error Control

The RAS 1500 is set at the factory to &M4, causing it to try for an error control connection and, if that is not possible, to proceed with the call in Normal mode. The RAS 1500 first tries to make a V.42 connection, then an MNP connection. The following information is based on the setting of &M4.

### Automatic Repeat Request

Automatic Repeat Request (ARQ) is a method used in many error control protocols to ensure that any data that has been corrupted in transit is retransmitted.

### V.42 Error Control

This international standard includes a two-stage handshaking process:

- A Detection phase that is based on an exchange of predefined characters.
- A LAPM (Link Access Procedures for Modems) negotiation phase, during which the devices identify their capabilities concerning maximum data block size and the number of outstanding data blocks allowed before an acknowledgment is required.

## Microcom Networking Protocol Error Control

Microcom Networking Protocol (MNP) is supported by the ITU-T V.42 Recommendation. It was originally developed by Microcom®, Inc. and is now in the public domain. MNP is based on special protocol frames. If the remote device does not recognize an MNP Link Request, error control is not possible.

## Error and Flow Control

Flow control of data from the computer is required under error control for two reasons:

- The transmitting device buffers a copy of each frame it transmits to the remote end until it is acknowledged by the receiving device.
- If errors are encountered, retransmission activity can cause a steady stream of data from the computer to overflow the buffer.

Error control is required for data compression and recommended for all calls above 2400 bps.

Cyclic redundancy checking is used to detect errors. An ARQ is issued when a corrupted data frame is detected, and the data frame is retransmitted. ARQ denotes error control in U.S. Robotics error control commands and response codes.

A modem can retransmit a data frame a maximum of twelve times, after which the modem aborts the call. Disconnection from retry timeout only occurs under serious line disturbances.

## Using Error Control

### Disabling Error Control

Action	Command	Default
Disable error control. Not recommended for calls above 2400 bps.	AT&M0	AT&M4 (Enabled)

### Establishing Error Control-only Connections

Use this setting to guard against the transfer of data at high speeds without the reliability of error control. Modem disconnects (hang up on call) if ARQ connection cannot be made.

Action	Command	Default
Establish Error Control ONLY connections	AT&M5	AT&M4 (establishes non-ARQ call)

### V.42/MNP Negotiation Method

This method determines the error control handshaking mode. When set to disable either V.42 or MNP, the modem only attempts to negotiate the enabled protocol. If you know the remote modem does V.42, set to Disable Detection Phase. The V.42 detection phase is skipped during the handshaking process, allowing for a faster connection.

The commands used are AT&S27.4 and AT&S.27.5. See the Table 32 for setting information.

**Table 32** V.42 MNP Negotiation Method

AT&S27.4=n	AT&S.27.5=n	Result
1	0	Disable MNP
0	1	Disable V.42
1	1	Disable Detection Phase

The defaults are to complete handshaking sequence (.4 and .5 = 0).

### Configuring Carrier Delay Times

Carrier delay time is the amount of time the modem waits to disconnect after detecting the absence of a carrier signal. These delay times allow you to configure modems to handle specific situations, such as when a modem string contains a pause code after disabling a call waiting service, without disconnecting.

## Modifying Carrier Receive Delay

Table 33 provides the carrier receive delay commands.

**Table 33** Carrier Receive Delay

Setting	Command	Parameters	Default
The duration (tenths of a second) of the remote modem carrier signal before the local modem recognizes the signal. Ignored at speeds above 2400	ATS9=n	<n> = 0–255	ATS9=6
The duration (tenths of a second) that the modem waits after the loss of the remote modem carrier signal before hanging up.  This setting allows the modem to distinguish between a momentary lapse due to line quality and a true disconnect by the remote modem. If this value is set to 255, the modem does not hang up on loss of carrier.  It hangs up only when it receives the (+++) escape code sequence and returns to Command Mode	ATS10=n	<n> = 0–255	ATS10=7
The duration and spacing (milliseconds) of dialed touch tones.	ATS11=n	<n> = 0–255	ATS11=70
The 2100 Hz answer tone to disabled, allowing V.42 modems to connect more quickly and/or eliminating problems with older 2400-bps modems that do not recognize this tone	ATS27.3=1		ATS27.3=0 (Enable)
The guard time (50ths of a second) for the modem escape code sequence	ATS12=n	<n> = 0–255	ATS12=50 (1 second)

## Configuring Link Option Settings

This section explains how to change the settings that affect link options between the RAS 1500 module and the modems it connects to.

### Link Speed Index

The following table shows the index number used in configuring both minimum and maximum connect speeds. Refer to Table 34 obtain the correct index number when configuring link speeds.

**Table 34** Link Speed Index Numbers

Link Speed	Index	Link Speed	Index	Link Speed	Index
Highest Speed	0	33600	16	48000	32
300	1	28000	17	49333	33
1200	2	29333	18	50666	34
2400	3	30666	19	52000	35
4800	4	32000	20	53333	36
7200	5	33333	21	54666	37
9600	6	34666	22	56000	38
12000	7	36000	23	57333	39
14400	8	37333	24	58666	40
16800	9	38666	25	60000	41
19200	10	40000	26	61333	42
21600	11	41333	27	62666	43
24000	12	42666	28	64000	44
26400	13	44000	29		
28800	14	45333	30		
31200	15	46666	31		

### Setting the Highest Possible Connect Speed

The &N command allows you to set the highest possible connect speed. When a remote modem connects to an RAS 1500, it limits the maximum speed of the connection based on the value specified with &N. If the &U argument is zero, the connection is limited to the single speed implied by the &N argument.

#### Example:

AT&N16 configures the highest possible connect speed to 33600 bps.

AT&U6 configures the lowest possible connect speed to 9600 bps.

### Setting the Lowest Possible Connect Speed

The &U command allows you to set the lowest possible connect speed. When a remote modem connects to an RAS 1500, it limits the minimum speed of the connection based on the value specified with &U. If the &U argument is zero, the connection is limited to the single speed implied by the &N argument.

### Setting a Range of Possible Connect Speeds

By setting &N and &U values, you can control the range of speeds at which an RAS 1500 connects with remote modems. When a remote modem connects to an RAS 1500, it limits the range of speeds of the connection based on the value specified with &U and &N. If the &U argument is zero, the connection is limited to the single speed implied by the &N argument.

For asymmetrical links, &N and &U are used to constrain the speed of the higher speed direction of the link. The speed of the lower speed direction is constrained by values given in S registers.



*If the link speed associated with the &U argument is greater than the link speed associated with the &N argument, the RAS1500 treats the &U argument as if it were zero and limits the connection to a single speed.*

Use Table 35 to understand the relationship between &U and &N commands:

**Table 35** Connect Speeds

<b>IF &amp;U</b>	<b>and &amp;N</b>	<b>Modem Action</b>
Equals zero	Equals zero	Connects at the highest possible speed.
Equals zero	Is greater than zero	Connects at the &N speed only.
Is greater than zero	Is greater than zero and greater than &U	Connects at the highest possible speed in the range from &U to &N.

### Understanding Base Rates and True Rates

The x2 speeds listed in the &U and &N table are base rates. From each base rate an additional 6 true rates can be derived. There are 30 true rates. The same x2 true rate could be derived from multiple base rates. It is possible to get an x2 connection at a true rate that is less than the minimum rate implied by the &U value.

### Controlling the Minimum Low-speed Direction

Low-speed direction speed is the send/receive baud rate of the slowest end of a connection. Use the following S74 settings in Table 36 to control the minimum low-speed direction speed:

**Table 36** S74 Lower Limit Link Speeds

Lower Limit Link Speed	Setting	Example
No lower limit	0	ATS74=0
2400	1	ATS74=1
4800	2	ATS74=2
7200	3	ATS74=3
9600	4	ATS74=4
12000	5	ATS74=5
14400	6	ATS74=6
16800	7	ATS74=7
19200	8	ATS74=8
21600	9	ATS74=9
24000	10	ATS74=10
26400	11	ATS74=11
28800	12	ATS74=12
31200	13	ATS74=13
33600	14	ATS74=14



## Controlling the Maximum Low-speed Direction

Low-speed direction speed is the send/receive baud rate of the slowest end of a connection. Use the S75 settings in Table 37 to control the maximum low-speed direction speed:

**Table 37** S75 Upper Limit Link Speeds

Upper Limit Link Speed	Setting	Example
No upper limit	0	ATS75=0
2400	1	ATS75=1
4800	2	ATS75=2
7200	3	ATS75=3
9600	4	ATS75=4
12000	5	ATS75=5
14400	6	ATS75=6
16800	7	ATS75=7
19200	8	ATS75=8
21600	9	ATS75=9
24000	10	ATS75=10
26400	11	ATS75=11
28800	12	ATS75=12
31200	13	ATS75=13
33600	14	ATS75=14

## Obtaining Modem Call Information

AT commands allow you to obtain and view both configuration and statistical information for a specific modem port. This section lists the AT commands used to obtain call information, and modem characteristics, for both current and previous calls on any specific modem port.

- Modem Query Commands
- Displaying Link Diagnostics of Current or Previous Calls
- Understanding Link Diagnostic Results
- Understanding Disconnect Messages

## Modem Query Commands

Table 38 lists each command available.

**Table 38** Modem Query Commands

Display	Command
Product name	ATi3
Current modem settings	ATi4
Settings stored in the modem's NVRAM. If your modem connects to a modem that has Link Security and local access enabled, you cannot view the stored phone numbers	ATi5
Link diagnostics of the current or previous call, including characters transferred, data blocks retransmitted under error control, disconnect reasons, line source, and other information	ATi6
Product configuration. Displays code date, revision, the slot and channel number of the modem, and other information used by 3Com Technical Support to diagnose problems	ATi7
Advanced Link Diagnostics	ATi11
ISDN information	ATi12



*ATi8, ATi0, ATi2, and ATi18 are reserved.*

## Understanding Link Diagnostic Results

Link diagnostic result parameters are displayed by the AT16 command. Table 39 explains each parameter.

**Table 39** Link Diagnostic Results

Result	Indication
Octets	Compressed characters; may be greater than the number of characters sent due to buffering operations.
Blers	Errors in data and protocol (non-data) blocks, but corrected by ARQ (Error Control).
Link Timeouts	Error correction protocol severed momentarily (during which no data was transferred), but the protocol was able to recover.
Link NAKs	Negative acknowledgments (one or more blocks).
Data Compression	The type of data compression negotiated for the call (V.42 <i>bis</i> or MNP5) or NONE. A V.42 <i>bis</i> response includes the size of the dictionary and the maximum string length used (for example: 2048/32).
Equalization Long/Short	The status of S15 bit 0; Long if bit 0=0, Short if bit 0=1
Fallback Enabled/Disabled	Whether or not the modems negotiated online fallback during the connection sequence.
Protocol	The error control protocol negotiated (LAPM, MNP, NONE) or SYNC for a synchronous call.
Speed	The last rates at which the receiver/transmitter were operating before disconnecting.

The possible reasons for disconnect are explained in Table 40.

**Table 40** Disconnect Reasons

<b>Disconnect Reason</b>	<b>Indication</b>
Keypress Abort	The modem detected a keypress while training.
Escape code	The operator sent the modem the (+++) escape code.
GSTN (General Switch Telephone Network) Clear Down	The connection was a non-ARQ and DTR was dropped from one side of the connection, or the DISC frame was corrupted due to noise.
Loss of Carrier	The modem detected loss of the remote modem's carrier and waited the duration specified in S10 (default is 0.7 seconds).
Inactivity Timeout	The modem detected no activity on the line for the duration specified in S19. Default is 0, timer disabled.
MNP Incompatibility	The modem is set to &M5 and the remote modem does not have MNP capability, or there was an MNP negotiation procedure error.
Retransmit limit	The modem(s) reached the maximum of twelve attempts to transfer a data frame without error.
LD received	The remote modem sent an MNP error control Link Disconnect request.
DISC	The remote modem sent a V.42 Disconnect frame.
Loop loss disconnect	The modem detected a loss of current on the loop connecting it with the telephone company central office (CO). This usually occurs because the remote modem has hung up: the CO drops current momentarily when there is a disconnect at the other end of the call. Unless S38 is set higher than zero, the modem immediately hangs up at loop loss.
Unable to Retrain	After several attempts, disturbances on the phone line prevented the modems from retraining, and they could no longer transmit or receive data.
Invalid speed	The modem is set to &N1 or higher, for a fixed link rate, and the remote modem is not operating at the same rate.
XID Timeout:	The modems failed to negotiate the V.42 Detection (XID Exchange) phase.
SABME Timeout (Set Asynchronous Balance Mode Extended)	The modems failed this part of V.42 link negotiation.
Break Timeout	Incompatible processing of a Break signal occurred.
Invalid Codeword	The modem received an invalid V.42 <i>bis</i> frame.
A Rootless Tree	The modem received an invalid V.42 <i>bis</i> .

## Working with Modem Memory

Modems inside an RAS 1500 module have a user-configurable memory type known as Flash memory. You can store, retrieve, and change settings in Flash. Each modem also uses Random Access Memory (RAM) to store current settings, however modem configurations stored in RAM are lost as soon as the modem is power cycled or turned off. Since this information is saved in the modem Flash, a loss of power does not affect your settings.

- Viewing Modem Settings in Memory
- Storing Settings in Flash Memory
- Saving a Phone Number to Flash Memory
- Working with the Flash Memory Template

### Viewing Settings

When you issue an AT configuration command, the modem stores the command RAM as a current setting. Any setting(s) that you change and do not save to the modem are active until you reset or power off a modem.

View	Command
Current settings	ATI4
Saved settings in Flash memory	ATI5

### Storing Settings in Flash Memory

Save modem settings to Flash memory by adding the &W to the end of the AT command. This changes the default setting for that modem after the current call is completed. The following table shows how to use the &W command to save S-Register values to Flash memory.

Action	Command	Example
Change a default setting and write it to Flash at the same time	AT[Value you are changing]&W	ATX6&W



*Any other setting changed, that can be saved to Flash memory, is also saved when you issue the &W command.*

### Saving a Phone Number to Flash Memory

Each modem in an RAS 1500 can store up to four different telephone numbers. Table 41 explains how to store these numbers in modem Flash memory.

**Table 41** Saving a Phone Number to Flash Memory

Action	Command
Dial the phone number you saved with a special setting. In this example, &M0 (no error control) comes before the DS2.	AT&M0DS2
Dial the phone number you saved.	ATDS2
Store the phone number 555-1234 at position two.	AT&Z2=555-1234
View the saved phone numbers.	ATI5



**CAUTION:** Do not include modem commands in `AT&Zn=s`.

### Working with the Flash Memory Template

Each modem permanently stores one configuration template (a prepared set of commands) in Flash memory. You can retrieve a template and load it into current memory using the `&F0` command.

#### Saving Configuration Templates in Flash Memory

Save a configuration template in Flash memory as you save any other AT command. For example, to save factory defaults into Flash memory:

```
set modem interface rm0/slot1/mod:4 at_command AT&F08W
```

Configuration templates cannot be customized since they are a part of the modem ROM. However, you may load a template into active memory, modify it, and save it to Flash memory.

Example:

```
set switched interface rm0/slot1/mod:1 at_command
at&f0&k3s10=40&A2&W.
```



*Insert your changes after the `&F0` command but before `&W`. If you do not, the changes are be overwritten by `&F0`.*

#### Flash Memory Initialization Strings

Most communications applications send an initialization string to the modem when you load the program. To modify your software initialization string to reflect the modem factory settings, use the following initialization string: **AT&B0&H0&R1X1&A1**

## Changing Settings Temporarily

Any setting can be changed just for the current session. You may want to use this feature for experimentation if you are experiencing performance difficulties. If the change does not achieve the desired effect, reset the modem (described below) to return it to its previous saved configuration. For example, the ATX6 command changes the result code setting, but the power-on/reset default remains intact.

## Resetting a Modem

Resetting the modem restores the modem to the configuration saved in Flash. This can be accomplished by issuing the ATZ command.

## Customizing Flash Settings

To modify the active configuration in Flash, type your changes and then save them to Flash with the &W command, as in the following example:

```
AT &K3 X3 S10=40 &A2 T &W
```

---

## Configuring Modem Call Control Settings

You can use AT commands to configure how modems operate. You can control the following types of call control settings:

- Enabling Answer In Originate Mode
- Setting ARQ Negotiation
- Setting Carrier Wait Time After Dialing
- Setting Idle Time Before Disconnect
- Setting MNP/V.42 Link Request Timeout
- Setting V.32 300/600 Hz Tone Times
- Setting the Number of Rings for Auto Answer

### Enabling Answer In Originate Mode

Setting	Command	Default
Auto Answer in Originate mode	ATS13.2=1	ATS13.1=0 (Disabled)

### Setting ARQ Negotiation

If ARQ negotiation is set to None, ASYNC connections are allowed without error control. If set to Normal ARQ (default), the local modem attempts to connect under error control, but connects without it if cannot be negotiated. If set to ARQ Only, the local modem attempts to

use error correction and hangs up if the remote modem is not using error correction.

Setting	Command
None (Normal)	AT&M0
Normal ARQ (Default)	AT&M4
ARQ Only	AT&M5

### Setting Carrier Wait Time after Dialing

Setting	Command	Parameters	Default
The duration, in seconds, that the local modem waits to detect a carrier signal from the remote modem.	ATS7=n	<n> = 0-255	60

### Setting Idle Time Before Disconnect

Setting	Command	Parameters	Default
Idle time before disconnect.  If set in minutes, to greater than 0, the Inactivity Timer is activated when there is no data activity in either the transmit or receive direction.  If no data activity is detected by the timeout period, the modem hangs up.	ATS19=n	<n> = 0-255	0

### Setting MNP/V.42 Link Request Timeout

Setting	Command	Parameters	Default
The duration of the timeout, in seconds, when the modem is negotiating an MNP/V.42 link request for 1200/2400 answer mode.	ATS52=n	<n> = 0-14	5



## Setting V.32 300/600 Hz Tone Times

Setting	Command	Parameters	Default
The duration, in tenths of a second, of the EIA-specified Multimode Training sequence for V.32 modems, which includes 3Com Dual Standard modems set to answer V.32 calls (set to B0).  The delay gives V.32 modems additional time to connect with most U.S./Canada modems at 9600 bps before falling back to attempt a V.21 connection (to answer overseas calls, 300 bps), 1200 bps with a 75-bps back channel). The fallback occurs only if the modem is set for V.21 (S27, bit 0 enabled).	ATS28=n	<n> = 0-255	8

## Setting the Number of Rings for Auto Answer

Setting	Command	Parameters	Default
The number of rings on which to answer incoming calls when the modem is in Auto Answer mode. Setting to 0 disables the modem Auto Answer feature.	ATS0=n	<n> = 0-255	1

## Setting Time to Start Dialing

Setting	Command	Parameters	Default
The number of seconds the modem waits to dial after detecting a dial tone.	ATS6=n	<n> = 0-255	2

## Configuring 56 Kbps Technology

V.90 and x2 are ground-breaking technologies that allow servers to send data at speeds up to 56 Kbps and clients to send data at speeds up to 33.6 Kbps.

The RAS 1500 supports V.90 as dial-in only.

### Factory-enabled Protocol

The RAS 1500 ships with the V.90 protocol factory-enabled.

### Controlling Server x2

Use the following setting to disable server x2:

Command: ATS76=2

### Disabling V.34 Connections

The RAS 1500 allows the selective disabling of V.34 connections depending on whether or not they are made with an x2 capable modem (Table 42).

**Table 42** Disabling V.34 Connections

Action	Command
Allow V.34 and x2 connections	ATS54.7 = 0
Allow V.34 and x2 connections only with x2 modems	ATS56.6 = 0 (for x2 modems only)ATS56.7 = 1ATS27.2 = 1ATS13.5 = 1
Allow V.34 connections to all modems	ATS56.6 = 0ATS76.3 = 0
Disable V.34 and x2 connections to all modems	ATS54.7 = 1
Disable V.34 connections to non-x2 modems, but allow V.34 connections to x2 modems	ATS56.6 = 1ATS76.3 = 0
Disable V.34 connections to x2 modems	ATS56.6 = 0ATS76.3 = 1
Disable V.34 connections, but allow x2 connections to all modems	ATS56.6 = 1ATS76.3 = 1



*S-Register S76, bit 3 can be set only via AT commands at this time.*

### Configuring ISDN

The RAS 1500 supports X.75 frame and window size configuration.

#### Enabling X.75

To enable X.75, set S68=0.

#### Frame Size

Frame size is the number of data bytes sent in an X.75 frame.

#### Window Size

Window size is the number of frames sent before an acknowledge (ACK) is received.



*Window size is an important consideration in the performance of the system. The larger the window, the more frames that can be transferred without an acknowledgment. However, the more frames that are transferred without an acknowledgment, the more the receiver is required to allocate additional buffer space to handle the incoming transmissions.*

### Selecting Frame and Window Size

Use the following AT commands to select frame and window size:

**Table 43** AT Commands

Setting	Command	n Value	Default size
Frame size	AT*X0=n	Between 1 and 2048	2048 bytes
Window size	AT*X1=n	Between 2 and 7	7

### Relationships Between Frames and Windows

Although you can set the frame size on the RAS 1500 up to 2048, use Table 44 to determine the actual values allowed by the RAS 1500.

**Table 44** Frame and Windows Sizes

Setting	Modem Window Size
2048	2
1024	4
512	7

### Viewing Current Frame and Window Size Settings

Use the following command to view current frame (\*X0) and window (\*X1) size settings:

**ATI4**

### Best Possible Connection

Every time a call comes in the RAS 1500 goes through a link negotiation process (called "handshaking") with the remote device.

The way the RAS 1500 handles outgoing and incoming calls depends on the call type setting you chose. You can set the RAS 1500 to handle incoming calls seven different ways:

- Best possible connection (Universal Connect)
- Clear channel synchronous
- V.120 only
- V.110 only
- X.75 only
- Analog modem emulation
- Synchronous PPP

## Universal Connect Call Flow

The RAS 1500 tries a number of calls and detection processes (Table 45).

**Table 45** Universal Connect Call Flow

Attempt	Call Type	Protocol	Command
1	64 Kbps	V.120, X.75, or Synchronous PPP	AT*U1
2	56 Kbps	V.120, X.75, or Synchronous PPP	
3	38.4 Kbps	V.110	AT*U2
4	3.1 kHz Audio	V.34, V.FC, V.32 terbo, and other analog call types	AT*U3



*When you set the RAS 1500 to Universal Connect and make or receive a call, the RAS 1500 attempts a V.110 connection only if you set S67.0=1. In Universal Connect answer mode, when V.110 is enabled, the RAS 1500 makes the V.110 attempt third in the Universal Connect sequence.*

## Answering and Originating Calls

Use Table 46 to set the answer and originate call type.

**Table 46** Answering Call Types

Setting	Command
Autodetect	AT *V2=0
V.120 rate adaption only	AT *V2=1
V.110 rate adaption only	AT *V2=2
Modem	AT *V2=3
Clear channel synchronous only	AT *V2=4
Asynchronous to synchronous PPP only	AT *V2=5
X.75 connection only	AT *V2=6



*If you set the call to a specific type (\*V2=1-6) and the desired connection cannot be made, the RAS 1500 does not negotiate for other types of connections. Default configuration to V.120 with X.75 turned off.*

## Setting the Originate Call Type

You can set the originate call type for each B-channel. These commands are only valid when auto detect is used (\*V2=0).



