SuperStack®
Remote Access System 1500
Reference Guide

Release 3.0

http://www.3com.com/

Part No. 10041004 Rev AA
November, 2000

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

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.

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

1 ROUTER CONFIGURATION OVERVIEW

A MODEM COMMAND REFERENCE

B MODEM DISCONNECT AND RESULT CODES

C ADDRESSING SCHEMES

D Event Messages

Index

ABOUT THIS GUIDE

This guide describes how to configure the software for the SuperStack Remote Access System (RAS) 1500.

This guide is intended for administrators with knowledge of networking, telephony, and remote-access applications. While the initial configuration can be accomplished with the help of the RAS 1500 Quick Setup program, a more substantial configuration requires a broader understanding of networking principles.

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

Conventions

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

Table 1 Notice Icons

Icon	Notice Type	Description
i	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`	The word “syntax” means you must evaluate the syntax provided and supply the appropriate values. Placeholders appear in angle brackets for values that you must supply. Example: Set callback user primary dial-back number `Set user <name> phone_number <number>` In this example, you must supply the username for <name> and phone number for <number>.
`Commands`	The word “command” means you must enter the command exactly as shown in text and press the Return or Enter key. Example: To list the current IP routes, enter the following command: **`list IP routes`** *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.*
`Screen displays`	This typeface represents information as it appears on the screen.
The words “enter” and “type”	When you see the uppercase word “enter” in this guide, press the Enter key. Do not press Enter when an instruction simply says “type.”
Words in *italics*	Italics are used to indicate the following: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify CLI command parameters, for example: Supply the *IP address* parameter.

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 Remote Access System 1500*

This document describes how to perform the memory upgrade for the Remote Access System 1500.

- *Firmware Upgrade SuperStack Remote Access System 1500*

  This document describes how to perform the upgrade procedures for the SuperStack Remote Access (RAS) 1500 Base Unit and the RAS 1500 Port Expansion Unit.

- *I/O Module Installation Guide SuperStack 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 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 Remote Access System 1500 Quick Setup Guide*

  This guide describes the installation and initial configuration of the RAS 1500 system.

- *SuperStack Remote Access System 1500 System Management Guide*

  This guide describes how to configure your RAS 1500 system. It is located on the RAS 1500 Resource CD-ROM.

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`

1

ROUTER CONFIGURATION OVERVIEW

The SuperStack Remote Access System (RAS) 1500 and related components are Simple Network Management Protocol (SNMP) manageable by a RAS 1500 via a Telnet connection. The parameters you set through these interfaces are stored in a number of tables that reside in the card FLASH memory.

This chapter includes the following sections:

- Setting Up Applications
- Configuration Command Overview
- Configurable Table Overview

Setting Up Applications

The command line interface (CLI) allows you to perform the four basic applications listed below. Refer to the appropriate chapter in the *SuperStack Remote Access System (RAS) 1500 System Management Guide* for more information.

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

Configuration Command Overview

Configuration data is stored in several tables (user and interface tables, for example). You can change most parameters in these tables using the generic `set` command:

```
set [user|interface|system|etc.] <parameter name> <value>
```

Example:

```
set user maximillian message “Mexico is Mine”
```

Many objects, such as users, must be created before they can be configured. Use the generic `add` command:

```
add [user|filter|etc] <name>
```

Anything that you can add can also be deleted, disabled or enabled. Use these generic commands:

```
delete [user|filter|etc.] <name]
disable [user| filter|etc.] <name]
enable [user|filter|etc.] <name]
```

You can view current configuration information with either the `show` or `list` command. List commands display table entries, show commands display information about a specific table or non-table entry.

Example:

```
show network backbone
show user John
list networks
list users
```

For a complete list of commands and options see Chapter 4, "Router Command Reference." Also, you can access the online `help` command by typing the following:

```
help <command> ENTER
```

Configurable Table Overview

This section briefly describes some important internal databases, or tables, that contain configuration information accessed by `list <keyword>` commands. Not *all* RAS 1500 tables are detailed.

Interface Tables

These tables contains Call Information Process (CIP) and local area network (LAN) information about all interfaces, including modem groups, modem ports, and Ethernet interfaces. They include the *CIP Port Parameters Table, Modem Port Parameter Table, Modem Group Interface Table,* and *Modem Group Table.*

User Table

This table contains authentication and configuration information for five types of users: Login, Network, Callback, Dial-out, and Manage.

Login	Login users are remote users dialing in to request terminal service from an IP host. Once such a user is authenticated, he or she is connected to a host with a login service such as Telnet or Rlogin
Network	Network users are remote users dialing in to become a virtual node of the local network. Such a user may be an individual attaching to the network or an entire LAN dialing in to route packets onto the local network.
Callback	Callback users are remote users who dial into the device. Once the user is authenticated, the RAS 1500 disconnects and dials the user back, using a predefined or user-entered telephone number.
Dial-out	Dial-out users are local or remote users who login then connect to a remote host.
Manage	Manage users have administrator-level privileges on the Console or a dial-up session.