*These state of these new commands is saved in flash.*

## Originating HDLC 64 Kbps and 56 Kbps Protocols

Use Table 47 to control the originating High-level Data Link Control (HDLC) 64 Kbps and 56 Kbps protocols:

**Table 47** HDLC 64Kbps and 56 Kbps Protocols

Setting	Command
None	*U1=0
V.120	*U1=1
X.75	*U1=2
PPP	*U1=3

## Originating Non-HDLC Protocols

Use the commands in Table 48 to control the originating non-HDLC 64 protocols.

**Table 48** Non-HDLC 64 Protocols

Setting	Command
None	*U2=0
V.110	*U2=1

## Originating Analog Modem Mode

Use the commands in to control the originating analog modem mode.

**Table 49** Originating Analog Call Type

Setting	Command
None	*U3=0
Analog Modem	*U3=1



# 11

## CONFIGURING THE RAS 1500 ROUTER

This chapter covers administrative commands used for the following:

- Reconfiguring Your System
- Communicating with Remote and Local Sites
- Troubleshooting Commands
- Displaying System Information

---

### Reconfiguring Your System

The commands detailed in this section control configurable aspects of your system.

#### Customizing CLI Parameters

##### Local Prompt

Use `set` command if you have more than one SuperStack II Remote Access System (RAS) 1500 and want to differentiate between them or you just want to customize your prompt from the default. The prompt can be up to 64 characters. Use the following command:

```
set command local_prompt <"prompt message">
```

Example:

```
set command local_prompt Welcome!
```

##### Command History

If you want to customize the history function to change the default (10), use the following command. The command history limit is 500 commands.

```
set command history <depth>
```

### Idle Timeout

If you want to make sure that a console login user is using the link constructively — and not leaving the system vulnerable to a security breach — set an idle timeout using the following command:

```
set command idle_timeout <0-60 minutes>
```

Example:

```
set command idle_timeout 5
```

### Login Required

You can force a console user to login after the idle timeout interval has elapsed. Use the following command:

```
set command login_required [yes | no]
```

### Global Prompt

If you want to specify a separate prompt for a command file process, use the `prompt` parameter. The global prompt value is useful if you are running a number of processes and want to differentiate between the global and session prompts. Or, if you are Telnetting to the system, for instance, and want to create a separate, easily identifiable prompt. If your prompt consists of more than one word, remember to enclose it in quotes. Use the following command:

```
set command prompt <string>
```

Example:

```
set command prompt "TELNET Session"
```

### Setting the System

The `set system` command designates a name and location for your system, contact information and a keyword necessary to make a PPP connection to a remote router over the WAN. Use this command:

```
set system
  name [name]
  location [location]
  contact [contact information]
  transmit_authentication_name [keyword]
```

Example:

```
set sys na "white house" loc DC cont "staff, ext 555" tran
"FOB"
```



## Running Script Files

The `do` command is a powerful tool to configure multiple users, protocols, or other functionality by running a script file containing CLI commands. To use this command, create a file containing the CLI commands you want to implement, TFTP the file to the FLASH ROM, and type `do <filename>`. See the example below covering many system functions. Some commands are commented out or abbreviated.

```
; RAS 1500 CONFIGURATION FILE;
;   FACILITIES LOGLEVEL;
set facility ip loglevel verbose
set facility ppp loglevel verbose
set facility user loglevel verbose
set facility call loglevel verbose
;
;   SYSTEM INFO;
set system name "marauder"
set system contact "Henry Stimson"
set system location "3Com Lab"
;
;   SETTING THE LOCAL COMMAND PROMPT;
;set command prompt "RAS 1500"
;
;   SETTING THE SYSTEM COMMAND HISTORY;
;set command history 100
;
;   SNMP COMMUNITIES;
add snmp community sqatest a 0.0.0.0 a rw
add snmp community bearcat a 0.0.0.0 a rw
add snmp community public a 0.0.0.0 a ro
;
;   IP NETWORKS;
add ip network "ipnet-157.172.248.0" address 157.172.248.38/c
rm0/eth:1
set ip network "ipnet-157.172.248.0" routing_protocol ripv1
;set ip network "ipnet-157.172.248.0" routing_protocol ripv2
;set ip network "ipnet-157.172.248.0" routing_protocol none
;set ip network "ipnet-157.172.248.0" rip_policies ripv1_rec
ripv1_receive ripv1
;
;   ADDING STATIC IP ROUTES;
;add ip route 204.249.182.0 gateway 157.172.228.1 metric 1
;
;   DNS ADD;
add dns host louvre address 157.172.248.54
```

```
add dns host wimpy address 157.172.248.40
;add dns server preference 1 address 157.172.248.40 name
louvre
;
;          SYSLOG HOST ADD;
add syslog 157.172.248.54 loglevel verbose
;
;          LOCAL AUTHENTICATION;
enable authentication local
;
;          REMOTE AUTHENTICATION;
set authentication radius_secret testing12326.54
secondary_server 157.172.248.40
;
;          REMOTE AUTHENTICATION;
; enable authentication remote
;
;          ACCOUNTING;
set accounting primary_server 157.172.248.54 secondary_server
157.172.248.40
enable accounting
enable ip rip
enable ip routing
enable security_option remote_user_administration dialin or
telnet
;
; ;          ADDING USERS;
; ROOT - ADMIN/MANAGER;
add user root password root type manage
;
;          NETWORK_SERVICE;
;enable network_service root
add user henry type network,dial_out
set network user henry ip_routing both
set network user henry send_password georgef
;
add user son type network
set network user son remote_ip_address 157.172.248.105/c
set network user son ip_routing both send_password gordo
set network user son address_selection negotiate
;
save all;
```

## Discarding and Renaming Files

There are several `delete` commands you can use to discard various files.

- `delete configuration` — discards all configuration files, reboots the system and restores system configuration to factory defaults
- `delete file` — removes a file from the FLASH file system
- `delete filter` — pulls a filter entry from the filter table and discards it from FLASH memory
- `rename file` — copies files within the FLASH file system. Use the command:

```
rename file <input_file> <output_file>
```

---

## Communicating with Remote and Local Sites

### Dial, Disconnect, and Hangup Commands

You can dial up a remote or local site with the `dial` command and log in to hosts with the `rlogin` and `telnet` commands. You can use the `hangup` and `logout` commands to clear those lines.

#### Dial Command

The `dial` command makes an immediate connection for a manual dial-out user using the dial-out information in the user's profile. Use the following command:

```
dial <user_name>
```



*To use this command, the username must already exist in the system.*

#### Hangup Command

To close an interface (`hangup` and leave the interface(s) in an ENABLED state), use the following command:

```
hangup interface <interface_name>
```

To make a modem group unavailable for dial-in users, use the following command. It has the same effect as hanging up the phone.

```
hangup modem_group <name>
```

### Disconnect Command

To disconnect a user (disconnect and leave the user in an inactive state), use the following command:

```
disconnect user <user_name>
```

### Reboot Command

Use the `reboot` command to recycle the system. But first, be sure to use the `save all` command to preserve any configuration changes.

### Dial-in User Message

Use the `set switched interface` command to display a configurable message to your dial-in users when the connection is set over the specified modem. This information is helpful for diagnostic purposes. Using the `show user` command displays the message as it was configured. The options are:

- `$date` — current date according to system uptime
- `$callid` — user call number according to system uptime
- `$port` — port occupied by user (rm0/mod:y)
- `$hostname` — user host name
- `$sysname` — user system name (same as hostname)
- `$time` — time of call according to system uptime



*Like all CLI string values, the message must be enclosed in quotations.*

Example:

```
set switched interface rm0/slot1/mod:1 message "Welcome to  
the Stack, $hostname. You're Caller # $callid connected on  
$port at $time on $date."
```

Upon dial-up, RAS 1500 will display:

```
Welcome to the Stack, janedoe. You're Caller #2345 connected  
on rm0/slot1/mod:1 at 5:39 pm on September 5, 2001.
```

### Exiting the CLI **Bye, Exit, Leave, Quit Commands**

The `bye`, `exit`, `leave`, and `quit` commands all serve to shut down the CLI but leave the connection open.

## Logout Command

Logout exits the CLI and closes the connection, ending a dial-in user or Telnet session.

## Network Services

To use ClearTCP, Simple Network Management Protocol (SNMP), or DialOut and to set values associated with them, add each network service and related parameter. Telnet and Trivial File Transfer Protocol (TFTP) are already enabled at startup although you can add additional services whenever necessary.

## Adding Network Services

Use the `add network service` command shown below:

```
add network service [service_name]
    close_active_connections [false | true]
    data [ancillary entry]
    enabled [no | yes]
    socket [socket number]
    server_type [cleartcpd, dialout, snmpd, telnetd, tftpd]
```

Example:

```
add network service DIALOUT close_active_connections true
socket 99 data "auth=off,login_banner=\"Welcome to my Net\",
service_type=dialout,drop_on_hangup=on login_prompt=\"My
Session\""
```



*To edit a network service, you must first disable it. After editing the service, enable it again.*



*Enclose all DATA values in double quotations and all stringed DATA values in forward slashes and a second set of double quotes.*

**close\_active\_connections** Indicates whether or not to close any active connections when a service is disabled.

**data** Ancillary data. Format one or more values with syntax from Table 50.

**Table 50** Ancillary Data Values

Data Value	Description
"auth=on/off"	On indicates that login/ password authentication should be performed on incoming connections. Default: on
"login_banner=\"string\""	ASCII string sent to a client when the connection is made. It must be enclosed in quotes and forward slashes. Default: none
"login_prompt=\"string\""	ASCII string specifying the login prompt to be sent during authentication. It must be enclosed in quotes and forward slashes, and auth must be on. Default: login.
"service_type=manage/dialout"	Indicates whether the service is offering modem sharing service or manage service. Modem sharing service connects the client to a modem. Manage service connects the client to the command line, to manage the system. Applicable only to Telnet servers; you cannot ClearTCP into the system to manage. Default: manage
"modem_group=\"string\""	Used for modem sharing service, indicating the modem group the service will allocate a modem from. String must be double quoted and offset by forward slashes. Default: none.
"drop_on_hangup=on/off"	Used for modem sharing service. on causes the TCP session to be dropped when the modem hangs up. off causes the connection to remain active. Default: off

Using the `list services` command after typing the example above will display the following (for example):

```
CONFIGURED NETWORK SERVICES
                        Server Admin
Name                   Type SocketClose Status
tftpd   TFTPd 69 FALSE  ENABLED
DATA:
dialout          DialOut32773FALSE  DISABLED
DATA: auth=off, login_banner= "Welcome to My Net",
login_prompt="My Session,drop_on_hangup=on
telnetd          TELNETD23FALSE  ENABLED
DATA:
TELNET server    TELNETD99FALSE  DISABLED
DATA: "
```

**enabled** When you add a network service, it is enabled by default. When changing any parameter, you must first disable the service then re-enable it.

Example (abbr.):

```
set network service "telnet user" server_type telnetd data
"auth=off" enabled yes
```

**server\_type** Type of service being offered: ClearTCPd, Dialout, SNMPd, Telnetd, TFTPd).

**socket** Sets the port number the RAS 1500 listens on for network service requests.

### Enabling and Disabling Network Service

By default, the network service is enabled when you add it. To edit the service, you must first disable it:

```
disable network service <service_name>
```

To enable network service:

```
enable network service <service_name>
```

### Deleting a Network Service

To delete a network service:

```
delete network service <service_name>
```

## Using TFTP

TFTP (Trivial File Transfer Protocol) can be used to transfer files to and from the system. Since this network service is enabled by default, set it up by first configuring your computer as a TFTP client of the stack by entering this command:

```
add TFTP client <hostname or IP address>
```



*If you want to allow any system to TFTP into your system, set a TFTP client to 000.000.000.000.*

Next, from a machine that has access to the same network, use the following TFTP commands to transfer the filter file to FLASH memory:

```
tftp <RAS 1500 IP address>  
put <filename>
```



*Use `list files` to verify the file was sent to RAS 1500.*

If you want to obtain a file from another network host, add that host as a TFTP client, and, from within the system, use Telnet to access that host and use the following command to obtain the file:

```
get <filename>
```



*Do not transfer binary files. Transferring binary files of any type will cause unexpected results and may cause RAS 1500 to “hang.”*

## Using Rlogin and Telnet

You can connect to a specific host on the network using the `rlogin` or `telnet` commands. You must first have used the `add dns host` or `add dns server` commands for RAS 1500 to recognize an IP host name. Both services are enabled at startup.



*Rlogin is not supported into RAS 1500. You can only use rlogin to communicate out of RAS 1500.*

Rlogin and Telnet use the following syntax:

```
rlogin <IP name or address>  
  login_name <name>  
  tcp_port <number>
```

or:

```
telnet <IP name or address>
```



For example, to Telnet to a host with an IP address of 167.199.76.23, use the following command:

```
telnet 167.199.76.23
```



*When using Telnet or rlogin on a TCP connection via a global interface (RAS 1500 internal interface), you should run RIP. Without RIP running on the internal network, you will not learn of remote networks should the Ethernet interface be disabled. See Chapter 5, “Configuring Telnet Network Dial-Out” for more information.*

### Telnet Status

The `status` command displays the IP address of the remote host you (Console port user only) are Telnetted into and the value of the Telnet escape character. Typing status at the `telnet:` prompt will produce something like this:

```
Connected to 172.144.122.144.
Escape character is ^]
```

### Telnet Control Characters

Console port users (service unavailable to login users) can use the `send` command to transmit a Telnet control character to a host.

After you have established a Telnet session (logged in and given your password), type the Telnet escape character: `C ]` (Ctrl right bracket) followed by one of the ten other control characters, making sure that the characters are all uppercase. Your choices are shown in Table 51.

**Table 51** Telnet Control Characters

Parameter	Description
AYT	Are you there
IP	Interrupt process
BRK	Break
AO	Abort output
EC	Erase character
EL	Erase link
GA	Go ahead
NOP	No operation
EOR	End of record
SYNC	

For example, at the host prompt, use the following command:

```
C ] send AYT
```

You can use the `set_escape` command to change the Telnet escape character to a character of your choice. Use a *carat* (^) to precede another character.

Example:

```
set_escape ^X
```

### Closing a Connection

The `close` command shuts down an active Telnet connection.

---

## Troubleshooting Commands

### Viewing Facility Errors

The `set facility` command allows you to set and view log levels for the system processes, ensuring that error messages reaching the threshold for that facility will be output to the console port.



*Although messages are sent to the Console port by default, you can configure a SYSLOG host to receive messages. This would free up the Console since sending messages uses system resources and can slow down the connection.*

Log levels range from the lowest state, debug, to the highest, critical. The default is critical. Use the following command:

```
set facility <name>  
    loglevel [common | critical | debug | unusual | verbose]
```

Example:

```
set facility snmp loglevel unusual
```



*Use the `list facilities` command to view a log level change.*

### Terminating an Active Process

The `kill` command terminates an ongoing process. You can kill a process only after it has started. For instance, if you want to kill a `ping` request that has run too long. Use the `list processes` command to view current active processes.

## Resolving Addresses

The `arp` command performs IP address resolution. Use the following command:

```
arp <ip address or host name>
```

The system will respond with an IP address (and MAC [Ethernet] address if found on a locally connected network) of the host.

Example:

```
ARP: 172.122.120.118 -> 08:00:09:cc:58:bf
```

## Resolving Host Names

The `resolve name` command returns an IP address for a specified host name by sending it to a DNS server for resolution. But before you can resolve a host, you must have added a DNS local host and server entry for resolution. To do so, use the `add dns host <name> address <ip address>` and `add dns server <ip address>` commands.

You can resolve names locally or remotely as follows:

Locally — `add dns host hahvahd.college-hu.com address 133.114.121.15 resolve name hahvahd`

Remotely — `add dns server 133.114.121.45 preference 1 name "Our DNS server"`

Screen output example:

```
Network Name: hahvahd.college-hu.com is resolved to Address: 133.114.121.015
```

## Using Ping The ping Command

The `ping` command is very helpful in testing RAS 1500 connectivity with other network devices. Options let you set ping attempts (`count`), the period between ping attempts (`interval`), the time before quitting (`timeout`), a string value specifying data to be sent (`data`), the ping packet dimension (`size`), the ping process off screen (`background`), the progressive ping output for each ping request (`verbose`), and the erasure of entries in the Remote Ping Table (`self_destroy_delay`).

The CLI can perform a ping with either `verbose` or `background` selected, but not both. `verbose` causes the CLI to display information for each PING transmitted. `background` causes the CLI to start the PING request and then ignores it.

This diagnostic tool can also be initiated from an SNMP station. Use the following command:

```
ping <IP address>
    background [yes | no]
    count [1-1000]
    data [string]
    interval [1-65535]
    self_destroy_delay [minutes]
    size [1-1400]
    timeout [1-60]
    verbose [yes | no]
```

Example:

```
ping 199.55.55.55 count 3 verbose yes
```

The command would display the following:

```
PING Request: 1 Time (ms): 10
PING Request: 2 Time (ms): 0
PING Request: 3 Time (ms): 0
PING Destination: 199.55.55.55          Status: ALIVE
Count:          3
Timeouts Occurred:0
Minimum Round Trip (ms):          0
Maximum Round Trip (ms):10
Average Round Trip (ms):1
```

### Listing ping settings

You can use the `show ping settings` command to display ping results.

Example:

```
PING
Maximum rows in table: 20
```

## Showing ping Settings

The `show ping row <number>` command is an alternative to display ping statistics.

Example:

```
PING SETTINGS for ROW: 1 DESTINATION: www.cnn.com
Status:                               ACTIVE
Resolved IP Address:207.25.71.28
Count:      20
Interval:1
Size:      64
Timeout:20
Self Destroy Delay:10
```

Use the `delete ping row <number>` command to erase a row in the Remote Ping Table.

## Setting ping Row Ceiling

The `set ping maximum_rows` command sets the maximum number of rows permissible in the Remote Ping Table. Setting this parameter to a number smaller than the current number of rows will not cause any row deletions immediately but in the future. Default: 20. Range: 1-1000.

## Configuring a ping User

You can configure a ping user to test the connectivity of a specified login host using the `add user` command. This user pings a login host, gets a successful/unsuccessful message, and is disconnected. Use the following commands:

```
add user <username> type login
set user login user <username> login_service ping
login_host_name <host name>
```

## Viewing RAS 1500 System Information

You can use the `show system` command to see the firmware revision number, the date, and the time that this revision was compiled as well as other system information that may be useful when consulting 3Com Technical Support.

Example:

```
SYSTEM DESCRIPTION
System Descriptor:
SuperStack II Remote Access 1500
Built on Dec 19 1996 at 06:59:26.1.3.6.1.4.1.429.2.19
Object ID:
System UpTime:      2d 02:47:54
System Contact:     Larry Johnson
System Name:        RAS 1500
System Location:    westboro
System Services:    Internet EndToEnd
Applications
System Transmit Authentication Name: RAS 1500
System Version:     V1.5
```

## Viewing Interface Status, Settings

Several commands are useful to display the active/inactive status and settings of specific interfaces (ports). They are: `list switched interfaces`, `list interfaces` and `show interface settings`, and `show switched interface <rm0/slot[1-2]/mod:[1-y]>`.

## Monitor PPP Activity

The `monitor ppp` command lets you view the following real-time PPP activity:

- PPP call events
- Events on specific interfaces
- Events on the next session
- Events for specific users

Decode or hexadecimal output can be displayed.

---

## Displaying System Information

**List Commands** You can use `list` commands to view current configurations for all values stored in tables as well as facilities, files (FLASH memory configuration), and other data.

### List Critical Events

The `list critical events` command displays the last *ten* critical status events, and the system time when each occurred. You can change which events are displayed on the console and syslogged over Telnet sessions, using the `set facility` command, which is useful for troubleshooting and debugging.

**Show Commands** You can use `show` commands to view the current configuration and its routing activity. A few of the `show` commands used for troubleshooting are covered in this section, including `show memory`, `show connection settings`, `show connection counters`, and `show accounting settings`.

### Show Memory

The `show memory` command displays the system DRAM memory utilization.

Example:

```
SYSTEM MEMORY RESOURCES
Total System Memory Resources: 22387 KB
Free Memory:                    3584 KB
Code Size:                       2490 KB
Initialized Data Size:           0 KB
Uninitialized Data Size:         6080 KB
Stack Size:                      0 KB
```

### Show Dial-in Connection Settings and Counters

The `show connection` command summarizes settings and the number of incoming calls for dial-in connections. You can reset default settings with the `set connection` command.

```
show connection [settings] [counters]
```

Example:

```
CONNECTION SETTINGS
Host Selection Method:ROUND-ROBIN
Global User Name: default
Service Prompt: Login/Network User:
Message Prompt: manage:
```

- `Host Selection Method` — means of choosing a host. Choices are `round-robin` or `random`.
- `Global Username` — `default` is the default
- `Service Prompt` — displays when dial-in user is linked
- `Message Prompt` — prompts user for login/network service when (administrative) user.

### List Dial-in Connections

The `list connections` command displays all connections established on switched interfaces as configured with the `set connections` command. It lists:

- `IfName` — modem slot and interface of current connections
- `Username` — name of users currently connected
- `Type` — current type of connections established on modems. They include:
  - `On-demand` — user connection established for on-demand purposes
  - `Dial-back` — user connection established for callback purposes
  - `Continuous` — user connection established for continuous utilization
  - `Manual` — user connection established manually
  - `Timed` — user connection established for a particular interval
  - `ShrMod` (Shared-modem) — dial-out user connection to a modem utilizing a login service (Telnet or rlogin). LED does not light until call is unhooked (amber) and connected (green).
  - `Dial-in` — user connection established for dial-in purposes. LED lights *amber* when modem is unhooked, *green* when call is connected.
  - `Bond` — user connection utilizing bandwidth allocation
  - `Dedicated` — user connection established for a particular user



- **DLL** — data link layer that the specified dial-in session is connected to: NONE, PPP, SLIP, FCP, RLG, TLNT, PING, ADMN, CLTCP
- **Start Date** — start date of a connection established on the specified interface
- **Start Time** — start time of a connection established on the specified interface

Example:

CONNECTIONS

```
IfName User Name Type DLL Date Time Start Start
rm0/slot1/mod:2 ginger SHRMOD NONE 05-AUG-2041 13:57:2
rm0/slot1/mod:1 Larry DIALIN PPP 01-SEP-1997 00:34:25
rm0/slot1/mod:2 larry DIALIN NONE 05-AUG-2041 13:56:1
```



# 12

## USING SECURITY AND ACCOUNTING

This chapter contains the following:

- Authentication Overview
- Local Authentication
- RADIUS Authentication
- NOS Authentication
- RADIUS Accounting

---

### Authentication Overview

You can perform user authentication with either the SuperStack II Remote Access System (RAS) 1500 local authentication facility, Remote Authentication Dial-In User Service (RADIUS) authentication, network operating system (NOS) authentication, or local authentication and either RADIUS or NOS. The following list describes each option:

- **Local authentication only** — The RAS 1500 grants or denies access based on information in the local user table only.
- **RADIUS authentication only** — The RAS 1500 sends a request to the RADIUS server and grants or denies access based on the response.
- **NOS authentication only** — The RAS 1500 sends a request to the NOS authentication server and grants or denies access based on the response.
- **Local authentication and either RADIUS or NOS authentication** — The RAS 1500 first checks the local user table. If the user is defined in the local user table, the RAS 1500 grants or denies the user access based on information in the table. If the user is not defined in the user table, the RAS 1500 sends a request to the RADIUS or NOS authentication server and grants or denies access based on the response.

---

## Local Authentication

The RAS 1500 provides user authentication locally using a user table defined by the administrator. Local authentication is enabled by default.

To enable local authentication, use the following command line interface (CLI) command:

```
enable authentication local
```

To disable local authentication, use the following CLI command:

```
disable authentication local
```

To display authentication settings, use the one of the following CLI commands:

```
show authentication settings
```

or

```
show configuration
```

---

## RADIUS Authentication

**Overview** Use the RADIUS authentication for centralized authentication services on your network. RADIUS authentication is enabled by default.

The RADIUS authentication process consists of two parts: an authentication server and RADIUS client. The authentication server is installed on a machine on your network. The RAS 1500 acts as a RADIUS client, sending authentication requests to the authentication server, and acting on responses sent back from the authentication server.

The RAS 1500 software has built-in client support for RADIUS authentication. Because RADIUS is an open standard, many RADIUS server implementations are available. The RAS 1500 operates with most protocol implementations.

The RAS 1500 integrates the following enhanced RADIUS features:

- 128 challenge responses up to 128 bytes
- A filter rule format allowing filter names and rules to be downloaded to the RADIUS client
- Dynamic RADIUS server changes of a user filter rules
- Increased RADIUS security through RADIUS server verification of source IP address and UDP port
- Configuration of one secret and UDP port per server

### **RADIUS Authentication Process**

When a user dials into RAS 1500, and RADIUS authentication is enabled, the following occurs:

- 1 The RAS 1500 checks its own user table. If the RAS 1500 finds a local entry, the RAS 1500 grants or denies the user access based on information in the table. RADIUS authentication is not attempted. If the RAS 1500 cannot find a local entry, it uses the RADIUS server to authenticate the user.



*The preceding step is performed only if local authentication is enabled.*

- 2 The RAS 1500 encrypts the user's password using an encryption key shared by both the RAS 1500 and the RADIUS server, and passes the username and encrypted password to the RADIUS server.
- 3 The RADIUS server checks the username and password against its users file, determines whether to grant or deny access, and passes this information back to the RAS 1500.
- 4 If access is denied, the RAS 1500 disconnects the user. If access is granted, the RADIUS server forwards the appropriate user configuration information (such as what host or what protocol the user needs) to the RAS 1500.

### **CHAP Authentication Using RADIUS**

The username of the remote device must be the user ID it sends during Challenge Handshake Authentication Protocol (CHAP) authentication. The password must be in clear text for the MD5/MD4 comparison to succeed. This password is called a *shared secret*. The remote device uses the same password. If the RAS 1500 does not have a user table entry for the remote device, there must be an entry for the remote device in the RADIUS users file.

## Configuring RADIUS Authentication on the RAS 1500

This section provides procedures to configure RADIUS authentication through the CLI. You can also use the Web Configuration Interface to configure RADIUS authentication. Refer to the Web Configuration Interface online help for more information.

### Configuring RADIUS Authentication Settings

This section assumes the RADIUS authentication server is up and running on a computer on your network.

Use the following CLI command to configure RADIUS authentication settings:

```
set authentication
  primary_port <port_number>
  primary_secret <string>
  primary_server <name_or_ip_address>
  secondary_port <port_number>
  secondary_secret <string>
  secondary_server <name_or_ip_address>
  retransmissions <number>
  timeout <seconds>
  type <nos | radius>
```

Each of the following steps describes a parameter. An example is shown after the final step.

- 1 Set the authentication type. Use the following command:  

```
set authentication type radius
```
- 2 Select the primary RADIUS security server: Use the following command:  

```
set authentication primary_server <ip_address>
```
- 3 *Optional.* Select the secondary RADIUS security server. Use the following command:

If your network has more than one RADIUS server, indicate which one is considered the secondary server. If for some reason the primary server is unavailable, the RAS 1500 checks with the secondary server.

```
set authentication secondary_server <ip_address>
```

- 4 Set the primary encryption key or secret. Use the following command:

This is the first key the RAS 1500 uses to encrypt passwords and the RADIUS server uses to decrypt them. The RADIUS server(s) must be set to the same secret (encryption) key. The encryption key is entered into the clients file for the RADIUS server. The encryption key can be up to 15 characters long. See your RADIUS documentation for more information.

```
set authentication primary_secret <encryption key>
```

- 5 *Optional*. Set the secondary secret key. Use the following command:

```
set authentication secondary_secret <encryption key>
```

- 6 Set the number of *retransmissions*. This value is the total number of times the RAS 1500 retransmits an authentication request to both primary and secondary RADIUS servers. Use the following command:

```
set authentication retransmissions <count>
```

- 7 Set the UDP port to match the UDP port setting on the RADIUS server. The default is 1645. Use the following command:

```
set authentication primary_port <port_number>
```

or

```
set authentication secondary_port <port_number>
```

- 8 Set the interval (in seconds) between retransmissions. Use the following command:

```
set authentication timeout <number_seconds>
```

- 9 Configure authentication:

```
set ppp receive authentication [CHAP | PAP | either | none]
```

The following example configures authentication and saves the changes. (Three separate commands are shown.)

```
set authentication type radius primary_server 3.3.3.2
secondary_server 3.3.3.4 primary_secret nuncio
secondary_secret pope retransmissions 3 timeout 60
primary_port 5555 secondary_port 5556
```

```
set ppp receive authentication PAP
```

```
save all
```

### Enabling and Disabling Remote Authentication

Remote authentication is enabled by default. To set the *type* of remote authentication (RADIUS or NOS), see the previous procedure, “Configuring RADIUS Authentication Settings.”

To enable remote authentication (in this case, RADIUS), use the following CLI command:

```
enable authentication remote
```

To disable remote authentication, use the following CLI command:

```
disable authentication remote
```

### Displaying authentication settings

To display authentication settings, use one of the following commands:

```
show authentication settings
```

or

```
show configuration
```

---

## NOS Authentication

**Overview** NOS authentication is an alternative to RADIUS authentication for local and dial-in users using Novell or Windows NT networks. NOS authentication allows you to control network access by remote users through an existing network security mechanism.

NOS authentication has the following limitations:

- It does not support ARAP and PPP clients using CHAP authentication.
- Spaces are not allowed in the user ID and password fields.
- User ID and password fields are case-sensitive.
- The NOS authentication server does not assign configuration information to the user. Instead, the RAS 1500 assigns each NOS-authenticated user the “default” user profile.



## NOS Authentication Process

When a user dials into the RAS 1500 and NOS authentication is enabled, the following occurs:



*In these steps, the terms “security client” and “security server” refer to either a Novell NetWare or Windows NT platform.*

- 1 The RAS 1500 checks its own user table. If the RAS 1500 finds a local entry, the RAS 1500 grants or denies the user access based on information in the table. NOS authentication is not attempted. If the RAS 1500 cannot find a local entry, it uses the NOS authentication server to authenticate the user.



*The preceding step is performed only if local authentication is enabled.*

- 2 The RAS 1500 server generates a validation request to the security client.
- 3 The security client initiates an authentication session with the server.
- 4 Based on the result of the authentication session, the security client sends a validation response to the RAS 1500 server and indicates to the user that the authentication has failed or passed.
- 5 The RAS 1500 assigns the “default” user profile to the dial-in user.

## Installation Overview

For NOS authentication to operate correctly, perform the following steps (detailed in later sections):

- Install NOS authentication software on your Novell NetWare or Windows NT server. This chapter contains separate procedures for each type of server.



*The RAS 1500 Resource CD contains the NOS authentication software.*

- Configure the RAS 1500 to support NOS authentication (using the CLI). The procedure is the same for Novell NetWare and Windows NT servers.

## Installing and Configuring NOS Authentication Software (Novell NetWare)

The RAS 1500 Security Package-NetWare/Workgroup Version 1.2 software provides two NetWare Loadable Module (NLMS):

- The RAS 1500 Security Client for Novell NetWare Bindery Services (or, “bindery security client”), which is compatible with Novell NetWare Server 3.1x
- The RAS 1500 Security Client for Novell NetWare Directory Services (or, “NDS security client”), which is compatible with Novell NetWare Server 4.x or 5.x

These NLMs reside on their respective server. They provide the appropriate agent software to interface between the RAS 1500 and the respective security server.

### Installing the Software

- To install the Bindery/NDS Security Client on a NetWare server, do the following (on the Novell NetWare server):



- *You MUST load the software application on an Novell Server. The time on the RAS 1500 and the Novell NetWare server must be within 15 minutes of each other.*

- 1 Copy the appropriate security NLM (see below) from the RAS 1500 Resource CD to the sys:system directory on the Novell server:

- For NDS, Client\Security\Novell\SNDS.NLM
- For bindery, Client\Security\Novell\SBINDERY.NLM

- 2 Add TCP/IP to the Novell server.

- 3 On the Novell server, open the SYS:ETC\SERVICES file. In the "unix services" section of the file, add the following line:

```
crsecace 888/udp
```

## \etc\services example

```
# SYS:ETC\SERVICES
#
# Network service mappings. Maps service
# names to transport protocol and
# transport protocol ports.
#
echo                7/tcp
discard             9/tcp                sink null
systat              11/tcp
daytime             13/tcp
netstat             15/tcp
ftp-data            20/tcp
ftp                 21/tcp
telnet              23/tcp
smtp                25/tcp                mail
time                37/udp                timeserver
name                42/udp                nameserver
whois               43/tcp                nickname
domain              53/tcp
hostnames           101/tcp                hostname
sunrpc              111/udp
#
# Host specific functions
#
tftp                69/udp
finger              79/udp
link                87/udp                ttylink
x400                103/tcp
x400-snd            104/tcp
csnet-ns            105/tcp
pop-2               109/tcp
uucp-path           117/tcp
nntp                119/tcp                usenet
News                114/tcp                news
#
# UNIX specific services
#
# these are NOT officially assigned
#
exec                512/tcp
login               513/tcp
shell               514/tcp                cmd
printer             515/tcp                spooler # experiment
courier             530/tcp                rpc
```

biff	512/udp	comsat
who	513/udp	whod
syslog	514/udp	
talk	517/udp	
route	520/udp	router routed
new-rwho	550/udp	new-who
rmonitor	560/udp	rmonitor
monitor	561/udp	
ingreslock	1524/tcp	
snmp	161/udp	
snmp-trap	162/udp	
<b>crsecacc</b>	<b>888/udp</b>	

You may need to unload, then reload NetWare server to make the changes take effect.

- 4 Insert the distribution diskette into the floppy drive. Load the RAS 1500 Security Client for Bindery (sbindery.nlm), or for Novell Directory Services (NDS) (snds.nlm), (depending upon your NetWare Server version and which service is used).

#### **:load sbindery 3Com**

where **sbindery** is NLM name for the RAS 1500 Security Client for Novell NetWare Bindery. **3Com** is the default password for the RAS 1500 Security Client.

#### **:load snds 3Com**

where **snds** is NLM name for the RAS 1500 Security Client for Novell NetWare Directory Services. **3Com** is the default password for the RAS 1500 Security Client

- 5 On the Novell console, enter the appropriate command:

- For NDS:

```
:load snds < secret_password(key)> /c:< context_name>
debug
```

- For bindery:

```
:load sbindery < secret_password(key)> debug
```

To ensure the security client starts each time the system is rebooted, add the above commands in `autoexec.ncf` file:

- For NDS, add the command after TCP/IP, binding IP to an interface, and LOAD DSAPI.
- For bindery, add the command after TCP/IP and binding IP to an interface.

## NetWare Directory Example

```

set Time Zone = PST8PDT
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time = (APRIL SUNDAY FIRST
2:00:00 AM)
set End Of Daylight Savings Time = (OCTOBER SUNDAY LAST
2:00:00 AM)
set Default Time Server Type = SINGLE
set Bindery Context = O=b010
file server name SATURN
ipx internal net af0bfed9
load clib
load tcp/ip
load conlog
load 3C5X9 slot=5 frame=ETHERNET_802.2 NAME=3C5X9_1
bind IPX to 3C5X9_1 net=AA440000
load 3c5x9 slot=5 frame=ETHERNET_II name=3c5x9_2
bind ipx to 3c5x9_2 net=cc100001
load 3C5X9 slot=5 frame=ETHERNET_802.3 NAME=3C5X9_3
bind IPX to 3C5X9_3 net=AA330000
load 3c5x9 slot=5 frame=ETHERNET_SNAP name=3c5x9_4
bind ipx to 3c5x9_4 net=AA550000
bind IP to 3c5x9_2 addr=192.147.72.3 mask=255.255.255.0
set maximum concurrent directory cache writes = 50
set maximum directory cache buffers = 4000
load cpqhlth
load cdrom
cpqsnmp
mount all
unload conlog
load monitor
#####
# RAS 1500 NetWare Security Client Software
#####
load sbindery 3Com

```

- 6 Add the user on the Novell system.

### Changing the encryption key

For security reasons, the messages between the RAS 1500 and the Novell server are encrypted with an encryption key.

To change the encryption key, follow these steps:

- 1 Unload the security client on the Novell server:

```
UNLOAD SNDS or UNLOAD SBIN "secret"
```

- 2 Reload the security client on the server with the new secret.

```
LOAD SNDS "secret_password(key)"c:\"context_name" debug
```

or

```
LOAD SBINDERY "secret_password(key)" debug
```



*The RAS 1500 does NOT support CHAP authentication with Novell NOS Authentication. This means that the password sent by the client to the RAS 1500 is not encrypted. The password sent from the RAS 1500 to the Novell Security Client is encrypted as described above.*

### **Installing and Configuring NOS Authentication Software (Windows NT)**

The RAS 1500 NT Security Client 1.1 application software provides centralized user logon authentication service for the RAS 1500 on an NT workstation. The advantage of this authentication mechanism is that a large number of user accounts can be easily administered on NT user account database with NT User Account Manager.

This application software is a NT service that processes authentication requests from the RAS 1500. The NT Security Client uses a 3Com proprietary communication protocol to communicate with the RAS 1500. This protocol, which runs on top of registered UDP service "crsecacc", provides secured end-to-end communication services such as messages encryption and the protection against message replay.

When an RAS 1500 is setup to use NT authentication service, the logon username and password are forwarded to the designated NT workstation for authentication. After receiving the authentication request, the RAS 1500 Security Client uses the NT Security Support Provider (SSP) library to perform authentication against NT user account database. Once the authentication is complete, the RAS 1500 Security Client sends the results back to the RAS 1500.

This application software has to run on NT 3.51 or later release. In addition, the NT workstation has to have TCP/IP service installed.

Depending on the NT workstation setup, the user authentication can be performed on three different databases:

- The local user accounts database, if the workstation is setup as a workgroup or as a member of a domain and the user login name matches one of the user account names in the user account database.
- The user account database on the NT Domain Controller, if the NT workstation is setup as a member of a NT domain and the user login name does not exist in the local user account database.
- The user account database on the trusted NT Domain Controller, if the user account on the trusted Domain Controller has the user right of "log on locally" to the NT workstation that runs the RAS 1500 NT Security Client.

Use the following steps to install and configure NOS authentication software on a Windows NT server or workstation:



*The time on the RAS 1500 and the Windows NT server must be within 15 minutes of each other. If you change the time on a Windows NT Server, you must reboot the server for the change to take effect.*

- 1 Insert the RAS 1500 Resource CD into the Windows NT server or workstation.
- 2 Locate Client\Security\NT\Setup.exe.
- 3 Double-click SETUP.EXE. The software loads.
- 4 From the Windows NT desktop, click *Start*, then *Programs*, then *Accessbuilder WIN NT Security*, then *Enable Authentication*.
- 5 Follow the directions to enable the service on the NT platform. This ensures the service starts each time the machine is rebooted.
- 6 On the Windows NT platform, do the following:
  - a Add the user.
  - b Assign the user to the appropriate groups.
  - c Confirm the user is configured to allow dial-in access.
  - d Login to the LAN network using this user to ensure that the user is present and operating correctly.
- 7 Reboot the Windows NT server or workstation.

The RAS 1500 does not support MS-CHAP authentication with Windows NT NOS authentication.



Users must logon locally to allow the user to use Windows NT security with the RAS 1500. For example, follow these steps:

- 1 Log on to the NT Server as Administrator.
- 2 Open the Administrative Tools Program Group.
- 3 Double-click the User Manager for Domains Program Group icon. The User Manager screen appears.
- 4 Click the single or multiple users you want to assign remote-access rights.
- 5 In the User Rights from *Policies* list, select "logon locally."
- 6 Click OK.

Table 52 shows NT event viewer messages that help when troubleshooting the RAS 1500.

**Table 52** Event Viewer Messages

Message ID	Message
1	Security Service installed successfully
2	Security Service disabled
3	Security Service enabled successfully with encryption key ( <i>key</i> )
4	Security Service stopped
5	User successfully authenticated <i>user</i> RAS 1500 IP Address
6	User failed to authenticate <i>user</i> RAS 1500 IP Address

### Changing Encryption Key

For security reason, the messages communicated between the RAS 1500 and the NT Security Client are encrypted with an Encryption Key. The default Encryption Key is "3com". The Encryption Key is stored in the NT Registry database in the entry of "EncryptionKey", under the subkey HKEY\_LOCAL\_MACHINE\system\CurrentControlSet\Services\ABSecurityClient.

You can change the default encryption key by using NT Registry Editor. If you change the encryption key, make sure that you also update the *ScrtCIntPasswd* parameter in the RAS 1500.

If the NT Security Client is already running when you change the encryption key, you must disable the NT Security Client service and re-enable the service for the changes to take effect.

## Configuring NOS Authentication on the RAS 1500

Complete the following procedures to configure NOS authentication on the RAS 1500. You can also use Web Configuration Interface to configure NOS authentication. Refer to the Web Configuration Interface online help for more information.

### Setting NOS Authentication Parameters

Use the following steps to configure NOS authentication:

- 1 Set NOS authentication:

```
set authentication type nos
```

- 2 Configure the primary NOS authentication server:

```
set authentication primary_server [domain name or ip address]  
primary_port 888 primary_secret 3com
```



*The industry standard port setting for NOS authentication server is 888. Your NOS authentication server may differ. If you want to change the primary\_secret, refer to the readme file provided with the Security application.*

- 3 Configure the secondary NOS authentication server:

```
set authentication secondary_server [domain name or ip  
address]  
secondary_port 888 secondary_secret 3com
```



*The industry standard port setting for NOS authentication server is 888. Your NOS authentication server may differ. If you want to change the secondary\_secret, refer to the readme file provided with the Security application.*

- 4 Configure the number of server retransmissions:

```
set authentication retransmissions [0-100]
```

- 5 Configure PPP parameters:

```
set ppp receive_authentication pap
```

- 6 Save your work:

```
save all
```

### Enabling and Disabling Remote Authentication

Remote authentication is enabled by default. To set the *type* of remote authentication (RADIUS or NOS), see the previous procedure, "Configuring RADIUS Authentication Settings."

To enable remote authentication (in this case, NOS), use the following CLI command:

```
enable authentication remote
```

To disable remote authentication, use the following CLI command:

```
disable authentication remote
```

### Displaying Authentication Settings

To display authentication settings, use one of the following commands:

```
show authentication settings
```

or

```
show configuration
```

### Setting the Time Zone

Use the following command to specify the time zone (GMT offset) of the RAS 1500. This setting is between -12:00 and +14:00, inclusive.

```
set timezone <+/-hh:mm>
```



See Appendix A, “GMT Time Zones” to find the GMT offset for your location.

Eastern United States example:

```
set timezone -5:00
```

### Setting Daylight Saving Time

Configuring daylight saving time (DST) on the RAS 1500 requires two steps. First, set the begin time, end time, and adjustment for DST. Second, enable DST.



Only those time zones impacted by DST need to enable this parameter.

Use the following command to set specify when DST begins and the time adjustment to make:

```
set dst on week_of_month <1-5> day_of_week <day> month  
<month> time_to_correct <time> amount_to_correct <amount>
```

For example, to begin DST on the first Sunday of April at 2:00 AM and adjust 1 hour:

```
set dst on week_of_month 1 day_of_week sunday month april
time_to_correct 02:00:00 amount_to_correct 01:00:00
```

Use the following command to set specify when DST ends and the time adjustment to make:

```
set dst off week_of_month <1-5> day_of_week <day> month
<month> time_to_correct <time> amount_to_correct <amount>
```

The following example ends DST on the last Sunday of October at 2:00 AM and adjusts 1 hour:

```
set dst off week_of_month last day_of_week sunday month
october time_to_correct 02:00:00 amount_to_correct 01:00:00
```

Use the following command to enable DST on the RAS 1500:

```
enable dst
```

### Setting the Date

Use the following command to set the date on the RAS 1500:

```
set date <dd-mon-yyyy>
```

Example:

```
set date 10-jan-1999
```

### Setting the Time

For the RAS 1500 and the NOS authentication server to operate correctly together, set their system times within 15 minutes of each other. The RAS 1500 expresses time in 24-hour format. Use the following command to set the time on the RAS 1500:

```
set time <hh:mm:ss>
```

The following example sets the time to 1:00:00 PM:

```
set time 13:00:00
```

### Displaying the Date and Time Settings

To display the date, time, and GMT offset settings, use the following command:

```
show timezone
```

To display the daylight saving time settings, use the following command:

```
show dst
```

### Save Your Work

To save your work, use the following command:

```
save all
```

## Troubleshooting NOS Authentication

If NOS authentication does not operate properly, verify the following:

- The time on the NOS authentication server and the RAS 1500 are within 15 minutes of each other.
- The GMT offset and daylight saving time settings are the same on the NOS authentication server and the RAS 1500.
- The settings for IP address and port number of the primary and secondary NOS authentication servers are correct.

---

## RADIUS Accounting

The RAS 1500 performs local session accounting using a user table defined by the administrator.

The RAS 1500 sends frames to the RADIUS accounting server that enables RADIUS to perform accounting functions. The RADIUS accounting server uses the same basic protocol as the RADIUS authentication server. You can run both servers on the same host, or you can choose a different host to provide each function.

The RADIUS accounting server performs session accounting for the stack. Session accounting information includes date and time, user information, and service type. When RADIUS accounting is enabled, the RAS 1500 forwards an accounting record of each session for storage on the accounting server.



*The RAS 1500 SYSLOG facility also performs local session accounting.*

The accounting server creates a separate account file for each RAS 1500 in the following directory:

```
/usr/adm/radacct/<RAS 1500-hostname>/detail
```



*Your configuration may differ depending on your RADIUS server implementation.*

This section describes:

- Configuring RADIUS accounting settings
- Enabling and disabling RADIUS accounting
- RADIUS accounting examples

## Configuring RADIUS Accounting

Use the following CLI command to configure RADIUS accounting settings:

```
set accounting
    primary_port <port_number>
    primary_secret <string>
    primary_server <name_or_ip_address>
    retransmissions <count>
    secondary_port <port_number>
    secondary_secret <string>
    secondary_server <name_or_ip_address>
    start_time <authentication | connection
    timeout <seconds>
    use_servers <one | both>
```

Configure RADIUS accounting parameters by setting the following values. Each step describes a parameter. An example is shown after the final step.