User table entries override settings for the interface to which the user is connected.

Local and Login Hosts Tables

The Local Hosts Table contains a list of local hosts and associated Internet Protocol (IP) addresses. It is used to translate names to IP addresses and vice versa. This allows users and administrators to type host names rather than addresses.

The *Hosts Table* is especially useful if your network does not have a name service such as Domain Name Service (DNS). If your network has a name server, the server first tries to match the host name with an IP address using the Hosts Table before using the name server.

The *Login Host Table* contains hosts you configured using the `add login_host` command.

Initialization Script and Global Host Tables

These tables contain generic modem initialization setup scripts that can be sent to a modem each time the port is reset. (A modem resets itself every time it disconnects.)

Initialization scripts for modems will probably contain the AT commands needed to configure them for use on your network. This table contains information accessed by the `list init_scripts` command.

Facility Level Table

This table is used to configure the log level of all *facilities* (software systems) on the RAS 1500. It contains each event facility and its associated log level. Each facility generates unique event messages during processing that can be sent to a SYSLOG server you define as a means of judging system performance.

Facilities are configurable in that you can change log levels from the defaults shown below. Available log levels are *verbose, common, unusual, and critical*, with critical being the most severe event. This table contains information accessed by the `list facilities` command.

Module Table

This table contains information used by *processes* or management features that run in the background. Display a list of these items using the `list processes` command.

IP Network Table

The *IP Network Table* contains all generic protocol information about IP networks entered with the `add ip network` command.

IP Address Pool Table

This table holds information on user-configured IP addresses entered with the `add ip pool` command.

IP Interface Block Table

This table contains IP addresses associated with each system interface. Interfaces with point-to-point connections show the neighbor field with the address of the remote system. Use the `list ip interface_block` to display this table.

Forwarding and IP Routing Tables

These tables contain static and dynamic routing information. Dynamic routes are updated by broadcasts received from other routing devices on the network using Routing Information Protocol (RIP). Static routes are added to the table manually. A static route to a given site will override a dynamic route.

Static routes to a given site are required when the site is not running dynamic routing. Without dynamic routing protocol messaging, the RAS 1500 cannot gather information on the location of other routers, gateways, and remote hosts. The RAS 1500 must know exactly where to send a packet.

SNMP Configuration Tables

The RAS 1500 provides support for SNMP version 1 and industry standard MIB-II variables. These variables are fully described in your MIB-II documentation.

The *SNMP Community Table* stores information about which SNMP servers (if any) are permitted to make SET and GET requests, as well as Read and Write Communities.

The *SNMP Trap Community Table* saves names and addresses of trap communities.

The *SNMP Community* table saves names and addresses of communities as associated pools.

SYSLOG Table

This table contains IP addresses of SYSLOG hosts to which event messages are sent. You can define multiple SYSLOG hosts that record event messages by the message's log level. Use the `list syslogs` command to display this table.

Event Critical Messages Table

This table contains event messages logged *critical*. Using the `list critical events` command displays these messages to Telnet and dial-in sessions as well as the default Console session.

Filter and Associated Tables

Filter file names of filters you create are stored in the *Filter Table* but the filters themselves are stored as ASCII text in FLASH memory. The *Access Filter Table* determines whether user filters take precedence over interface filters. Use the `list filters` command to display this table.

File Table

This table contains system files and other files you may have loaded in the RAS 1500 including filter files. Use the `list files` command to display this table.

Network Services and Available Servers Tables

The *Network Services* and *Available Servers* tables hold information related to the RAS 1500-supported network services such as Telnet, SNMP, ClearTCP, Dial-Out, and Trivial File Transfer Protocol (TFTP). These default services can be edited or new services created with the `add` and `set network services` commands. Use the `list network services` and `list available servers` commands to display these tables.

Dial-Out Port Table

This table lists virtual ports available for NCSI dial-out service. Use the `list dial_out` command to display this table.

UDP Listeners Table

This table details User Datagram Protocol (UDP) ports being used by the RAS 1500. These ports correspond to processes that are receiving UDP data (for example, SNMP, User Management, TFTP service). Use the `list udp listeners` command to display this table.

TCP Connections Table

The *TCP Connections Table* contains information regarding all system and user-created Transmission Control Protocol (TCP) links. Use the `list tcp connections` command to display this table.

DNS and Associated Tables

The DNS tables in the RAS 1500 contain resource records about address resolution. The tables include the *DNS Host Table, DNS Server Table, DNS Cache and Negative Cach*e tables, and *Resolve Cache* and *Negative Cache* tables. Use the `list dns` command to display these tables.