- 1 Select the primary RADIUS accounting server. Use the following command:

```
set accounting primary_server <ip_address>
```

- 2 *Optional.* Select the secondary RADIUS accounting server. If your network has more than one RADIUS accounting server, indicate which one is considered the secondary server. If for some reason the primary server is unavailable, the RAS 1500 checks with the secondary server. Use the following command:

```
set accounting secondary_server <ip_address>
```

- 3 Set the primary and secondary secret (encryption) keys.

These are the first and secondary encryption key that the RAS 1500 uses to encrypt passwords and the RADIUS server uses to decrypt them. Specify with a string of up to 15 ASCII characters for each server. Use the following commands:

```
set accounting primary_secret <string>
set accounting secondary_secret <string>
```

- 4 Determine whether accounting information is sent to the primary server only (the secondary server acts as a backup) or whether accounting information is sent to both the primary and secondary servers until a response is received from both servers. Use the following command:

```
set accounting use_servers [ONE | BOTH]
```

- 5 Set the number of retransmissions. This is the total number of times the RAS 1500 retransmits an authentication request to both the primary and secondary RADIUS servers. Use the following command:

```
set accounting retransmissions <count>
```

- 6 Set the time at which the RAS 1500 begins accounting, either at the point of authentication or the point of connection. Use the following command:

```
set accounting start_time [authentication | connection]
```

- 7 Set the interval (in seconds) between retransmissions. Use the following command:

```
set accounting timeout <number_seconds>
```

- 8 Set the UDP port to match the UDP port setting on the RADIUS server. The default is 1646. Use the following command:

```
set accounting primary_port <port_number>  
set accounting secondary_port <port_number>
```

The following example configures accounting and saves the changes. (Two separate commands are shown.)

```
set accounting primary_server 2.2.2.2 secondary_server  
2.2.2.3 primary_secret bishop secondary_secret cardinal  
use_servers both retransmissions 3 start_time connection  
timeout 60 primary_port 4444 secondary_port 4445
```

```
save all
```

## Enabling and Disabling RADIUS Accounting

RADIUS accounting is enabled by default. It can be enabled or disabled from the CLI.

To enable RADIUS accounting, use the following CLI command:

```
enable accounting
```

To disable RADIUS accounting, use the following CLI command:

```
disable accounting
```



*SYSLOG accounting is always enabled as long as a SYSLOG sink is defined.*

Below are some examples of RADIUS accounting output. The first describes a login user who has just begun a session.

```
Thurs Jan 16 22:00:55 1999
Acct-Session-ID="06000003"
User-Name=cindyg
Acct-Status-Type=Start
Acct-Authentic=RADIUS
User-Service-Type=Login-User
Login-Host=NY_Sales
Login-Service=Telnet
```

When the user above ends the session with the host, a record similar to the one below is sent to the accounting server:

```
Thurs Jan 16 23:15:31 1999
Acct-Session-Id="06000003"
User-Name=cindyg
Acct-Status-Type=Stop
Acct-Authentic=RADIUS
Acct-Session-Time=4476
User-Service-Type=Login-User
Login-Host=NY_Sales
Login-Service=Telnet
Acct-Delay-Time=0
```



If a PPP or SLIP (framed) user begins a session with the network, a record similar to the one below is sent to the accounting server:

```
Thurs Jan 16 16:15:53 1999
Acct-Session-Id="06000004"
User-Name=harryk
Client-Id=201.123.234.79
Client-Id-Port=5
Acct-Status-Type=Start
Acct-Authentic=Local
User-Service-Type=Framed-User
Framed-Protocol=PPP
Framed-Address=122.132.124.152
Framed-Netmask=255.255.124.0
```

When the framed user ends the session, a record similar to the one below is sent to the accounting server:

```
Thurs Jan 16 16:25:57 1999"
Acct-Session-Id="06000004"
User-Name=harryk
Client-Id=201.123.234.79
Client-Id-Port=5
Acct-Status-Type=Stop
Acct-Session-Time=664
Acct-Authentic=Local
User-Service-Type=Framed-User
Framed-Protocol=PPP
Framed-Address=122.132.124.152
Framed-Netmask=255.255.124.0
Acct-Delay-Time=0
```



# 13

## USING FRAME RELAY

This chapter contains the following information:

- Overview
- Before You Begin
- Basic Frame Relay Configuration Using the Command Line Interface
- Frame Relay Data Link Configuration
- Frame Relay PVC Configuration
- Monitoring and Troubleshooting
- Case Study



*The Frame Relay Stack complies with the Idacom Conformance Test Suite. When ordering Frame Relay service, tell your Frame Relay service provider.*

---

**Overview**

The SuperStack II Remote Access System 1500 (RAS 1500) supports a Frame Relay interface to a wide area network (WAN). This allows for dedicated high throughput, low error connectivity to remote locations using public or private Frame Relay. Frame Relay technology is standardized and supported by a variety of remote access devices allowing the RAS 1500 to operate with remote access device from other manufacturers.

**What is Frame Relay?**

Frame Relay is a data-link layer protocol that provides for frame/packet switched wide area networking. It operates at the physical and data-link layers of the OSI model, so it is transparent to the network layer. It uses statistically multiplexed virtual circuits within a single physical bearer. Each of the circuits can be configured to provide a guaranteed throughput and allow for bursts of extra traffic.

Frame Relay supports “congestion management,” which attempts to notify endpoints that the network is experiencing congestion and that the volume of traffic should be reduced to stop Frame Relay nodes from discarding frames.

Frame Relay reduces its error-correction overhead by assuming high-quality transmission lines and relying on the endpoints to detect and correct transmission errors. This reduces the latency to packet throughput within the Frame Relay network.

Frame Relay operates at speeds up to 2.048 Mbps. Typically, Frame Relay services are provided by a public carrier such as your telephone company. However, some organizations, such as large corporations or governments have created private Frame Relay networks of their own.

**Permanent and Switched Virtual Circuits**

Frame Relay uses both permanent virtual circuits (PVCs) and switched virtual circuits (PVCs) to connect locations. The RAS 1500 currently supports only PVCs.

**Data Link Connection Identifier**

Each Frame Relay frame is addressed to its destination using the Data Link Connection Identifier (DLCI). A DLCI identifies each end of the PVC.

<b>Committed Information Rate</b>	Frame Relay controls the data throughput rate with the Committed Information Rate (CIR) parameter. CIR is the data rate the carrier guarantees without data loss. CIR is determined at the time the Frame Relay circuit is ordered and typically determines the cost of the Frame Relay service. Bursting above the CIR is allowed by most carriers however data in excess of the CIR may be discarded by the carrier in case of congestion on the Frame Relay network.
<b>Forward and Backward Explicit Congestion Notifications</b>	Frame Relay employs a method of flow control using Forward Explicit Congestion Notification (FECN) and Backward Explicit Congestion Notification (BECN) to control data loss when a network is congested. By sending a FECN the receiving station is notified of network congestion. A BECN notifies the sending station when there is network congestion. The routers and switches can then reduce the data rate until congestion is no longer reported. Thus reducing discarded data due to congestion.
<b>Local Management Interface</b>	Frame Relay devices such as routers and switches manage the Frame Relay interface the using Local Management Interface (LMI). LMI provides a polling mechanism that allow switches and routers to request the status of all PVCs on a given interface.
<b>Supporting Frame Relay</b>	The RAS 1500 provides a synchronous serial interface capable of supporting data rates between 9.6 kbps and 2.048 mbps. The RAS 1500 routes IP and IPX over Frame Relay. The RAS 1500 supports RFC 1490, which is a standard that provides for routing of multiple protocols over a single Frame Relay link. RFC 1490 also provides for interoperability with Frame Relay equipment from other manufacturers.
<b>Congestion Control</b>	The RAS 1500 automatically reduces the Committed Burst Size (Bc) to control congestion when it receives too many BECN frames. The RAS 1500 uses BECN Monitoring to determine if more BECN frames than non-BECN are received during a BECN Congestion Monitoring Period (BECN_CMP). When the number of BECN frames is greater than the number of non-BECN frame, the RAS 1500 adjusts the Committed burst size downward. Each downward adjustment is equal to 1/8 of the difference between Bc_MAX and Bc_MIN until the Bc_MIN value is reached. When congestion is no longer occurring and the number of non-BECN frames is greater than the number of BECN frames the unit will begin to adjust Bc upward in steps of 1/16 of the difference between Bc_MAX and Bc_MIN until Bc_MAX is reached. For more information on Frame Relay Terminology see Table 53.

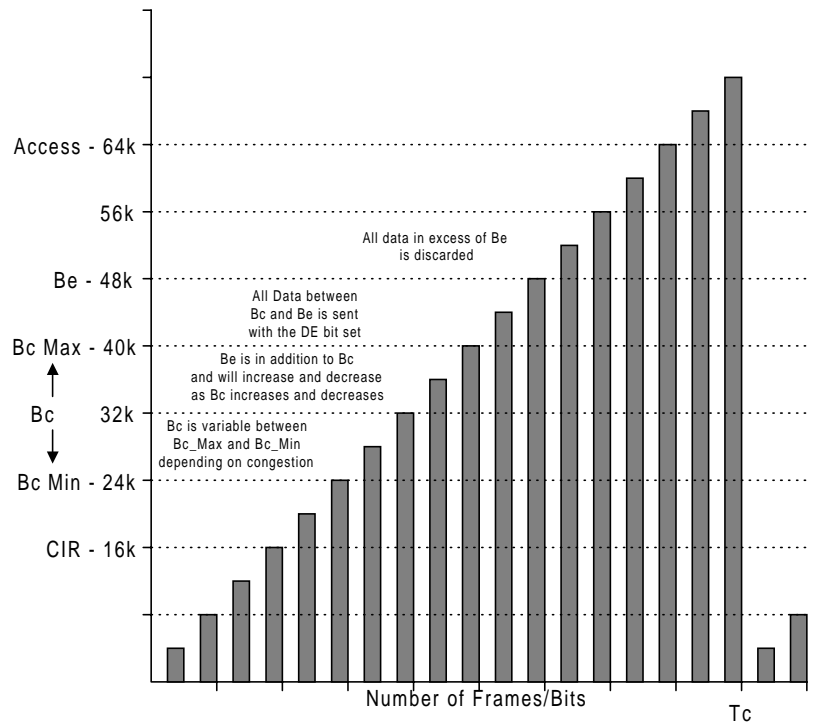
**Table 53** Frame Relay Terminology

Abbreviation	Term	Description
Bc	Committed Burst Size	The number of bits above CIR that are transmitted during a time interval Tc without setting the DE bit.
Be	Excess Burst Size	The number of Bits that are transmitted during a time interval Tc in excess of Bc that will have the DE bit set.
Tc	Committed Rate Measurement Interval	The time interval in which Bc and Be are measured. See formulas below.
DE	Discard Eligible	A bit in the Frame Relay frame informing the network that the frame can be discarded in case of congestion.
CIR	Committed Information Rate	The data rate the carrier guarantees without data loss. Bursting above the CIR is allowed by most carriers, but data in excess of the CIR may be discarded by the carrier in case of congestion on the Frame Relay network.

### How Congestion Control Works

The chart below illustrates the congestion control process. This example assumes that all Frames are 4 k bits in size. Figure 13 shows what happens as the number of transmitted bits increases during the Committed Rate Measurement Interval (Tc). When 16 k bits have been transmitted, CIR is reached.

After CIR is reached, the unit begins to count bits until Bc is reached at 24 k bits. Once Bc is reached between 24k bits and 40k bits depending on congestion levels all data is marked with the Discard Eligible (DE) bit set. This allows the network to discard these frames if congestion is encountered. At 48 k bits the Excess Burst Size (Be) is reached. Any data in excess of Be is discarded. All data is discarded until a new Tc begins.



**Figure 13** Frame Relay Congestion Control

---

## Before You Begin

Before you configure the RAS 1500 for Frame Relay you must determine the following information:

- LMI protocol used: Annex A, Annex D, or LMI
- DLCIs of all PVCs on the Frame Relay network
- CIR monitoring support
- CIR of each PVC
- Protocols supported over the Frame Relay line
- Network addresses for the protocols routed over Frame Relay

---

## Basic Frame Relay Configuration Using the Command Line Interface

Once you have obtained all required information, installed the RAS 1500, and configured all required system level parameters, you are ready to begin configuring the RAS 1500 to use Frame Relay.

There are three basic components to a Frame Relay configuration:

- Frame Relay user
- Frame Relay data link
- PVC/User mappings

The parameters specified in these components define the physical Frame Relay interface, the protocols to routed over Frame Relay and the relationship between Frame Relay users and an individual PVC.

## Frame Relay User Configuration

Use the following steps to configure a Frame Relay user:

- 1 Add a Frame Relay user.

```
add user <username> type network,dial_out network_service  
fr_1490
```

- 2 Specify the user network parameters.

```
set network user <username> ip [enable | disable] ipx [enable  
| disable] appletalk enable | disable] bridging disable
```



### 3 Specify additional network parameters for the user.

- a** If you are configuring an unnumbered interface, use the following command:

```
set network user <username> remote_ip_address
<xxx.xxx.xxx.xxx/x>
```

The `remote_ip_address` for an unnumbered link may be the IP address of the remote router Ethernet port, depending on the configuration of the remote router.

- b** If you are configuring a numbered interface, use the following command:

```
set network user <username> remote_ip_address
<xxx.xxx.xxx.xxx/x>
set dial_out user <username> local_ip_address
<xxx.xxx.xxx.xxx>
```

The `remote_ip_address` for a numbered link is the IP address of the remote router WAN port. The `local_ip_address` is the IP address of the local router WAN port.

### 4 Set the user routing options as follows. For a command description see Table 54.

```
set network user <username> ip_routing [both | send | listen
| none] rip [ripv1 | ripv2]
```

**Table 54** IP Routing Levels

Command	RAS 1500
Listen	Listens to RIP updates from the user and updates the local routing table
Send	Sends RIP updates to the user
Both	Listens to and send RIP updates
None	Does not listen to nor send RIP updates

### 5 For IPX, specify the network address, WAN status, routing options, and spoofing status.

```
set network user <username> ipx_address <ipx net address>
ipx_wan [enable | disable] ipx_routing [all | listen | none |
respond | send] spoofing [enable | disable]
```

### 6 For IPX, specify an internal IPX system number to support IPX\_WAN.

```
set ipx system number <number> name <system name>
```

## Frame Relay Data Link Configuration

Use the following steps to configure the Frame Relay data link:

- 1 Add the Frame Relay data link.

```
add datalink frame_relay interface rm0/wan:1 enabled yes
```

- 2 Configure the following interface-level parameters:

```
set frame_relay on interface rm0/wan:1
    access_rate [0-2048000]
    management_type [ansi | itu | lmi | no_lmi]
    mtu [260-2048]
```



*Both ends of the Frame Relay link must be configured for the same management type, otherwise the link is assumed to have failed.*

- 3 Configure optional advanced configuration parameters.

```
set frame_relay on interface rm0/wan:1
    error_theshold [1-10]
    full_enquiry_interval [1-255]
    monitored_events [1-10]
    polling_interval [5-30]
```



*The parameters in Table 55 do not usually need modification. They are based on the management type configured in Step 2.*

**Table 55** Frame Relay Parameters

Parameter	Description
access_rate	Speed in bits per second of the Frame Relay access line.
management_type	Type of LMI protocol used by the Frame Relay carrier: <ul style="list-style-type: none"> <li>■ ANSI - ANSI T1.617 Annex D</li> <li>■ ITU - ITU Q.933 Annex A</li> <li>■ LMI - LMI rev.1</li> <li>■ No LMI - Turns off the LMI protocol</li> </ul>
mtu	Maximum transmission unit - Maximum size of a Frame Relay packet.
error_threshold	Maximum number of unanswered LMI Status Inquiries the RAS 1500 will accept before the access line is declared down.
full_enquiry_interval	Number of LMI Status Inquiries before a Full Status Inquiry is issued.
monitored_events	Sets the number of status polling intervals over which the error threshold is counted.
polling_interval	Number of seconds between LMI Status Inquiries.

## Frame Relay PVC Configuration

To route over Frame Relay, users must be mapped to the correct PVC. This ensures that the correct IP and IPX addresses are associated with the correct PVC.

On the RAS 1500, a user profile defines most aspects of the WAN connection across a Frame Relay link. A PVC definition describes the Frame Relay portion of the WAN connection. The PVC definition includes a reference to the associated user profile.



*There is one PVC per user. You must create a user for each PVC that you configure.*

Use the following steps to configure the Frame Relay PVC:

- 1 Add the Frame Relay PVC and DLCI, and associated user profile.

```
add frame_relay pvc <pvc name> dlci <dlci number> interface
rm0/wan:1 user <username>
```

Example:

```
add frame_relay pvc chicago dlci 16 interface rm0/wan:1 user
tom
```

- 2 Configure the optional PVC parameters () as required. The following defaults are recommended:

```
set frame_relay pvc [pvc name]
    bc_max [0-2048000]
    bc_min [0-2048000]
    be [0-2048000]
    becn_cmp [1-100]
    becn_monitoring [on/off]
    cir [0-2048000]
    cir_monitoring [on/off]
```

**Table 56** Optional PVC Parameters

<b>Parameter</b>	<b>Term</b>	<b>Description</b>
<code>bc_max</code>	Maximum Committed Burst Rate	When BECN Monitoring is enabled this value is used as the starting point for Bc calculations. Bc is the number of bits a PVC is allowed to burst above CIR during a Committed Rate Measurement Interval (Tc). Any data in excess of Bc is marked DE.
<code>bc_min</code>	Minimum Committed Burst Rate	This is lowest possible value for Bc. The Bc algorithm may not calculate a Bc lower than <code>bc_min</code> .
<code>be</code>	Excess Burst Size	The number of bits above Bc that a PVC is allowed to burst. All data above Bc is marked DE. Any data in excess of Be is discarded.
<code>becn_cmp</code>	Backward Explicit Congestion Notification Congestion Monitoring Period	The number of seconds in each BECN Monitoring Interval.
<code>becn-monitoring</code>	Backward Explicit Congestion Notification Monitoring	Determines the ratio of BECN frames to non-BECN frames during a <code>becn_cmp</code> . If there are more BECN frames than non-BECN frames Bc is adjusted lower.
<code>cir</code>	Committed Information Rate	The rate in bits per second that the carrier guarantees for a given PVC.
<code>cir_monitoring</code>	Committed Information Rate Monitoring	If enabled, the RAS 1500 will monitor the throughput for a given PVC and calculate Bc in conjunction with <code>becn_monitoring</code> . If disabled the PVC is allowed to send data at up to the access line rate.

---

## Monitoring and Troubleshooting

There are several ways to monitor and troubleshoot your RAS 1500.

### Show the Settings at the Interface Level

Use the following command to show the setting at the interface level:

```
show frame_relay on interface rm0/wan:1 settings
show frame_relay on interface rm0/wan:1 counters
show frame_relay on interface rm0/wan:1 lmi_statistics
```

### Show the Settings at the PVC Level

Use the following command to show the setting at the PVC level:

```
show frame_relay pvc <pvc name> settings
```

### List PVC Statistics

Use the following command to display a list of PVC statistics:

```
show frame_relay pvc <pvc name> counters
```

### List the Status of all Frame Relay PVCs

Use the following command to list the status of all Frame Relay PVCs:

```
list frame_relay
```

---

## Case Study

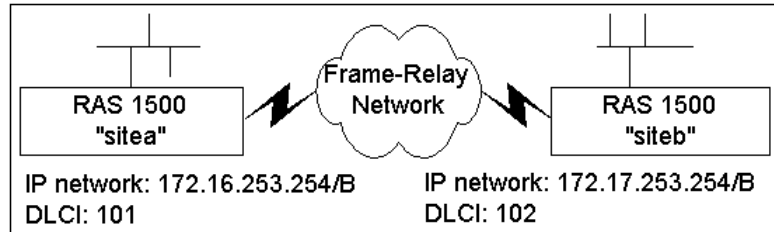
**Goal** Use a Frame Relay link to connect the "sitea" RAS 1500 (located at Site A) to the "siteb" RAS 1500 (located at Site B).

- Assumptions**
- Each site has a functioning RAS 1500.
  - Use the RIPv1 routing protocol.
  - Each site has separate IP network: Site A has 172.16.0.0/B; Site B has 172.17.0.0/B.
  - The Frame Relay service has assigned a DLCI for each site. Site A is 101; Site B is 102.
  - The Frame Relay service provider provides a CIR as negotiated for the two sites with the service provider.

**Strategies** The goals can be achieved in two ways: an unnumbered IP link between the sites (strategy 1 below) or a numbered IP link between the sites (strategy 2 below).

### Strategy 1 (unnumbered link)

Configuring the RAS 1500 for Site A:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network sitea interface rm0/eth:1 address
172.16.253.254/b
```

- 2 Set the IP network routing protocol.

```
set ip network sitea routing_protocol ripv1
```

- 3 Enable the IP network.

```
enable ip network sitea
```

- 4 Add a Frame Relay user.

```
add user siteb type network network_service fr_1490 enabled
no
```

- 5 Set the user protocol settings.

```
set network user siteb ip enable ipx disable appletalk
disable bridging disable
```

- 6 Set the user remote IP address.

```
set network user siteb remote_ip_address 172.17.253.254/b
```

- 7 Set the user routing settings.

```
set network user siteb ip_routing both rip ripv1
```

- 8 Enable the user.

```
enable user siteb
```

- 9 Configure the Frame Relay data link.

```
add datalink frame_relay interface rm0/wan:1 enabled yes
```

- 10 Configure a Frame Relay PVC and associate a user with it.

```
add frame_relay pvc atob dlci 101 interface rm0/wan:1 user
siteb enabled yes
```

- 11 Save your work.

```
save all
```

Configuring the RAS 1500 for Site B:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network siteb interface rm0/eth:1 address
172.17.253.254/b
```

- 2 Set the IP network routing protocol.

```
set ip network siteb routing_protocol ripv1
```

- 3 Enable the IP network.

```
enable ip network siteb
```

- 4 Add a user.

```
add user sitea type network network_service fr_1490 enabled
no
```

- 5 Set the user protocol settings.

```
set network user sitea ip enable ipx disable appletalk
disable bridging disable
```

- 6 Set the user remote IP address.

```
set network user sitea remote_ip_address 172.16.253.254/b
```

- 7 Set the user routing settings.

```
set network user sitea ip_routing both rip ripv1
```

- 8 Enable the user.

```
enable user sitea
```

- 9 Configure the Frame Relay datalink.

```
add datalink frame_relay interface rm0/wan:1 enabled yes
```

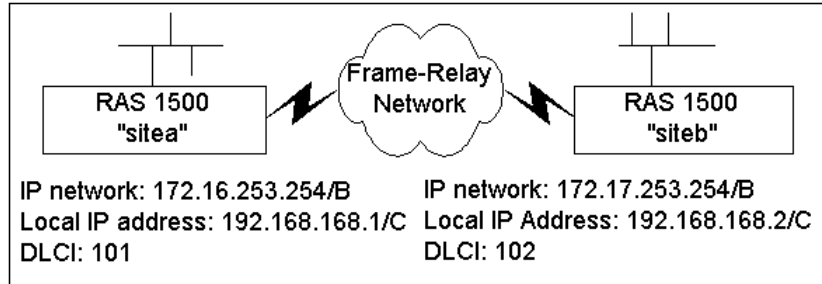
- 10 Configure a Frame Relay PVC and associate a user with it.

```
add frame_relay pvc btoa dlci 102 interface rm0/wan:1 user
sitea enabled yes
```

- 11 Save your work.

```
save all
```

### Strategy 2 (numbered link)



Configuring the RAS 1500 for Site A:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network sitea interface rm0/eth:1 address
172.16.253.254/b
```

- 2 Set the IP network routing protocol.

```
set ip network sitea routing_protocol ripv1
```

- 3 Enable the IP network.

```
enable ip network sitea
```

- 4 Add a Frame Relay user.

```
add user siteb type network,dialout network_service fr_1490
enabled no
```

- 5 Set the user network parameters.

```
set network user siteb ip enable ipx disable appletalk
disable bridging disable
```

- 6 Set the user WAN link IP address.

```
set network user sitea remote_ip_address 192.168.168.2/c
set dial_out user sitea local_ip address 192.168.168.1
```

- 7 Set the user routing settings.

```
set network user siteb ip_routing both rip ripv1
```



- 8 Configure the user dial-out parameters.  
`set dial_out user siteb local_ip address 192.168.168.1`
- 9 Enable the user.  
`enable user siteb`
- 10 Configure the Frame Relay datalink.  
`add datalink frame_relay interface rm0/wan:1 enabled yes`
- 11 Configure a Frame Relay PVC and associate a user with it.  
`add frame_relay pvc atob dlci 101 interface rm0/wan:1 user siteb enabled yes`
- 12 Save your work.  
`save all`

Configuring the RAS 1500 for Site B:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.  
`add ip network siteb interface rm0/eth:1 address 172.17.253.254/b`
- 2 Set the IP network routing protocol.  
`set ip network siteb routing_protocol ripv1`
- 3 Enable the IP network.  
`enable ip network siteb`
- 4 Add a Frame Relay user.  
`add user sitea type network,dialout network_service fr_1490 enabled no`
- 5 Set the user network parameters.  
`set network user sitea ip enable ipx disable appletalk disable bridging disable`
- 6 Set the user WAN link IP address.  
`set network user sitea remote_ip_address 192.168.168.1/c  
set dial_out user sitea local_ip address 192.168.168.2`
- 7 Set the user routing settings.  
`set network user sitea ip_routing both rip ripv1`

- 8 Enable the user.  
`enable user sitea`
- 9 Configure the Frame Relay datalink.  
`add datalink frame_relay interface rm0/wan:1 enabled yes`
- 10 Configure a Frame Relay PVC and associate a user with it.  
`add frame_relay pvc btoa dlci 102 interface rm0/wan:1 user sitea enabled yes`
- 11 Save your work.  
`save all`

# 14

## HANDLING PACKET FILTERS

This chapter describes how to set up packet filters on the SuperStack II Remote Access System (RAS) 1500. The following topics are discussed:

- Filtering Overview
- Filter Types
- Creating Filters
- Configuring Filters
- Managing Filters
- General Filter Setup
- Filter Examples



*This chapter describes how to use a text editor and the command line interface (CLI) to use filters. Transcend Remote Access Manager (TRAM) provides the same functionality using a graphical interface - for more information, see TRAM online Help.*

---

## Filtering Overview

Packet filters are used primarily in networks that cross organizational or corporate boundaries. They control inter-network data transmission by accepting or rejecting the passage of specific packets through network interfaces based on packet header information.

When data packets are received by a network interface such as a modem, a packet filter analyzes packet header data against its set of rules. Based on rules that you define, the filter permits the packet to pass through or discards it.

## Filtering Capabilities

The RAS 1500 supports the following filtering capabilities:

- Input/output filtering — Packet filters can be used to control inbound or outbound data packets.
- Source/destination address filtering — A packet filter can accept or deny access to a host or user based on the address of the source and/or destination.
- Protocol filtering — Inbound or outbound network traffic can be evaluated based on the protocol.
- Source/destination port filtering — A packet filter can control what services local or remote users can access.
- Call filtering can control whether a packet can initiate an outgoing call.
- Controls the content of IP Routing Information Protocol (RIP) packets sent or received on specific ports.
- Remote Authentication Dial-In User Service (RADIUS) and TACACS+ filtering. See Chapter 12, “Using Security and Accounting” for more information.

---

## Filter Types

Filters can be classified by the following types:

- Data filters — based on protocol-specific packet information
- Advertisement filters — based on broadcast packet information
- Generic filters — based on packet structure
- Call filters — based on outgoing calls

### Data Filters

Data filters control network access based on protocol, source/destination address, and source/destination port designation (for example, Transmission Control Protocol [TCP]/User Datagram Protocol [UDP] port designations) of the packet.

The RAS 1500 supports Internet Protocol (IP) and Internetwork Packet Exchange (IPX)-related filters. This filter type controls network access based on the protocol and source/destination address. IP filter rules allow filtering on source address, destination address, protocol type, source port, and destination port of the IP packet. IPX filter rules allow filtering on source network, destination network, protocol type, source socket, destination socket, source node, and destination node of the IPX packet.

### Advertisement Filters

Advertisement filters act on network protocol packets that contain information such as Routing Information Protocol (RIP). Filtering these packets is performed by the specific protocol process.

IP-RIP, IPX-RIP, and IPX-Service Advertising Protocol (SAP) are supported by the RAS 1500. The IP-RIP filter type controls the content of IP RIP packets that are sent out or received. The IP- and IPX-RIP filtering process filters addresses from the RIP packet upon transmission (output filter) and does not enter routes into the Routing Table upon receipt (input filter).

The IPX-SAP filter type controls the content of SAP packets that are transmitted or received. The IPX-SAP filter rules allow filtering on service type, server name, network address, node address, and the socket number fields of the service entry. The forwarding process uses the filter information to prevent service data from being included in the SAP packet.

**Call Filters** IP-Call filters are employed to screen outgoing calls for an ondemand user or a per interface basis. Filtering rules can comb source, destination, and host addresses, port numbers of TCP and UDP protocols, and Internet Control Message Protocol (ICMP) messages and protocols.

**Generic Filters** Generic filters are set by byte and offset values in a packet. Packets are filtered by comparing their offset value and byte information with the values you define in the filter. The RAS 1500 accepts or rejects the packet based on the result.



*Creating generic filters can be a complex task. Only experienced users should use generic filters and strictly in cases where data and advertising filters cannot provide necessary filtering capabilities.*

---

## Creating Filters

The RAS 1500 performs packet filtering based on rules you create. This section describes how to create packet filters.

### Filter File Components

Filter rules are defined within filter files. Filters are text files stored either in FLASH memory or on a RADIUS server. You can create and modify filter using the following:

- The Windows-based TRAM
- An off-line text editor

### File Descriptor

To be valid, a filter file must always have the following file descriptor on the first line:

```
#filter
```



*Eliminate blank space before the descriptor, otherwise an error will occur.*

The remainder of the filter file is partitioned into protocol sections. Each protocol section has a descriptive header preceding filter rules for that protocol.

## Protocol Sections

A single filter file can contain protocol sections in any order, but sections cannot be repeated. The following conditions cause errors or prevent filtering:

- If you do not specify a protocol section in the filter file, no filtering will occur and packets of that protocol type will be accepted.
- If you specify a protocol section but do not define rules, an error will occur.
- If you omit a line number or insert a line out of sequence, errors will occur.



*To comment out a protocol section, you must place a pound (#) sign before the section header and before all rules defined in that section.*

Table 57 describes valid protocol sections you can define in the filter file.

**Table 57** Valid Protocol Sections

Protocol	Description
IP:	IP protocol data filter section
IP-CALL:	IP protocol call filter section
IP-RIP:	IP RIP advertising filter section
IPX:	IPX protocol data filter section
IPX-CALL:	IPX protocol call filter section
IPX-RIP:	IPX RIP advertising filter section
IPX-SAP:	IPX SAP advertising filter section
LOGIN-ACCESS:	Login Access filter section
ATALK:	Appletalk protocol data filter section
ATALK-CALL:	Appletalk protocol call filter section
ATALK-RTMP:	Appletalk RTMP advertising filter section
ATALK-ZIP:	Appletalk ZIP advertising filter section

## Protocol Rules

You define protocol rules within each protocol section in the filter file. These rules set which packets may and may not access the network. The following is the rule syntax:

```
<line #> <verb> <keyword> <operator> <value>;
```

The combination of keyword, operator, and value forms a condition which, when combined with a verb, sets whether packets are accepted or rejected.

When a packet is filtered, an IP packet for example, the RAS 1500 parses each rule defined in the IP protocol section sequentially according to the line number. Filtering is performed based on the first occurring match. Without a match, the packet is accepted by default. For this reason, you should order your protocol rules so that rules you expect to be most frequently matched are situated early in the section to reduce parsing time during filtering.

Table 58 describes each field used in the rule syntax.

**Table 58** Protocol Rules

Field	Description
line #	Each rule must have a unique line number (1–999). You must arrange rules in increasing order.
verb	This field can be one of the following: <ul style="list-style-type: none"> <li>■ ACCEPT — allow packet access if condition is met</li> <li>■ REJECT — do not allow packet access if condition is met</li> <li>■ AND — logically use the AND condition with condition of the next rule to determine if packet is accepted or rejected: both defined conditions must be met. <i>IMPORTANT:</i> No more than 15 consecutive AND rules are permitted.</li> </ul>
keyword	For descriptions, see page 242
operator	Describes the relationship between the keyword and its value. The operator field must be one of the following (applies to the specific keyword used): <ul style="list-style-type: none"> <li>= Equal</li> <li>!= Not equal</li> <li>&gt; Greater than</li> <li>&lt; Less than</li> <li>&gt;= Greater or Equal</li> <li>&lt;= Less or Equal</li> <li>=&gt; Generic</li> </ul>
value	Contains an entity appropriate for the keyword.



*The OR operation can be implemented by successive ACCEPT rules. For example, to accept a packet if the source address is xxx, or the destination address is yyy, the following rules are used:*

```
IP:
010 ACCEPT src-addr = xxx;
020 ACCEPT dst-addr = yyy;
```



## Generic Filter Rules

Generic filter rules are similar in format to protocol filter rules. The following shows the rule syntax. The following is the rule syntax:

```
<line #> <verb> <keyword> <operator> origin = <DATA | FRAME>/
offset = <value>/length = <value>/mask = <hexadecimal value>/
value = <hexadecimal value>;
```

Table 59 describes each field used in the rule syntax.

**Table 59** Generic Filter Rules

Field	Description
line #	Each rule must have a unique line number (1–999). You must arrange rules in increasing order.
verb	This field can be one of the following: <ul style="list-style-type: none"> <li>■ ACCEPT — allow packet access if the condition is met</li> <li>■ REJECT — do not allow packet access if the condition is met</li> <li>■ AND — logically use the AND condition with condition of the next rule to determine if packet is accepted or rejected. Both defined conditions must be met. <i>IMPORTANT:</i> No more than 15 consecutive AND rules are permitted.</li> </ul>
keyword	The keywords for a generic filter rule is always <code>GENERIC</code> .
operator	The operator for a generic filter rule is always: <code>=&gt;</code>
origin	Can be either <code>FRAME</code> or <code>DATA</code>
offset	This is the number of bytes offset from the origin.
length	This is the number of bytes to compare and mask.
mask	This is the bit mask, in hexadecimal format, for logical and packet content. (00 or FF)
value	This value, in hexadecimal format, is used to compare with contents of masked packet

For example, a generic filter rule might look like the following:

```
010 ACCEPT generic => origin = data/offset = 22/length = 6/
mask = 0xFFFFFFFFFF/value = 0x0800096f39c8;
```

## Specifying the Filtering Action

You can specify the filtering action for each protocol section that determines whether a packet is accepted or rejected if no match occurs with any of the rules defined in the section. To do so, enter one of the following values as the *last* rule line of the section:

- ACCEPT
- DENY

For example, the following entry would reject IP packets that did not match any of the rules defined in the IP protocol section:

```
#filter
IP:
010 ACCEPT tcp-dst-port > = 24;
020 ACCEPT src-addr = 128.100.033.001;
030 ACCEPT dst-addr = 200.135.038.009;
040 DENY;
```



*If you do not specify a filtering action, the default filtering action is permit.*

## Creating Filter Files

To create a filter, use a text editor on your computer to create or edit a filter file. Use the Trivial File Transfer Protocol (TFTP) to load the file in the RAS 1500 FLASH memory. (If you TFTP an edited file to the RAS 1500, it replaces the original file.)

Be careful, the following steps require frequent switching between your computer and the RAS 1500. To create a filter file on your computer, perform the following:

- 1 Create a new text file. Enter a file descriptor on the first line.

```
#filter
```



*Eliminate blank space before the descriptor, otherwise an error will occur.*

- 2 Enter a file section header followed by a colon to begin a protocol section. For example, to define IP filtering rules, enter the following section header:

```
IP:
```



*If you want to comment a section header out, put a # (pound) sign before the header. It is useful to insert a placeholder for a protocol section you will define later.*

- 3 Enter the protocol rules for the protocol section you are defining. Be sure to perform the following:
  - Begin each rule with a unique line number (1-999).
  - Arrange rules in increasing order within each protocol section.
  - Arrange rules so that the rules you expect to be matched *most frequently* are at the top of the list.
  - Delimit each rule with a semi-colon (;).

Example:

```
#filter
IP:
010 ACCEPT src-addr = 128.100.033.001;
020 ACCEPT dst-addr = 200.135.038.009;
```

- 4 Add filtering action if different from the default value of `PERMIT`.

Example:

```
030 DENY;
```

- 5 Continue to define protocol rules for each protocol section you want to filter. Then, check the file to ensure it meets the RAS 1500 requirements and save the file.



*To set up RADIUS filter files, see Chapter 12 “Using Security and Accounting”.*

- 6 Access the CLI on the RAS 1500. Configure your computer as a TFTP client by entering the following command:

```
add TFTP client <hostname or IP address>
```

- 7 Return to your computer. From a machine that has access to the same network as the RAS 1500, use the following TFTP commands to transfer the filter file to the RAS 1500 FLASH memory.

```
tftp <RAS 1500 IP address>
put <filter_filename>
```

- 8 Return to the CLI on the RAS 1500. The RAS 1500 does not recognize a filter file stored in its FLASH memory until you add it to the Managed Filter Table. Use the following command:

```
add filter <name>
```

When the filter is added, the RAS 1500 automatically verifies filter file syntax. If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, an error message is generated detailing the error source.



*Type `list files` to ensure the filter file was successfully stored in FLASH memory.*

- 9 Use the `verify filter` command to ensure filter file syntax is correct. Enter the following:

```
verify filter <filter name>
```



*Any subsequent entry of same name filter files requires the original filter files to be deleted using `delete filters`. Reverify and reapply using `set interface`. Use `show filter <filter name>` to view your file. If you are applying a filter to a RADIUS user, use `show remote user`.*

---

## Configuring Filters

Once a filter has been added to the managed filters list, turn filter access on or off and assign the filter to the RAS 1500 interfaces or users.

### Setting Filter Access

When filters are assigned to an interface, the `filter access` parameter must remain off (`default` setting). But, if configuring a filter for a user, you must enable filter access. This parameter acts as a toggle switch for interface or user filtering and, when enabled, overrides the default `interface` setting.



*If your filters are inoperative, it more than likely is because you have not correctly set filter access.*

To enable filter access for a specific user, use the following command:

```
set interface <rm0/slotx/mod:[1-4]> filter_access on
```

To enable filter access for a specific interface, use the following command:

```
set interface <rm0/slotx/mod:[1-4]> filter_access off
```



*Filter file changes take effect on an interface immediately when you issue the set interface command. The set switched interface and set modem\_group commands can also be issued to turn filter access on or off.*

## Interface Filters

You can configure interface filters for any *interface* or *modem group*. Interface filters control access to all networks available for both modem and non-modem (eth:1 or eth:2) interfaces.

You can specify whether a filter applies to packets entering the interface (input filter), packets leaving the interface (output filter), and packets that can initiate a call out (call filter). The RAS 1500 examines the filtering rules to determine whether the interface accepts or rejects the packet. Interface filters can be applied dynamically without having to disable and re-enable each network on that interface.



*If you prefer to configure a filter through a modem group, first issue the add modem\_group <name> interfaces <rm0/slot[1-2]/mod:[1-4] or pem[1-2]/slot[1-2]/mod:[1-4]> command.*

Use either of the following commands:

```
set interface <rm0/slot[1-2]mod [1-4]> input_filter  
<filter_name> output_filter <filter_name>  
set modem_group <name> input_filter <filter_name>  
output_filter <filter_name>
```

### Input Filter

If an input filter is configured on an interface, all received packets are checked against the filtering rules before being forwarded to another interface. In other words, an input filter handles data *from* an interface.

### Output Filters

If an output filter is configured on an interface, all outbound packets are checked against the filtering rules before exiting the interface. In other words, an output filter handles data *to* an interface.

### Call Filters

If a call filter is configured on an interface, all transmitted packets are checked against the filtering rules. The filtering rules determine whether the packet can initiate an outgoing call. Call filters are checked only after the packet has passed the output filter check. An interface without a call filter configured will allow packets from all properly configured users to initiate an outgoing call.

This filter is used for an ondemand call only.

### Input Filters vs. Output Filters

When possible, use the input filter to filter an incoming packet rather than wait to catch a packet as it attempts to exit. This is recommended for the following reasons:

- A packet is prevented from entering, keeping potential intruders from attacking the RAS 1500.
- The routing engine does not waste time processing a packet that is going to be discarded anyway.
- Most importantly, the RAS 1500 does not know which interface an outgoing packet came in through. If a potential intruder forges a packet with a false source address (to appear as a trusted host or network), there is no way for an output filter to tell if that packet came in through the wrong interface. An input filter, however, can filter out packets purporting to be from networks that are actually connected to a different interface.

### User Filters

You can configure filters for a specific user to control network access for that user. This filter type is applied for the duration of the user network connection only. As with interface filters, a user filter can be configured as an input, output, or call filter. Remember, input filters handle data *from* a user, while output filters handle data *to* a user.



*User filters are dynamic only via RADIUS. Filter access must be turned ON before the user connects and attempts a RADIUS request for filters.*

## Assigning a Filter to an Interface

To configure input or output filters on a specified interface, use the following command. The default `filter_access` setting (`off`) need not be set unless you have previously enabled filtering for a user. Use the following command:

```
set interface <rm0/slot[1-2]mod:[1-4]>
    input_filter <filter_name>
    output_filter <filter_name>
    filter_access off
```

For example, if you have not enabled a user filter on the interface, enter the following:

```
set interface rm0/slot1/mod:3 input_filter infilter.fil
```

If you have enabled a user filter on the interface, you must reset access. Enter the following:

```
set interface rm0/slot1/mod:3 output_filter outfilter.fil
filter_access off
```

If you want to set slot:4/mod:8 input and output filters at the same time, enter the following:

```
set interface rm0/slot1/mod:3 input_filter infilter.fil
output_filter outfilter.fil
```



*IP networks and interfaces must be disabled then enabled for interface filters to be effective.*

## Assigning a Filter to a User

To configure an input or output filter for a specific user, use these commands.



*Filter access must be turned on (off by default) on the interface to be used when setting a user filter.*

```
set user <user_name>
    input_filter<filter_name>
    output_filter<filter_name>
set interface <rm0/slot[1-2]mod:[1-4]> filter_access on
```

Example:

```
set user nancy input_filter infilter.fil ENTER
set interface <rm0/slot1/mod:3> filter_access on ENTER
```



*Filters take effect for a user the next time that user makes a connection.*

## Managing Filters

This section provides the following information about how to manage filters:

- Displaying the managed filter list
- Adding filters to the managed filter list
- Deleting filters from the managed filter list
- Verifying filter file syntax
- Displaying the contents of a filter



*When managing filters, if you edit an existing filter and do not first remove it from **every** interface or user profile for which it is configured and then reapply the new filter, the previously unedited version will still apply. See *Removing a Filter...* sections on the next page.*

### Displaying the Managed Filter List

To display the list of managed filters, use the following command:

```
list filters
```

The resulting display might look like the following example:

```
FILTERS
Filter Name      Status           Protocols
xfilter.in       NORMAL           IP IP-RIP
xfilter.out       VERIFY FAILED    IPX
ljc_filter.fi    NORMAL           IP-CALL
1
```

### Adding Filters to the Managed List

The `add filter` command verifies filter syntax before adding a filter to the managed list. If syntax is valid, no message is generated and the command prompt returns. If syntax errors exist, messages are sent describing them.

If the syntax is invalid, the filter is still added to the managed list with a status of `verify failed`. To correct filter file errors, you must make the changes to the original filter file using a text editor and re-TFTP the file to FLASH memory. You must then use the `verify filter` command to check the filter file syntax. For more information about `verify filter`, see “*Verifying Filter File Syntax*” on page 232.



To add a filter file to the list of managed filters, use the following command:

```
add filter <filter_name>
```



*It is helpful to use `list files` to see files successfully stored in flash memory.*

### Removing a Filter from an Interface

Removing a filter assigned to an interface is mandatory when editing it. The "" value is a null value that removes a defined filter from the interface. Enter the following:

```
set interface <interface_name>
  input_filter ""
  output_filter ""
```

For example, to remove an output filter from the `eth:1` interface, enter the following:

```
set interface rm0/eth:1 output_filter "" ENTER
```

Now be sure to reapply the filter with the `set interface` command. Enter the following:

```
set interface rm0/eth:1 output_filter <filter_name>
```

### Removing a Filter from a User Profile

Removing a filter assigned to a user profile is mandatory when editing it. The "" value is a null value that removes the defined filter from the user profile. Enter the following:

```
set user <user_name>
  input_filter ""
  output_filter ""
```

For example, to remove an input filter from a user named "john\_d," enter the following:

```
set user john_d input_filter "" ENTER
```

Now be sure to reapply the filter with the `set user` command. Enter the following:

```
set user john_d input_filter <filter_name>
```



*This command does not dynamically remove a filter from a user profile.*

### Deleting a Packet Filter

To delete a specific packet filter, removing the filter file from the filter list and permanently from FLASH memory, use the following commands:

```
delete filter <filter_name>
delete file <file_name>
```

### Verifying Filter File Syntax

The `verify filter` command is useful if you make changes to a filter file that has already been added to the managed list and re-TFTP the file back into FLASH memory (using the same filename). This command checks the filter syntax, compiles it and if valid, generates no message and returns the command prompt. If invalid, error messages are generated detailing the error sources.



*Filter file changes are designed to take effect on an interface immediately after you issue the `set interface` command. So remember to remove and reapply the filter to ensure new filter rules apply to all affected interfaces.*

To verify a filter file, use the following command:

```
verify filter <filter_name>
```

### Showing Filter File Contents

To view the contents of an entire filter file that has been added to the managed list of filters, use the following command:

```
show filter <filter_name>
```

To display the contents of the filter file by protocol, use the following command:

```
show filter <name> protocol [ ip | ip-call | ip-rip | ipx |
ipx-call | ipx-rip | ipx-sap | login-access]
```

### Generating SYSLOG Messages for Filtered Packets

You can save filtered packets to a configured SYSLOG server, allowing you to track down a potentially malicious user. Due to the large amount of traffic this command could generate, its anticipated use would only be for a short time.

Use the following command:

```
set packet_logging
    logging [all | radius | none]
    packet_size [0-493 bytes]
```

A description of each parameter follows.

- `All` — Creates SYSLOG messages globally for all filtered packets.
- `Radius` — Checks the RADIUS profile (Filter-Log-Packet attribute in the Access-Accept packet) on a per-user basis.
- `None` — No SYSLOG messages generated.
- `0-493 bytes` — Use a number between 0 and 493 to specify how many bytes of the discarded packet to send to SYSLOG. Setting to 0 causes the entire packet to be included in the SYSLOG message.

---

## General Filter Setup

This section describes the steps to configure a filter on the RAS 1500.

- 1 Create a filter using the filter rules described in the *Creating Filters* section. You may use an off-line editor and TFTP the file to the RAS 1500. For the purposes of this example, the input filter is named `ras1500.fil`.
- 2 If you are configuring a user filter - not an interface filter - enable `filter_access` (`off` by default) with the following command. Filter access should remain off for an interface filter.

```
set interface [rm0|pem1|pem2]/slot[1-2]/mod:[1-4]
```

- 3 Add the filter to the RAS 1500 Managed Filter Table with the following command:

```
add filter ras1500.fil
```

- 4 The RAS 1500 automatically verifies that new filters are syntactically correct. For added insurance, issue the following command:

```
verify filter ras1500.fil
```

- 5 Issue the following command to ensure the filter was stored in the RAS 1500 FLASH memory:

```
list files
```

- 6 Assign the filter to a previously created user with the following command. If using RADIUS, specify the Framed-Filter-ID attribute.

```
set user <any_user_name> input_filter ras1500.fil ENTER
```

- 7 Verify that the filter was applied to the user with either of the following commands:

```
show user <user_name>  
show remote user <user_name>
```

---

## Filter Examples

This section provides specific filter examples.

### IP Packet Filter Rule Examples

This section briefly describes IP packet filtering options and provides rule examples for each IP packet filtering capability. It includes the following topics:

- Source and Destination Address Filtering
- Masks
- TCP and UDP Parameter Filtering
- IP/IPX-RIP Packet Filtering
- IPX-SAP Filtering
- ICMP Packet Filtering
- IP/IPX-Call Filtering
- Login-Access Filtering

#### Source and Destination Address Filtering

Source and destination address filtering is generally used to limit permitted access to trusted hosts and networks only, to explicitly deny access to hosts and networks that are not trusted, or to limit external access to a given host (for example, a Web server or a firewall).



*Only the part of the IP address specified by the mask field is used in the comparison. If a match is found, the packet is forwarded (rules containing accept) or discarded (rules containing reject).*

The following rule example rejects forwarding of IP packets with a source address of 192.77.100.32:

```
#filter
IP:
010 REJECT src-addr = 192.77.100.32;
```

The following rule example prevents forwarding of IP packets with destination addresses that match the first 24 bits of the given IP address (that is, addresses beginning with 188.039.150):

```
#filter
IP:
010 REJECT dst-addr = 188.039.150.000/24;
```

The following rule example allows forwarding of IP packets with source address 192.077.100.032 and destination address 201.128.011.034:

```
#filter
IP:
010 AND src-addr = 192.077.100.032;
020 ACCEPT dst-addr = 201.128.011.034;
```

The following rule example limits a user to one host with an input filter:

```
#filter
IP:010 ACCEPT dst-addr = 143.134.45.56;
020 DENY;
```

## Masks

These fields specify the number of bits to be used in the source address and destination address comparisons. The following are valid values:

- 0 — Match all packets with any IP address. The contents of `source address` or `destination address` fields are unimportant.
- 8 — Compare the first byte (octet) in the IP addresses.
- 16 — Compare only the first two bytes of the IP addresses.
- 24 — Compare only the first three bytes of the IP Addresses.
- 32 — Match the entire IP address (default).

The masks are separated from `source address` and `destination address` by forward slashes (/).

## TCP and UDP Parameter Filtering

TCP and UDP packets are typically sent from and destined for standard port numbers that provide common network services, such as Domain Name Service, SNMP, and Telnet. You can filter TCP and UDP packets by source and destination ports by defining filter rules that compare the port number in a TCP or UDP packet to a specific value.

The following rule example accepts only TCP packets that have a source port number of 24 or greater.

```
#filter
IP:
010 ACCEPT tcp-src-port >= 24;
020 DENY;
```

The following rule example accepts only TCP packets that have a destination port number that is in the range of 24 to 39:

```
#filter
IP:
010 AND tcp-dst-port > 23;
020 ACCEPT tcp-dst-port < 40;
030 DENY;
```

The following rule example accepts only UDP packets that have a destination port number that is in the range of 24 to 39:

```
#filter
IP:
010 AND udp-dst-port > 23;
020 ACCEPT udp-dst-port < 40;
030 DENY;
```

The following rule example rejects TCP and UDP packets:

```
#filter
IP:
010 REJECT protocol = tcp;
020 REJECT protocol = udp;
```

## Standard Port Numbers

Table 60 lists standard port numbers for common services. For a complete list, see the most recent “Assigned Numbers” RFC.

**Table 60** Standard Port Numbers

TCP	UDP	Description
20	-	File Transfer Protocol (data)
21	-	File Transfer Protocol (control)
23	-	Telnet
25	-	Simple Mail Transfer Protocol
43	43	Who Is
53	53	Domain Name Service
-	69	Trivial File Transfer Protocol
70	70	Gopher
79	79	Finger
80	-	World Wide Web HTTP
88	88	Kerberos
110	-	Post Office Protocol - Version 3
111	111	Sun Remote Procedure Call
113	113	Authentication Service
119	-	Network News Transfer Protocol
123	123	Network Time Protocol
161	161	Simple Network Management Protocol
162	162	Simple Network Management Protocol trap
220	220	Interactive Mail Access Protocol v3
512	-	remote process execution
513	-	remote login (rlogin)
-	513	remote who (rwhod)
514	-	remote command (rsh)
-	514	Syslog accounting
515	-	lpd spooler
517	517	talk (terminal to terminal chat)
518	518	ntalk (new terminal chat)
-	520	RIP
540	540	uucp (UNIX to UNIX copy)
540	540	uucp-rlogin
543	543	klogin (Kerberized login)
1642	-	PortMux daemon
-	1645	Remote Authentication Dial-In User Service security
-	1646	Remote Authentication Dial-In User Service accounting

## IP and IPX-RIP Packet Filtering

RIP packets identify all attached networks and the number of router hops required to reach them. These responses are used to update a router's routing table. Define IP/IPX-RIP filtering rules in the IP-RIP and IPX-RIP protocol sections of the filter.

For example, to filter all routes except the IP network address 195.120.254.145, enter the following:

```
#filter
IP-RIP:
010 ACCEPT network = 195.120.254.145;
020 DENY;
```

This filter allows route 195.120.254.145 into the table, rejecting all others.

For example, if you want to filter all but the following IPX networks, enter the following:

```
#filter
IPX-RIP:
010 REJECT network != 00-00-99-ff;
020 REJECT network != 99-88-0-45;
030 REJECT network != 0-8-7-5;
```

To filter an IP route based on a subnet mask (all but 195.223.0.0 networks), enter the following:

```
#filter
IP-RIP:
010 REJECT network = 195.223.87.225/16;
```



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

## IPX-SAP Filtering

IPX-SAP filtering rules are defined in the IPX-SAP protocol section of the filter file. The IPX-SAP filtering process compares advertised server name, service type, network number, node (host) address, and socket number values to values defined in the IPX-SAP filter rules.



For example, to allow a packet to pass if it is advertised from the server named sales\_1 and its socket number is less than 32, enter the following:

```
#filter
IPX-SAP:
010 ACCEPT server sales_1;
020 ACCEPT socket < 32
```

When applied to an input filter, the following example will permit SAP service type 04 and deny everything else from entering:

```
#filter
IPX-SAP:
010 ACCEPT service 04
```

### ICMP Packet Filtering

ICMP packets contain messages exchanged by IP modules in both hosts and gateways to report errors, problems, and operating information. ICMP message types are listed in Table 61. Note that most are error messages necessary for the correct operation of TCP/IP.

**Table 61** ICMP Message Types

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

If you are concerned about security, filter out incoming type 5 messages. Sending ICMP redirects is an easy way for a vandal to change your routing tables. Although ping is a troubleshooting aid, it allows a potential intruder to obtain a map of your network by systematically pinging every possible address. If you are worried, filter out incoming type 8 packets or outgoing echo replies (type 0).

For example, to prevent vandals from changing your routing tables by sending ICMP redirects, enter the following:

```
#filter
IP:
010 REJECT icmp-type = 5
```

### IP/IPX-Call Filtering

You define IP/IPX-call filtering rules in the IP-CALL, IPX-CALL protocol sections of the filter file. Like the rules defined in the IP protocol section, the IP-CALL filtering rules compare the advertised source or destination network address, host address and port number, and values defined in the IP-CALL filter rules. IPX-CALL filtering rules compare source/destination network addresses, hosts, and socket numbers.



*Call filtering occurs after output filters are processed and are used for ondemand calls only.*

For example, to allow outgoing calls from the user of IP address 192.112.42.6, enter the following:

```
#filter
IP-CALL:
010 ACCEPT src-addr = 192.112.42.6;
020 DENY;
```

For example, to allow outgoing calls to IPX host 77-88-99-aa-bb-cc, and reject calls from the source socket number 0x3f00, enter the following:

```
#filter
IPX-CALL:
010 ACCEPT dst-host = 77-88-99-aa-bb-cc;
020 REJECT src-socket = 0x3f00;
```

### Login-Access Filtering

Login-Access filters are used to restrict login user accessibility to hosts connected to the RAS 1500. Filtering rules are set in the LOGIN-ACCESS protocol section of the filter file, using a subnet mask to restrict access from approved networks.

For example, to filter the host where login users initially connect to, enter the following:

```
#filter
LOGIN-ACCESS:
010 ACCEPT dst-addr = 187.243.71.54/24
```

This filter allows users on network 187.243.71.0 to access the configured host but rejects all others.

## **RAS 1500 Global Filtering**

The RAS 1500 can filter packets globally traveling in and out of dial-up ports as well as the network port. The options below provide tighter network security.

### **Global Switch to Drop IP Fragments with Offset = 1**

This global switch lets you discard all IP packets with an offset value equal to 1. This packet type typically occurs when a system is under attack from a user trying to bypass installed filters on an interface by sneaking the packet by the filter in fragmented form.

The RAS 1500 never generates a packet with an offset of 1. Some routers used on the same network RAS 1500 may be configured to filter out specific traffic. In some cases, these routers may not apply the filter correctly. Should this happen, those packets will be discarded. In accordance with RFC 1858, this security feature syslogs every instance of a packet being discarded. The following commands are associated with this feature:

```
enable ip security_option drop_all_fragoffset1 (default)  
disable ip security_option drop_all_fragoffset1 ENTER
```

### **Global Switch to Drop Packets with a Partial TCP Header**

This global option allows the global configuration to discard all IP packets with a partial TCP header. This command is similar to and a subset of the `enable ip security drop_all_fragoffset1` command. The default setting is `enabled` meaning these packets will be discarded. When a packet is discarded the event is syslogged. The following commands are associated with this feature:

```
enable ip security_option drop_tcp_fragoffset1 (Default)  
disable ip security_option drop_tcp_fragoffset1 ENTER
```

### Global Switch to Filter Out All IP Options

Sometimes IP options may be generated from an outside source in an attempt to get past routing tables in a network. The RAS 1500 provides a global feature to filter out all IP packets with IP options. By using the command below, you can discard all packets like this, which will create a SYSLOG message each time one of these packets is discarded. The following commands are associated with this feature:

```
enable ip security_option allow_all_header_options ENTER
disable ip security_option allow_all_header_options (Default)
```

### Global Switch to Filter Out IP Source Route Options

This global option addresses the particular path a sender chooses to take through the network to reach its destination, as specified in the sender packet IP header. Using this command, you can discard packets of this type although this is a lower level of security than All Header Options. The following commands are associated with this feature:

```
enable ip security_option disallow_source_route_options ENTER
disable ip security_option disallow_source_route_options
(Default)
```

---

## Keywords

This section describes valid keywords you can use for each protocol section.

### IP and IP-CALL Sections

Keyword	Description	Operators	Value
src-addr	source IP address	= or !=	ddd.ddd.ddd.ddd/mask
dst-addr	destination IP address	= or !=	ddd.ddd.ddd.ddd/mask
tcp-src-port	TCP source port #	all	1-65536
tcp-dst-port	TCP destination port #	all	1-65536
tcp-one-way	Not supported in this release		
udp-src-port	UDP source port #	all	1-65536
udp-dst-port	UDP destination port #	all	1-65536
icmp-type	ICMP message type	= or !=	0-255
protocol	protocol-specific field	= or !=	udp, tcp, icmp
generic	field offset, length, mask values	generic	generic

**IP-RIP Section**

Keyword	Description	Operators	Value
network	IP network address	= or !=	ddd.ddd.ddd.ddd/mask

**IPX and IPX-CALL Section**

Keyword	Description	Operators	Value
src-net	source network address	= or !=	xx.xx.xx.xx
dst-net	destination network address	= or !=	xx.xx.xx.xx
src-host	source host address	= or !=	xx.xx.xx.xx.xx
dst-host	destination host address	= or !=	xx.xx.xx.xx.xx
src-socket	source socket number	all	1-ffff in form 0Xxxxx
dst-socket	destination socket number	all	1-ffff in form 0Xxxxx

**IPX-SAP Section**

Keyword	Description	Operators	Value
network	network address	= or !=	xx.xx.xx.xx
node	node address	= or !=	xx.xx.xx.xx.xx
server	server name	= or !=	character string (max 32)
service-type	service type	= or !=	0-ffff in form 0Xxxxx
socket	socket number	all	1-ffff in form 0Xxxxx

**Login-Access Section**

Keyword	Description	Operators	Value
dst-addr	destination host address	= or !=	ddd.ddd.ddd.ddd

**AppleTalk Section**

Keyword	Description	Operators	Value
src-host	source host address	= or !=	0-65536
dst-host	destination host address	= or !=	0-65536
src-node	source node address	= or !=	0-255
dst-node	destination node address	= or !=	0-255
src-socket	source socket number	all	1-fe in form 0Xxx
dst-socket	destination socket number	all	1-fe in form 0Xxx
generic	field based on offset, length, mask, value	generic	generic

***AppleTalk Call Section***

<b>Keyword</b>	<b>Description</b>	<b>Operators</b>	<b>Value</b>
src-host	source host address	= or !=	0-65536
dst-host	destination host address	= or !=	0-65536
src-node	source node address	= or !=	0-255
dst-node	destination node address	= or !=	0-255
src-socket	source socket number	all	1-254
dst-socket	destination socket number	all	1-254
generic	field based on offset, length, mask, value	generic	generic

***AppleTalk RTMP Section***

<b>Keyword</b>	<b>Description</b>	<b>Operators</b>	<b>Value</b>
network	network address	= or !=	0-65536

***AppleTalk Zip Section***

<b>Keyword</b>	<b>Description</b>	<b>Operators</b>	<b>Value</b>
zone-name	AppleTalk zone name	= or !=	character string (max 48, spaces included)

# 15

## CONFIGURING DYNAMIC HOST CONFIGURATION PROTOCOL

This chapter contains the following information:

- Overview
- Configuring the RAS 1500 for Dynamic Host Configuration Protocol
- User Datagram Protocol Broadcast Forwarding

---

### Overview

Dynamic Host Configuration Protocol (DHCP) allows a server to provide Internet Protocol (IP) information (including IP address, subnet mask, default gateway, Windows Internet Naming Service (WINS) server addresses, and lease duration) to a local area network (LAN) user or a remote dial-in user, when the user requests it.

DHCP provides IP information on an as-needed basis. A user receives IP information when it is required and “returns” the IP information when finished with it. This is useful when IP addresses are limited or used temporarily.

DHCP allows centralized management and configuration of IP information. You avoid manually configuring each computer on the network (and at remote sites).

The SuperStack Remote Access System (RAS) 1500 can serve in one of two roles in the implementation of DHCP. As a “DHCP server” it provides information directly to local LAN users and dial-in users. As a “DHCP proxy server” it relays information from a DHCP server to local LAN users and dial-in users.

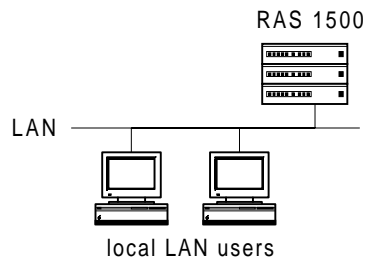
Five DHCP scenarios are shown below. The RAS 1500 acts as a DHCP server in scenarios 1 and 2. It acts as a DHCP proxy server in scenarios 3, 4, and 5.

**Acting as a DHCP server**, the RAS 1500 receives and processes the requests for IP information and provides the IP information directly back to the client.

**Acting as a DHCP proxy**, the RAS 1500 initiates a DHCP request to a DHCP server in behalf of the DHCP dial-in clients. The DHCP server receives and processes the request and sends the IP information back to the dial-in server via the RAS 1500.

**Acting as a DHCP relay**, the RAS 1500 passes on a request for IP information from a local user to a DHCP server.

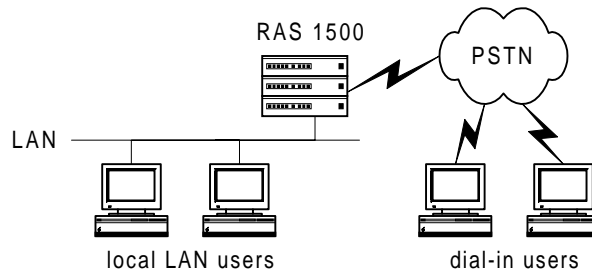
**Scenario 1** In this scenario, when a local user requests IP information, the RAS 1500, acting as a DHCP server, provides it.



**Figure 14** RAS 1500 as a DHCP server (local users)



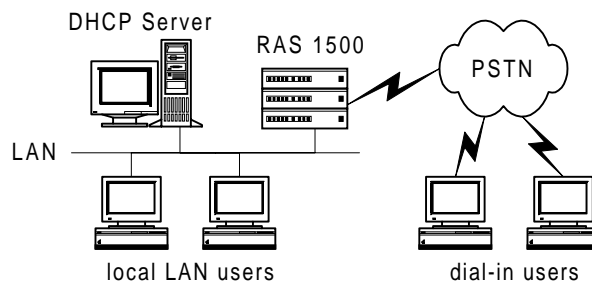
**Scenario 2** In this scenario, when a local user or dial-in user requests IP information, the RAS 1500, acting as a DHCP server, provides it.



**Figure 15** RAS 1500 as a DHCP server (local and dial-in users)

**Scenario 3** The following describes this scenario:

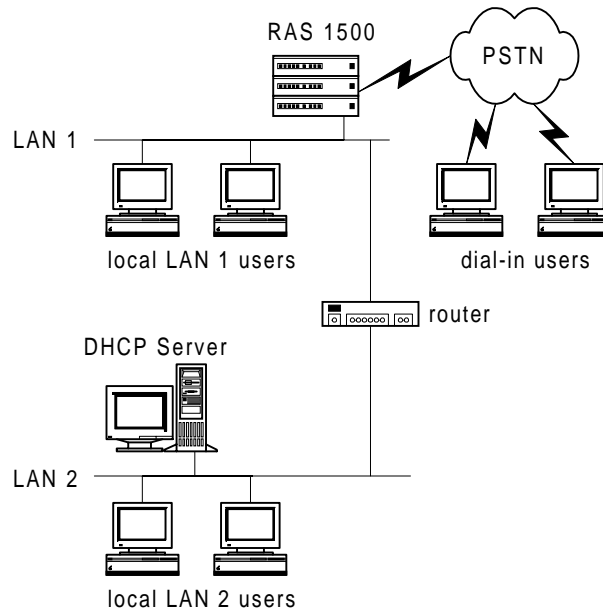
- When a local LAN user requests IP information, the DHCP server (not the RAS 1500) sends it to the user.
- When a dial-in user requests IP information, the RAS 1500, acting as a proxy server, relays the request to the DHCP server. The DHCP server processes the request and sends the IP information to the RAS 1500, which relays it to the dial-in user.



**Figure 16** RAS 1500 as a proxy server (DHCP server on the same LAN)

**Scenario 4** The following describes this scenario:

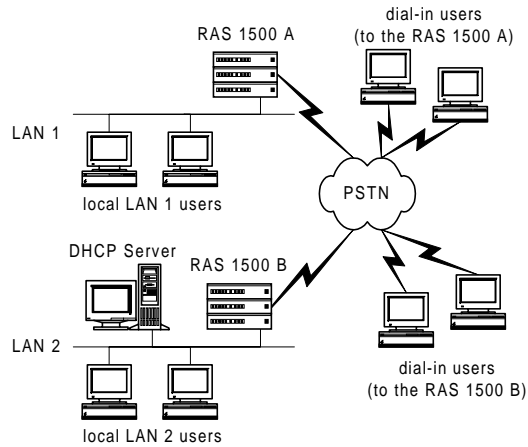
- When a local LAN 1 user requests IP information, the RAS 1500, acting as a proxy server, relays the request to the router. The router relays the request to the DHCP server on LAN 2. The DHCP server processes the request, then sends the IP information to the router. The router relays the information to the RAS 1500. The RAS 1500 relays the information to the local LAN 1 user.
- When a local LAN 2 user requests IP information, the DHCP server sends it to the user.
- When a dial-in user to the RAS 1500 requests IP information, the RAS 1500, acting as a proxy server, relays the request to the router. The router relays the request to the DHCP server on LAN 2. The DHCP server processes the request and sends the IP information to the router. The router relays the information to the RAS 1500. The RAS 1500 relays the information to the dial-in user.



**Figure 17** RAS 1500 as a proxy server (DHCP server on a different LAN)

**Scenario 5** The following describes this scenario:

- When a local LAN 1 user requests IP information, the RAS 1500 A, acting as a proxy server, relays the request through the PSTN to the RAS 1500 B. The RAS 1500 B relays the request to the DHCP server on LAN 2. The DHCP server processes the request, then sends the IP information to the RAS 1500 B. The RAS 1500 B relays the information to the RAS 1500 A. The RAS 1500 A relays the information to the local LAN 1 user.
- When a local LAN 2 user requests IP information, the DHCP server sends it to the user.
- When a dial-in user to the RAS 1500 A requests IP information, the RAS 1500 A, acting as a proxy server, relays the request through the PSTN to the RAS 1500 B. The RAS 1500 B relays the request to the DHCP server on LAN 2. The DHCP server processes the request, then sends the IP information to the RAS 1500 B. The RAS 1500 B relays the information to the RAS 1500 A. The RAS 1500 A relays the information to the dial-in user.
- When a dial-in user to the RAS 1500 B requests IP information, the RAS 1500 B, acting as a proxy server, relays the request to the DHCP server on LAN 2. The DHCP server processes the request and sends the IP information to the RAS 1500 B. The RAS 1500 B then relays the information to the dial-in user.



**Figure 18** Two RAS 1500s as proxy servers; each on a separate LAN

## Configuring the RAS 1500 for Dynamic Host Configuration Protocol

**DHCP Server** Use the following steps to configure RAS 1500 to act as a DHCP server:

- 1 Set the IP address assignment mode.
 

```
set ip address_assign_mode dhcp_proxy
```
- 2 Set the DHCP mode.
 

```
set dhcp mode server
```
- 3 Set parameters for DHCP users. These are the settings the DHCP server sends to users.
  - a Set the subnet mask and start and end addresses of the DHCP pool.
 

```
set dhcp server mask [subnet mask] start_address [ip address] end_address [ip address]
```



*Do not overlap the ip addresses of the DHCP pool and IP address pool.*

- b Set the lease duration.

```
set dhcp server lease [lease duration]
```

**c** Set the primary and secondary DNS servers.

```
set dhcp server dns1 [ip address] dns2 [ip address]
```

**d** Set the primary and secondary WINS servers and default gateway.

```
set dhcp server wins1 [ip address] wins2 [ip address] router  
[ip address of the default gateway]
```

**e** Set the DHCP server host name and domain name.

```
set dhcp server hostname [name of your RAS 1500] domain  
[domain name]
```

Example:

```
set dhcp server hostname testpc domain testnet.com
```

**f** Save your changes.

```
save all
```

**DHCP Proxy Server** Use the following steps to configure RAS 1500 to act as a DHCP server:

**1** Set the IP address assignment mode.

```
set ip address_assign_mode dhcp_proxy
```

**2** Set the DHCP mode.

```
set dhcp mode [disabled or relay]
```

**3** Specify the IP addresses of the primary and alternate DHCP servers.

```
set dhcp proxy server1 address [IP address of the primary  
DHCP server] server2 address [IP address of the secondary  
DHCP server]
```

---

## User Datagram Protocol Broadcast Forwarding

When a server on your network broadcasts User Datagram Protocol (UDP) packets, routers do not forward them, as described in RFC 1812, *Requirements for IP Version 4 Routers*. However, dial-in users may run applications that require UDP broadcasting.

Although RFC 1812 prevents routers from forwarding UDP packets, RAS 1500 has a solution that allows users to receive UDP packets.



**WARNING:** Do not use UDP broadcast forwarding on networks that contain loops. A loop happens when more than one link exists between two routers.

## Configuring UDP Broadcast Forwarding

To allow or disallow the RAS 1500 to forward UDP packets, use the following command:

```
[enable | disable] ip udp_broadcast_forwarding
```

For example, to enable UDP broadcast forwarding, use the following command:

```
enable ip udp_broadcast_forwarding
```



*By default, UDP broadcast forwarding is disabled.*

To add or delete a UDP broadcast forwarding port, use the following command:

```
[add | delete] ip udp_bcast_forwarding_port <port number>
```

For example, to add port 40001, use the following command:

```
add ip udp_bcast_forwarding_port 40001
```

## Displaying UDP Broadcast Forwarding Parameters

To display the status of UDP broadcast forwarding, use the following command:

```
show ip udp_broadcast_forwarding
```

To list the UDP broadcast forwarding ports, use the following command:

```
list ip udp_bcast_forwarding_port
```

# 16

## USING NETWORK ADDRESS TRANSLATION AND PORT ADDRESS TRANSLATION

This chapter contains the following information:

- Overview
- Configuring NAT and PAT
- Case Studies

---

### Overview

Network Address Translation (NAT) and Port Address Translation (PAT) act as address translators between public and private networks. They allow users on a privately addressed network to access the public network.

Use NAT if your Internet Service Provider (ISP) assigns you a public subnetwork. Use PAT if your ISP assigns you one IP address.

### Network Address Translation

NAT translates IP addresses.

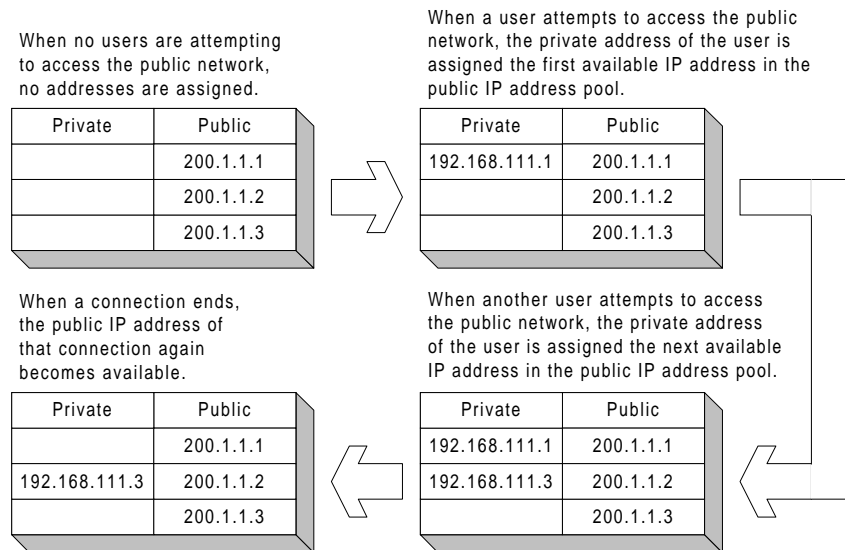
For example, assume your ISP assigns you a public subnetwork 200.1.1.0/28 from which you set aside a pool of public addresses from 200.1.1.1 to 200.1.1.10. When a user on 192.168.111.1 to 200.1.1.15 and a user on your private network (with an IP address of 192.168.111.1/C on the private network attempts to access a public host. The following happens:

- The SuperStack II Remote Access System (RAS) 1500, when it receives the “outbound” packet, uses NAT to translate the private address, 192.168.111.1, to the first free IP address in the public pool, 200.1.1.1. The RAS 1500 maintains a dynamic NAT mapping for this translation.
- Then, when an “inbound” packet addressed to 200.1.1.1 arrives at the RAS 1500 from the public network, the RAS 1500 uses the dynamic NAT mapping to reverse the translation (from 200.1.1.1 to

192.168.111.1), and the packet is routed to the correct user on the private network.

- The next user is assigned the next free IP address from the pool. For example, 200.1.1.2. When the connection for a user ends, the IP address is returned to the public address pool.

NAT is either “dynamic” or “static.” The preceding example is dynamic and is depicted in the following diagram. (Figure 19 shows fewer addresses in the pool than in the preceding example.)



**Figure 19** Dynamic NAT



Figure 20 depicts static NAT.

When a user attempts to access the public network, the private address of the user is assigned the public IP address defined in the table.

Private	Public
192.168.111.1	200.1.1.1
192.168.111.2	200.1.1.2
192.168.111.3	200.1.1.3
192.168.111.4	200.1.1.4

**Figure 20** Static NAT

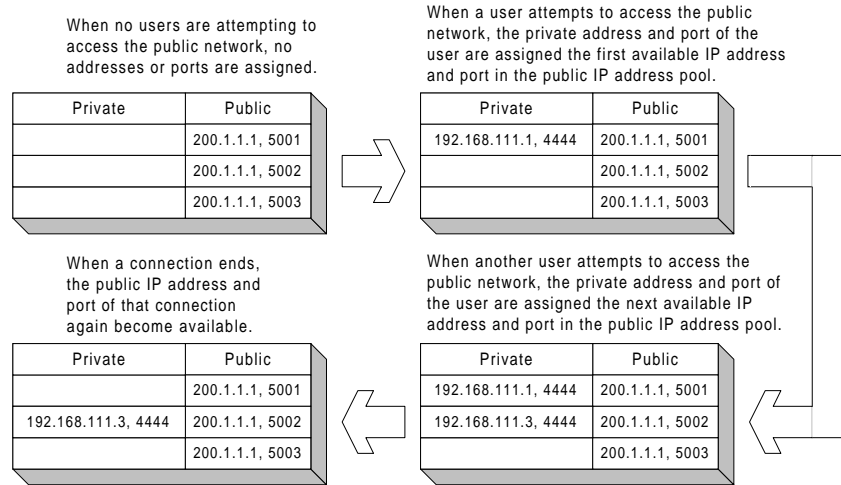
### Port Address Translation

PAT translates Internet Protocol (IP) addresses and User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) source port numbers.

For example, assume your ISP assigns you a public IP address of 200.1.1.1 and a user on your private network (with an IP address of 192.168.111.1, for example) attempts to access the public network. The following happens:

- The RAS 1500, when it receives the “outbound” packet, uses PAT to translate the private source address and source port number. For example, 192.168.111.1, port 4444 is translated to the ISP-assigned public IP address, 200.1.1.1, port 5001. The RAS 1500 maintains a dynamic PAT mapping for this translation.
- Then, when an “inbound” packet addressed to 200.1.1.1, port 5001 arrives at the RAS 1500 from the public network, the RAS 1500 uses the dynamic PAT mapping to reverse the translation (from 200.1.1.1, port 5001 to 192.168.111.1, port 4444), and the packet is routed to the correct user on the private network.
- The next user is assigned the same public IP address and the next free port number. For example, 200.1.1.1, port 5002. When the connection for a user ends, the port number becomes available for other users.

PAT is either “dynamic” or “static.” The preceding example is dynamic and is depicted in the following diagram. (Figure 21 shows fewer addresses in the pool than in the preceding example.)



**Figure 21** Dynamic PAT

Figure 22 depicts static PAT.

When a user attempts to access the public network, the private address and port of the user are assigned the public IP address and port defined in the table.

Private	Public
192.168.111.1, 4444	200.1.1.1, 5001
192.168.111.2, 4444	200.1.1.1, 5002
192.168.111.3, 4444	200.1.1.1, 5003
192.168.111.4, 4444	200.1.1.1, 5004

**Figure 22** Static PAT

---

## Configuring NAT and PAT

### Configuring Network Address Translation

#### Enabling and Disabling Users

To enable NAT for a user, use the following command:

```
set network user <username> nat_option nat
```

Example:

```
set network user nat_user nat_option nat
```

To disable NAT for a user, use the following command:

```
set network user <username> nat_option disable
```

Example:

```
set network user nat_user nat_option disable
```

#### Adding Dynamic and Static Address Assignments

To add a dynamic public address pool:

```
add nat dynamic user <>  
public_pool_start <ip address> count <number of addresses>
```

Example:

```
add nat dynamic user nat_user public_pool_start 200.1.1.1  
count 10
```

To add a static address assignment, use the following command:

```
add nat static user <username> public_address <ip address>
private_address <ip address>
```

Example:

```
add nat static user nat_user public_address 200.1.1.11
private_address 198.168.111.1
```

### View NAT Settings and Mappings

To show user settings, which includes its NAT settings:

```
show user <username>
```

Example:

```
show user nat_user
```

To list active NAT address mappings, use the following command:

```
list nat user <username> address
```

To list active NAT port mappings, use the following command:

```
list nat user <username> port
```

## Configuring Port Address Translation

### Enabling and Disabling Users

To enable PAT for a user, use the following command:

```
set network user <username> nat_option pat
```

Example:

```
set network user pat_user nat_option pat
```

To disable PAT for a user, use the following command:

```
set network user <username> nat_option disable
```

Example:

```
set network user pat_user nat_option disable
```



## Adding Dynamic and Static Address Assignments

*Unless you receive incoming connections from the public network, dynamic PAT does not need configuration beyond enabling a user and choosing PAT option.*

To add a static address assignment, use one of the following commands:

```
add pat tcp user <username> private_address <ip address>  
private_port <number> public_port <number>
```

or

```
add pat udp user <username> private_address <ip address>  
private_port <number> public_port <number>
```

Example:

```
add pat tcp user pat_user private_address 192.168.111.1  
private_port 80 public_port 80
```

Incoming packets from the public network whose destination port mappings do not exist in the dynamic PAT translation table are directed to a default host. To specify the default host, use the following command:

```
set network user <username> pat_default_address <IP address>
```

Example:

```
set network user pat_user pat_default_address 192.168.111.2
```

## Viewing PAT Settings and Mappings

To show user settings, which includes its PAT settings, use the following command:

```
show user <username>
```

For example,

```
show user pat_user
```

To list active PAT address mappings, use the following command:

```
list pat user <username> address
```

To list active PAT port mappings, use the following command:

```
list pat user <username> port
```

---

## Case Studies

This section contains one case study for NAT and one for PAT.

### NAT Case Study

A private network with a RAS 1500 requires access to a public network.

This access is across a PPP link with “ascend” compression initiated by the RAS1 500.

The user ID (“main”) and password (“ras”) have been agreed to by the ISP. In the NAT user profile, the transmit\_authentication setting must match the user ID (“main”), and the send\_password setting must match the password (“ras”).

The public subnet allocated by the ISP for use by this private network is 202.55.55.40/29.

The RAS 1500 is assigned the address 202.55.55.41/29.

The private network has two servers that will be accessed by hosts from the public network. The ISP access number is 3067.

The local area network (LAN) configuration of the RAS 1500 is the same as it would be without a NAT user added.

A NAT user is a normal user with some configuration differences. The differences are the following:

- IP address assignment for the wide area network (WAN) link
- Routing behavior over the WAN link
- Addition of static NAT mappings
- Addition of a public IP pool for dynamic NAT mappings

Private networks should not be advertised to the public network, hence the ip\_routing parameter is set to “listen.”

Static NAT is performed for 2 hosts on the private network. A dynamic public IP address translation pool is defined for other machines on the private network to be able to access the public network.

1 Set basic system settings.

```
set system name RASCNTRL
set command prompt RASCNTRL
set system transmit_authentication_name RASCNTRL
```

2 Set IP network settings.

```
add ip network ip address 192.168.111.254/C enable no
set ip network ip routing_protocol ripv2
enable ip network ip
```

3 Set authentication.

```
set ppp receive_authentication either
```

4 Add a modem group named 78.

```
add modem_group 78 interface rm0/slot:2/mod:[3-4]
```

5 Add and configure a user named "nat\_user."

```
add user nat_user password ras type network,dial_out
enable no
set user nat_user modem_group 78 phone_number 3067
set network user nat_user ppp compression_algorithm ascend
set network user nat_user transmit_authentication main
send_password ras
set network user nat_user ipx disable appletalk disable
bridging disable

set network user nat_user nat_option nat
set network user nat_user ip_routing listen rip ripv2
set network user nat_user default_route_option enable

set network user nat_user address_selection negotiate
set dial_out user nat_user local_ip_address 255.255.255.255

set user nat_user idle_timeout 120
set dial_out user nat_user site type ondemand
```

6 Configure NAT mappings.

```
add nat dynamic user nat_user
    public_pool_start 202.55.55.42/29 count 3
add nat static user nat_user private_address 192.168.111.106
    public_address 202.55.55.45
add nat static user nat_user private_address 192.168.111.140
    public_address 202.55.55.46
```

7 Enable the user.

```
enable user nat_user
```

8 Save your work.

```
save all
```

### PAT Case Study

The following case study configures PAT on the RAS 1500, with 2 channel multilink PPP connected to the ISP with dial-on-demand and bandwidth-on-demand. The 2 channels may be either ISDN or analog interfaces and assume that you have already configured the ISDN modems for proper operation. However, adding more than 4 Multi-Link Point-to-Point Protocol (MLPPP) links diminishes the gain of adding the channels because of the MLPPP overhead.

1 Specify the local Ethernet IP address.

```
add ip network ip address 192.168.1.1/C
```

2 Enter the local IP address pool for dial-in users.

```
add ip pool ippool initial_pool_address 192.168.1.10 size 24
```

3 Specify initial settings for the user named "pat\_user."

```
add modem_group PATMODEM interfaces
    rm0/slot:1/mod:1,rm0/slot:1/mod:2
add user pat_user password pat type network,dial_out
    enabled no
set user pat_user phone 15085551212
set user pat_user alternate_phone_number 15088711313
set user pat_user modem_group PATMODEM
set user pat_user idle_timeout 60
set network user pat_user network_service ppp
set network user pat_user ipx disable appletalk disable
    bridging disable
```



- 4 Set the username and password for your ISP account.

```
set network user pat_user transmit_authentication betty
set network user pat_user send_password fred
```

- 5 Specify additional user settings.

```
set network user pat_user ppp compression none
set network user pat_user address_selection negotiate
set network user pat_user default_route_option enable
set network user pat_user ip_routing listen
set network user pat_user nat_option pat
set network user pat_user pat_default_address 192.168.1.2
set dial user pat_user data async
set dial user pat_user local_ip_address 255.255.255.255
set dial user pat_user site type ondemand
```

- 6 Specify the default gateway.

```
add framed_route user pat_user ip_route 0.0.0.0 gateway
    255.255.255.255
set dial user pat_user site type ondemand
```

- 7 Set multilink PPP settings with bandwidth-on-demand.

```
set net user pat_user ppp max_channels 2
set net user pat_user ppp channel_expansion 70
channel_decrement 20
enable user pat_user
```

- 8 Save your work.

```
save all
```



# 17

## PPP OVER SERIAL WAN PORT

This chapter contains the following information about configuring the SuperStack II Remote Access System (RAS) 1500 to support Point-to-Point Protocol (PPP) over the serial wide area network (WAN) port.

- Overview
- Case Study
- Troubleshooting
- Properly configured network protocols

---

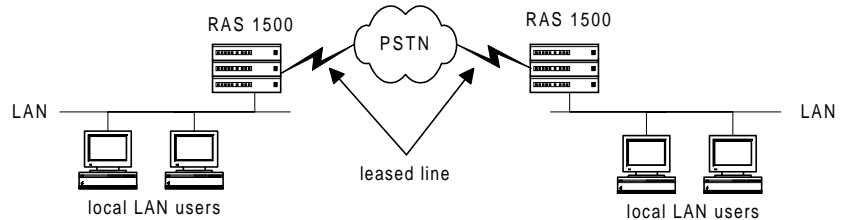
### Overview

The RAS 1500 supports a PPP connection over a leased line on its serial port. A leased line is a dedicated line between two sites and is permanently installed rather than a dialed up connection. PPP over the WAN port can connect to another RAS 1500 or any device that supports PPP.

PPP over leased line offers the following benefits:

- Constant connection. Once the connection between the sites is established, the link does not come down unless you issue a command to do so.
- Simple configuration. To prepare a RAS 1500 for leased-line PPP requires little configuration.
- Fast. The RAS 1500 supports speeds of 2.048 Mbps.

Figure 23 shows a typical PPP over leased line setup.



**Figure 23** Typical PPP over leased line setup

The RAS 1500 supports the following protocols through the WAN port. There are no settings on the RAS 1500, a different cable is used for each protocol.

- V.35
- RS-232E (V.28)
- RS-422 (V.11, X.21)
- RS-449 (V.11, V.10)
- EIA-530 (V.11, V.10)
- EIA-530A (V.11, V.10)

---

## Case Study

### Before You Begin

Before you configure the RAS 1500 for PPP over leased line, do the following:

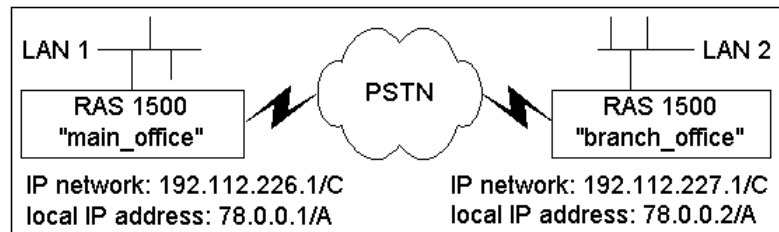
- 1 Work with the phone company to acquire a leased line between the two sites.
- 2 The leased line attaches to the Channel Service Unit/Data Service Unit (CSU/DSU) at both customer sites.
- 3 The leased line is responsible for providing a clock, either through the Central Office or through the CSU/DSU.

## PPP Over Serial WAN Port Case Study

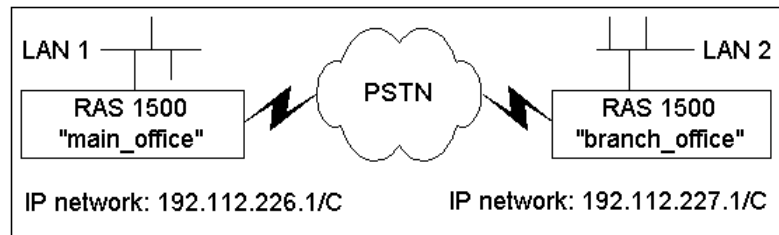
- Goals**
- Connect the "main\_office" RAS 1500, to the "branch\_office" RAS 1500 using a leased line connection PPP link.
  - Authenticate using PAP.
  - Idle timeout should be 300 seconds.

- Assumptions**
- Each office has a functioning RAS 1500.
  - Each office has a separate IP network. The main office has 192.112.226.0/C; the branch office has 192.112.227.0/C.
  - Use Routing Information Protocol (RIPv1).

**Process** The goals can be achieved with either a numbered IP link or an unnumbered link between the sites. Figure 24 shows a numbered link, and Figure 25 shows an unnumbered link.



**Figure 24** Numbered PPP over Serial WAN Port Link



**Figure 25** Unnumbered PPP over Serial WAN Port Link

To configure the RAS 1500 in the Main Office, perform the following:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network ipnet-1 address 192.112.226.1/C interface
rm0/eth:1
```

- 2 Add a user.

```
add user branch_office password chicago type network,dial_out
set user branch_office idle_timeout 300
```

- 3 Configure the user network parameters.

**a** Numbered link

```
set network user branch_office address_selection specified
remote_ip_address 78.0.0.2/A
set network user branch_office ipx disable appletalk disable
bridging disable
set network user branch_office send_password boston
```

**b** Unnumbered link

```
set network user branch_office address_selection specified
remote_ip_address 192.112.227.1/C
set network user branch_office ipx disable appletalk disable
bridging disable
set network user branch_office send_password boston
```

- 4 Configure the user dial-out parameters.

```
set dial_out user branch_office local_ip_address 78.0.0.1/A
set dial_out user branch_office site type ondemand
```

- 5 Configure the user routing parameters.

```
set network user branch_office ip_routing both rip ripv1
```

- 6 Add the PPP datalink.

```
add datalink ppp user <username> interface rm0/wan:1
```

Example:

```
add datalink ppp user test interface rm0/wan:1
```

- 7 Configure authentication.

```
set ppp receive_authentication pap
set system transmit_authentication_name main_office
```

- 8 Save your work.

```
save all
```

To configure the RAS 1500 in the Branch Office, perform the following:



*If an IP network has been defined, configured, and enabled on the RAS 1500, steps 1 through 3 are not necessary.*

- 1 Add an IP network.

```
add ip network ipnet-2 address 192.112.227.1/C interface
rm0/eth:1
```

- 2 Add a user.

```
add user main_office password boston type network,dial_out
set user main_office idle_timeout 300
```

- 3 Configure the user network parameters.

```
set network user main _office address_selection specified
remote_ip_address 78.0.0.1/A
set network user main _office ipx disable appletalk disable
bridging disable
set network user main _office send_password chicago
```

- 4 Configure the user dial-out parameters.

```
set dial_out user main _office local_ip_address 78.0.0.2/A
set dial_out user main _office site type ondemand
```

- 5 Configure the user routing parameters.

```
set network user main _office ip_routing both rip ripv1
```

**6** Configure authentication.

```
set ppp receive_authentication pap
set system transmit_authentication_name branch_office
```

**7** Save your work.

```
save all
```

**Disabling Leased-line  
PPP on the RAS 1500**

To bring down the connection, issue the following command:

```
disable datalink ppp interface rm0/wan:1
```

**Viewing the Status of  
the Connection**

To view the status of the link, use the `list ppp` command.

---

**Troubleshooting**

For debugging purposes, view the LCP negotiation, which is part of the PPP negotiation. These negotiations are only visible if the loglevel is set to "verbose" or "debug." You should also check the following:

- Cable type
- Users enabled
- Properly configured network protocols





# GMT TIME ZONES

Table 62 provides Greenwich mean time (GMT) offset information for locations around the world.

**Table 62** Greenwich Mean Time Offset

GMT Offset (Hours)	GMT Offset in Local Summer (Hours)	DST Change (Local Summer)	Region
-12		0	Kwajalein
-11		0	American Samoa Canton Enderbury Islands Midway Island Niue Island Samoa
-10		0	Christmas Islands Cook Islands French Polynesia Johnston Island Society Island Tahiti Tuamotu Island Tubuai Island USA Aleutian USA Hawaii
-9.5		0	Marquesas Islands
-9		0	Gambier Island
-9	-8	1	USA Alaska
-8	-7	1	Canada Yukon and Pacific Mexico Baja Calif Norte USA Pacific
-7		0	Mexico Nayarit Mexico Sinaloa Mexico Sonora USA Arizona

-7	-6	1	Canada Mountain USA Mountain
-6		0	Belize Costa Rica El Salvador Guatemala Honduras Mexico
-6	-5	1	Canada Central Easter Island Nicaragua USA Central
-5		0	Cayman Islands Colombia Ecuador Galapagos Islands Jamaica Panama Peru USA Indiana East
-5	-4	1	Bahamas Canada Eastern Cuba Haiti Turks and Caicos Islands USA Eastern
-4	-5	-1	Brazil Acre

-4		0	Anguilla Antigua Argentina western prov Aruba Barbados Bolivia Bonaire British Virgin Islands Curacao Dominica Dominican Republic Grenada Grenadines Guadeloupe Leeward Islands Martinique Netherlands Antilles Nevis Montserrat Puerto Rico Saba St Christopher St Croix St John St Kitts Nevis St Lucia St Maarten St Thomas St Vincent Trinidad and Tobago Venezuela Virgin Islands Windward Islands
-4	-3	1	Bermuda Brazil West Canada Atlantic Chile Falkland Islands Greenland Thule Paraguay
-3.5	-2.5	1	Canada Newfoundland
-3		0	Argentina French Guiana Guyana Suriname Uruguay
-3	-2	1	Greenland St Pierre & Miquelon
-3	-1	2	Brazil East
-2	-3	-1	Antarctica

-1	-2	-1	Brazil Atlantic Islands
-1		0	Cape Verde
-1	0	1	Azores Greenland Scoresbysun
0		0	Ascension Burkina Faso Cote d'Ivoire Gambia Ghana Guinea Iceland Liberia Mali Mauritania Morocco Principe Island Sao Tome e Principe Senegal Sierra Leone St Helena Togo
0	1	1	Canary Islands Channel Islands England Faroe Island Ireland Republic of Madeira Northern Ireland Scotland United Kingdom Wales
1		0	Angola Benin Cameroon Central African Rep Chad Congo Dahomey Equatorial Guinea Gabon Niger Nigeria Tunisia Zaire Kinshasa Mbandaka

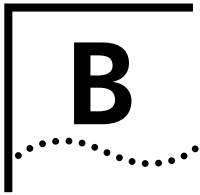
1	2	1	Albania Algeria Andorra Austria Balearic Islands Belgium Bosnia Hercegovina Croatia Czech Republic Denmark France Germany Gibraltar Hungary Italy Luxembourg Macedonia Mallorca Islands Malta Melilla Monaco Namibia Netherlands Norway Poland Portugal San Marino Slovakia Slovenia Spain Sweden Switzerland Vatican City Yugoslavia
2		0	Botswana Burundi Lesotho Libya Malawi Mozambique Rwanda South Africa Sudan Swaziland Zaire Kasai Zaire Haut Zaire Zaire Kivu Zaire Shaba Zambia Zimbabwe

2	3	1	Belarus Bulgaria Cyprus Egypt Estonia Finland Greece Israel Jordan Latvia Lebanon Lithuania Moldova Moldovan Rep Pridnestrovye Romania Russian Federation zone one Syria Turkey Ukraine
3		0	Azerbaijan Bahrain Djibouti Eritrea Ethiopia Kenya Kuwait Madagascar Mayotte Qatar Saudi Arabia Somalia Tanzania Uganda Yemen
3	4	1	Iraq
3.5		0	Iran
4		0	Georgia Mauritius Oman Reunion Seychelles United Arab Emirates
4	5	1	Armenia Russian Federation zone three Russian Federation zone two
4.5		0	Afghanistan

5		0	Maldives Pakistan Turkmenistan Uzbekistan
5	6	1	Kyrgyzstan Russian Federation zone four
5.5		0	India Sri Lanka
5.75		0	Nepal
6		0	Bangladesh Bhutan Tajikistan
6	7	1	Kazakhstan Russian Federation zone five
6.5		0	Myanmar
7		0	Cambodia Indonesia West Laos Thailand Vietnam
7	8	1	Russian Federation zone six
8		0	Australia Western Brunei China People's Rep Hong kong Indonesia Central Malaysia Mongolia Philippines Singapore Taiwan
8	9	1	Russian Federation zone seven
9		0	Indonesia East Japan Korea Dem Republic of Korea Republic of Palau
9	10	1	Russian Federation zone eight
9.5		0	Australia Northern Territory
9.5	10.5	1	Australia South
10		0	Australia Queensland Guam Mariana Island Northern Mariana Islands Papua New Guinea

10	11	1	Australia New South Wales Australia Victoria Australia Australian Capital Territory Australia Tasmania Russian Federation zone nine
10.5	11	0.5	Australia Lord Howe Island
11		0	Caroline Island New Caledonia New Hebrides Ponape Island Solomon Islands
11	12	1	Russian Federation zone ten Vanuatu
11.5		0	Norfolk Island
12		0	Fiji Kiribati Kusaie Marshall Islands Nauru Republic of Pingelap Tuvalu Wake Island Wallis and Futuna Islands
12	13	1	New Zealand Russian Federation zone eleven
12.75	13.75	1	Chatham Island
13		0	Tonga





# TECHNICAL SPECIFICATIONS

This chapter contains information about Technical Specifications for the RAS 1500.

---

## Certification

### **United States    FCC Part 15 Compliance Statement**

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. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**For More Information**

If these suggestions do not help, you might consult the following booklet:

Interference to Home Electronic Entertainment Equipment Handbook

You can order the booklet from the U.S. Government Printing Office, Washington, DC 20402. Ask for stock number 004-000-00498-1.

**Analog V.34 Model:  
FCC Part 68  
Compliance  
Statement**

This equipment complies with Part 68 of the FCC rules concerning:

- FCC Registration Number: labeled on the board
- Facility Interface Code: 02LS2
- Service Order Code: 9.OF
- USOC Jack: RJ11C
- REN: 0.4B
- Equipment Jack: CA-A11

**Canadian  
Installations**

**NOTICE:** The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction. Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment. Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.



**CAUTION:** *Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.*

### BRI U Model

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada (formerly the Canadian Department of Communications).

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par l'Industrie Canada (anciennement le ministre des Communications).

### Physical Dimensions

RAS 1500 has the following physical dimensions:

Length:	14.0"	35.56 cm
Width:	17.0"	43.18 cm
Height:	1.75"	4.445 cm

### Interfaces

#### Console Interface

- Electrical specification: RS-232-C (EIA/TIA-232-E standard)
- Connector: DB-9 male
- Configuration: DTE
- Transmission method: Unbalanced RS-232
- Transmission rate: 230 kbps

#### LAN Interface

- Data Transfer Rate: 10 Mbps
- Accessing Scheme: CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
- Topology: Star Wired hub (using multiport repeater)
- Maximum Nodes: Limited only by repeater used
- Transmission Medium: Unshielded Twisted Pair (UTP)
- Network Lobe Distance: 100 meters (328 ft.) suggested maximum. Longer cabling may be used at the expense of reduced receiver squelch levels.
- Connector: RJ-45 8-position modular jack, Stewart 88-360808 or equivalent

### **WAN Interface - Cabling Specifications**

- Wire Type: 10 Mbps: CAT 3 or CAT 5 twisted pairs 100 Mbps: CAT 5 twisted pairs
- Max. Cable Distance: 100 meters (328 ft.) suggested maximum. Longer cabling may be used at the expense of reduced receiver squelch levels.
- Cable Loss: Must be  $\leq 11.5$  dB/100 m for frequency range of 5-10 MHz
- Characteristic Impedance: 85-111 Ohms for frequency range of 5-10 MHz
- Propagation Delay: 5.7 nanoseconds/meter
- Cabling: RJ-45 plug to RJ-45 plug straight through for multiport repeater applications (transmit to receiver crossover cable for two-node network).

### **FireWire**

- Electrical specification: N/A
- Connector: IEEE P1394
- Configuration: N/A
- Transmission method: High Speed Serial Bus (HSSB)
- Transmission rate: N/A
- Environmental
- Shipping and Storage Temperature: 0°C - 40°C, 32°F - 104°F
- Shipping and Storage Relative Humidity: 0 - 95%, non-condensing
- Operating Temperature: 0°C - 40°C, 32°F - 104°F
- Operating Relative Humidity: 0 - 95%, non-condensing

## Power Requirements

Voltage (VDC)	Maximum Current (A)	Maximum Power Output (W)
12	2.5	30
5	12 *	35
3.3	10 *	33

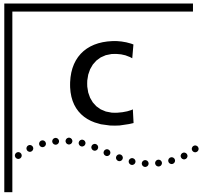


*The 5 and 3.3 VDC outputs “power-share.” Since the maximum power output of the 12 VDC supply is 30 W, the remaining 40 W is shared between the 3.3 and 5 VDC supplies. If no load in 3.3 V and 12 V limited to 0.6 A, then 5 V can deliver 12 A.*

Input Voltage: 90 - 264 VAC, 47 - 63 Hz

Maximum Input Current: 2.5 A





# TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the very latest, 3Com recommends that you access the 3Com Corporation World Wide Web site.

---

## **Online Technical Services**

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com FTP site
- 3Com Bulletin Board Service (3Com BBS)
- 3ComFacts<sup>SM</sup> automated fax service

## **World Wide Web Site**

Access the latest networking information on the 3Com Corporation World Wide Web site by entering the URL into your Internet browser:

**<http://www.3com.com/>**

This service provides access to online support information such as technical documentation and software library, as well as support options ranging from technical education to maintenance and professional services.

## **3Com FTP Site**

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com** (or **192.156.136.12**)
- Username: **anonymous**
- Password: **<your Internet e-mail address>**



*A user name and password are not needed with Web browser software such as Netscape Navigator and Internet Explorer.*

### **3Com Bulletin Board Service**

The 3Com BBS contains patches, software, and drivers for 3Com products. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

#### **Access by Analog Modem**

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

<b>Country</b>	<b>Data Rate</b>	<b>Telephone Number</b>
Australia	Up to 14,400 bps	61 2 9955 2073
Brazil	Up to 14,400 bps	55 11 5181 9666
France	Up to 14,400 bps	33 1 6986 6954
Germany	Up to 28,800 bps	4989 62732 188
Hong Kong	Up to 14,400 bps	852 2537 5601
Italy	Up to 14,400 bps	39 2 27300680
Japan	Up to 14,400 bps	81 3 3345 7266
Mexico	Up to 28,800 bps	52 5 520 7835
P.R. of China	Up to 14,400 bps	86 10 684 92351
Taiwan, R.O.C.	Up to 14,400 bps	886 2 377 5840
U.K.	Up to 28,800 bps	44 1442 438278
U.S.A.	Up to 53,333 bps	1 847 262 6000

#### **Access by Digital Modem**

ISDN users can dial in to the 3Com BBS using a digital modem for fast access up to 64 Kbps. To access the 3Com BBS using ISDN, use the following number:

**1 847 262 6000**



### **3ComFacts Automated Fax Service**

The 3ComFacts automated fax service provides technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3ComFacts using your Touch-Tone telephone:

**1 408 727 7021**

---

### **Support from Your Network Supplier**

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

---

### **Support from 3Com**

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, please call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Below is a list of worldwide technical telephone support numbers:

Country	Telephone Number	Country	Telephone Number
<b>Asia Pacific Rim</b>			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or
Hong Kong	800 933 486		021 6350 1590
India	61 2 9937 5085	Singapore	800 6161 463
Indonesia	001 800 61 009	S. Korea	
Japan	0031 61 6439	From anywhere in S. Korea:	82 2 3455 6455
Malaysia	1800 801 777	From Seoul:	00798 611 2230
New Zealand	0800 446 398	Taiwan, R.O.C.	0080 611 261
Pakistan	61 2 9937 5085	Thailand	001 800 611 2000
Philippines	1235 61 266 2602		
<b>Europe</b>			
From anywhere in Europe, call: +31 (0)30 6029900 phone			
+31 (0)30 6029999 fax			
From the following European countries, you may use the toll-free numbers:			
Austria	06 607468	Netherlands	0800 0227788
Belgium	0800 71429	Norway	800 11376
Denmark	800 17309	Poland	0800 3111206
Finland	0800 113153	Portugal	05 05313416
France	0800 917959	South Africa	0800 995014
Germany	0130 821502	Spain	900 983125
Hungary	00800 12813	Sweden	020 795482
Ireland	1 800 553117	Switzerland	0800 55 3072
Israel	177 3103794	U.K.	0800 966197
Italy	1678 79489		
<b>Latin America</b>			
Argentina	AT&T +800 666 5065	Mexico	01 800 CARE (01 800 2273)
Brazil	0800 13 3266	Peru	AT&T +800 666 5065
Chile	1230 020 0645	Puerto Rico	800 666 5065
Colombia	98012 2127	Venezuela	AT&T +800 666 5065
<b>North America</b>			
	1 800 NET 3Com		
	(1 800 638 3266)		

## Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	65 543 6500	65 543 6348
Europe, South Africa, and Middle East	+ 44 1442 435860	+ 44 1442 435718
From the following European countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	06 607468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0130 821502	
Hungary	00800 12813	
Ireland	1800553117	
Israel	177 3103794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	05 05313416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
Latin America	1 408 326 2927	1 408 326 3355
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266)	1 408 326 7120



# INDEX

---

## Numbers

- 2100 Hz answer tone
  - disable 139
  - enable 139
- 3Com bulletin board service (3Com BBS) 286
- 3Com URL 285
- 3ComFacts 287
- 56 kbps technology 151

---

## A

- accounting server
  - RADIUS 195
  - settings 195
- adding network services 163
- address pools
  - configuring 72
- administrative tools
  - adding network services 163
  - communicating with remote and local sites 161
  - deleting network services 165
  - dial and connect commands 161
  - disabling network services 165
  - discarding files 161
  - displaying system information 173
  - enabling network services 165
  - ending an active process 168
  - exiting the CLI 162
  - renaming files 161
  - resolving addresses with ARP 169
  - resolving host names 169
  - running script files 159
  - show connection attributes 173
  - show memory attributes 173
  - using network services 163
  - using Rlogin 166
  - using Telnet 166
  - using Telnet control characters 167
  - using TFTP 166
  - viewing facility errors 168
  - viewing interface status and settings 172
  - viewing system settings 172
  - viewing Telnet status 167

## ARP

- resolving addresses with 169
- using 169

## ARQ

- description 134, 136
- setting negotiation 149

## AT commands

- basic dial commands 131
- call control settings 149
- configuring data compression settings 134
- dial command options 132
- disconnecting 133
- error control 136
- help 131
- link options 140
- modifying carrier delay times 138
- overview 130
- sending 130
- using stored telephone numbers 133

## authentication

- RADIUS encryption key 179

## auto answer 151

## automatic repeat request. see ARQ

---

## B

- backward explicit congestion notifications 203
- bandwidth allocation 94
- Bc\_MAX 203
- Bc\_MIN 203
- BEEN 203
- bulletin board service 286

---

## C

- call waiting 138
- carrier wait time after dialing 150
- case study
  - dialin user 88
  - LAN-to-LAN user 105, 267
- CIR 203
- CLI
  - capabilities 20
  - configuring with 25

- exiting 162
  - Quick Setup 24
- command line interface. See CLI
- committed burst size 203
- committed information rate 203
- communicating with remote and local sites 161
- configuration
  - frame relay 206
- congestion control 203
- congestion monitoring period 203
- congestion notifications 203
- connect speed
  - maximum 140
  - minimum 140
- connect speeds 140
- conventions
  - notice icons, About This Guide 14
  - text, About This Guide 14
- critical events
  - displaying 173

---

## D

- data compression
  - MNP-5 134
  - V.42 bis 134
- data link connection identifier 202
- datalink configuration 208
- date
  - displaying 194
  - setting 194
- daylight saving time
  - displaying 194
  - setting 193
- dial command 161
- dial in connections
  - viewing settings 173
- dial tone 151
- dialout service
  - editing network services 65
  - Telnet case study 67
- disable auto answer 149
- disable server x2 151
- DISC 146
- disconnect reasons 146
- DLCI 202

---

## E

- enable auto answer 149
- error control
  - description 137
  - using 137

- escape code 146
- exit commands 162

---

## F

- fax service (3ComFacts) 287
- FECN 203
- files
  - deleting 161
  - renaming 161
- filters
  - adding filters to the managed list 230
  - advertisement filters 219
  - assigning filters 228
  - call filters 220
  - capabilities 218
  - configuring filters 226
  - creating 220
  - data filters 219
  - deleting 232
  - displaying managed filter list 227
  - file components 220
  - filter out all IP options switch 242
  - generating SYSLOG messages 232
  - generic filter rules 223
  - generic filters 220
  - global filtering 241
  - ICMP filtering 239
  - input filters versus output filters 228
  - interface filters 227
  - IP call filtering 240
  - IP filter examples 234
  - IP RIP filtering 238
  - keywords 242
  - managing filters 230
  - masks 235
  - overview 218
  - protocol rules 221
  - protocol sections 221
  - removing from a user profile 231
  - removing from an interface 231
  - setting filter access 227
  - source and destination address filtering 234
  - specifying the filtering action 224
  - standard port numbers 237
  - TCP/UDP filtering 235
  - types 219
  - user filters 228
  - verifying contents 232
  - verifying syntax 232
  - viewing filter files 232
- flash memory 147
- flow control 137

forward explicit congestion notifications 203

frame relay

Bc 203

BECN 203

BECN\_CMP 203

CIR 203

configuration 206

congestion control 203

datalink configuration 208

DCLI 202

LMI 203

PVC 202

PVC statistics 211

Tc 204

troubleshooting 211

---

## G

GMT offset

displaying 194

setting 194

GSTN clear down 146

---

## H

help

for AT commands 131

---

## I

idle time before disconnect 150

inactivity timeout 146

IP network user

case study 78, 89

configuring PPP parameters 76

setting idle and session timeouts 78

setting phone numbers 78

specifying a remote address 75

IP on Demand 110

IP terminal server setup

configuring login hosts 120

ISDN

configuring 152

selecting frame and window size 152

---

## K

keypress abort 146

---

## L

LAN-to-LAN routing 92

adding the user 98

bandwidth allocation 94

case study 105, 267

configuring network parameters 98

connection types 93

connections to remote gateways 96

dialout scripts 94

PAP and CHAP authentication 96

setting internal networks for unnumbered  
links 96

spoofing 96

LMI 203

local management interface 203

login hosts

configuring 120

login users

adding the user 121

case study 126

loop loss disconnect 146

loss of carrier 146

---

## M

manual setup

default gateway configuration 26

IP configuration 26

maximum connect speed 140

memory

viewing usage 173

MIBs 285

minimum connect speed 140

MLPPP

bandwidth allocation 94

MNP error control 137

MNP incompatibility 146

MNP-5 data compression 134

modem call information 144

---

## N

NAT 253

Network Address Translation. See NAT

network dial-in access

case study 88, 89

configuring address pools 72

configuring PPP parameters 76

remote computer setup 71

network dial-out access

configuration overview 61

network services

adding 163

deleting 165

disabling 165

enabling 165

network supplier support 287

---

## O

on-demand routing 96  
online technical services 285

---

## P

PAT 253  
pause code 138  
permanent virtual circuit 202  
permanent virtual circuits 202  
ping  
    set ping 171  
    using 169  
Port Address Translation. See PAT  
port numbers for common services 237  
PVC 202, 206  
PVC configuration 209  
PVC statistics 211

---

## R

RADIUS  
    accounting  
        enabling and disabling 198  
        examples 198  
    authentication  
        choosing primary server 180  
        configuring 180  
        shared secret 179  
RAS 1500 applications  
    applications overview 18  
    network dial-in access 18  
resolving addresses  
    with ARP 169  
retransmit limit 146  
returning products for repair 289  
RFC 1490 203  
Rlogin  
    setting for login user 121  
    setting port for login user 120  
    using 166

---

## S

scripts  
    example 159  
software configuration  
    configuring a manage user 32  
    finding IPX network number 27  
    IP configuration 26

    IPX configuration 27  
        setting default domain 30  
        setting IPX parameters 29  
spoofing 96  
standard port numbers 237  
switched virtual circuits 202  
system information  
    displaying 173  
system settings  
    viewing 172

---

## T

Tc 204  
technical support  
    3Com URL 285  
    bulletin board service 286  
    fax service 287  
    network suppliers 287  
    product repair 289  
Telnet  
    case study 67  
    setting port for login user 121  
    using 166  
    viewing status 167  
TFTP  
    using 166  
time  
    displaying 194  
    setting 194  
time zone  
    displaying 194  
    setting 194  
troubleshooting  
    frame relay 211  
    resolving addresses 168  
    resolving host names 168  
    using ping 169  
    viewing facility errors 168  
    viewing memory usage 173

---

## U

UDP broadcast forwarding 251  
Universal Connect 154  
URL 285  
user datagram protocol broadcast forwarding. See  
    UDP broadcast forwarding

---

## V

V.42 bis data compression 134  
V.42 error control 136



V.90 151

---

**W**

Windows 95 Dial Up Networking 89  
World Wide Web (WWW) 285

---

**X**

X.75 152



# 3COM LIMITED WARRANTY

## SuperStack II Remote Access System 1500

---

### HARDWARE

3Com warrants this hardware product to be free from defects in workmanship and materials, under normal use and service, for the following length of time from the date of purchase from 3Com or its authorized reseller:

Five (5) years

3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, 3Com may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

---

### SOFTWARE

3Com warrants that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. Free software upgrades are available through 3Com's support Web site. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with 3Com's published specifications or user manual.

---

### YEAR 2000 WARRANTY

In addition to the Hardware Warranty and Software Warranty stated above, 3Com warrants that each product sold or licensed to Customer on and after January 1, 1998 that is date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com product, including hardware, software, and firmware, accurately exchange date data with the 3Com product, with the exception of those products identified at 3Com's Web site, <http://www.3com.com/products/yr2000.html>, as not meeting this standard. If it appears that any product that is stated to meet this standard does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days after purchase or until April 1, 2000, whichever is later.

---

### OBTAINING WARRANTY SERVICE

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product.

*Dead- or Defective-on-Arrival.* In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

*Telephone Support*, with coverage for basic troubleshooting only, will be provided for ninety (90) days, on a commercially reasonable efforts basis. Telephone support from 3Com is available from 3Com only if Customer purchased this product directly from 3Com, or if Customer's reseller is unable to provide telephone support. Please refer to the Technical Support appendix in the user guide for telephone numbers.

---

## **WARRANTIES EXCLUSIVE**

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

---

## **LIMITATION OF LIABILITY**

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

---

## **DISCLAIMER**

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

---

## **GOVERNING LAW**

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

**3Com Corporation**  
5400 Bayfront Plaza  
Santa Clara, CA 95054  
(408) 326-5000