TFTP Access Table

The *TFTP Access Table* contains information about available clients for TFTP service. Use the `add tftp client` command to add entries to this table. Use the `list tcp clients` command to display this table.

Remote Ping and Ping Busy Out Tables

These tables contain a host of information regarding Internet Control Message Protocol (ICMP) entries for local and remote ping requests. Entries are added to the *Remote Ping Table* using the `ping` command.

Address Translation Table

This table contains the network address to physical address equivalences resolved by Address Resolution Protocol (ARP). Use the `arp <ip address>` command to display this table.

CIP Port Parameter Table

This *CIP Table* contains information regarding current connections on the RAS 1500 derived from the `list connections` command.

User Manager Active Sessions Table

This table contains protocol and other information regarding current network or login sessions. Use the `list sessions` command to display this table.

Modem Tables

Modem tables contain entries for *Data Compression, Call Control, Error Correction, Call Statistics,* and *Signal Conversion*, among others. These tables are associated with the `add modem_group` command.

PPP Tables

Several Point-to-Point Protocol (PPP) tables contain entries regarding PPP connections on the RAS 1500. These include the following tables:

- PPP Link Table
- PPP Authentication Table

2 ADMINISTRATIVE TOOLS

This chapter covers administrative commands used for the following:

- Reconfiguring Your System
- Troubleshooting Commands
- Displaying System Information

Reconfiguring Your System

The commands detailed in this section control configurable aspects of your system.

Customizing CLI Parameters

Command Prompt

Use `set command` if you have more than one SuperStack Remote Access System (RAS) 1500 and want to differentiate between them or want to customize your prompt from the default. The prompt can be up to 64 characters. Use the following command:

```
set command prompt <“prompt message”>
```

Example:

```
set command prompt Welcome!
```

Command History

If you want to customize the history function to change the default (10), use the following command. The limit is 500 commands. Use the following command:

```
set command history <depth>
```

Idle Timeout

If you want to ensure that a console login user is employing 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]
```

Local Prompt

If you want to specify a separate prompt for a command file process, use the `local_prompt` parameter. This 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 local_prompt <string>
```

Example:

```
set command local_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 wide area network (WAN). Use the following command:

```
set system
     name [name]
     location [location]
     contact [contact information]
     transmit_authentication_name [keyword]
```

Example:

```
set system name “big house” location DC contact “staff, ext
555” transmit_system_na “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 command line interface (CLI) commands. To use this command, create a file containing the CLI commands you want to implement, Trivial File Transfer Protocol (TFTP) the file to the FLASH ROM, and type `do <filename>`.

Software Downloads

For information about downloading software through the console port, refer to the *SuperStack Remote Access System 1500 System Management Guide*. For information about downloading software through the Web Configuration Interface refer to the Web Configuration tool online help.

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>`.

Dial, Connect and Hangup Commands

You can dial up a remote or local user 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 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>
```

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 write a configurable message to all dial-in users when connections are made on that modem. This information is helpful for diagnostic purposes. The `show interface` command displays the message as written.

All CLI string values including spaces must be enclosed in quotations.

Example:

```
set switched interface rm0/slot:1/mod:2 message “Welcome to
the RAS 1500”
```

Exiting the CLI

Bye, Exit, Leave, Quit Commands

The `bye`, `exit`, `leave`, and `quit` commands shut down the CLI but leave the connection open. These commands are only valid in dial-in and Telnet sessions.

Logout Command

`Logout` exits the CLI and closes the connection, ending a dial-in user or Telnet session.

Network Services

To use ClearTCP, SNMP, or Dial-Out and to set values associated with them, add each *network service* and related parameter. Telnet and TFTP are already *enabled* at startup although you can add additional services whenever necessary.

For more information about adding dial-out network service refer to the System Management Guide.

Adding Network Services

Use the `add network service` command shown below:

```
add network service [service_name]
     server_type [cleartcpd, dialout, snmpd,telnetd,tftpd]
     close_active_connections [false | true]
     data [ancillary entry]
     enabled [no | yes]
     socket [socket number]
```

Example:

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

To edit a network service, you must first disable it. After editing the service, enable it again.

If any data *value includes a space, enclose it in double quotations, for example, data modem_group=\"Boston calling\".*

`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 the following syntax.

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. Enclose in quotes and backslashes only when spaces are included. Default: **none**
login_prompt=string	ASCII string specifying the login prompt to be sent during authentication. Enclose in quotes and backslashes only when spaces are included. *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 allocates a modem from. Enclose in quotes and backslashes only when spaces are included. 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 network services` command after typing the example above displays the following:

```
CONFIGURED NETWORK SERVICES
                              Server                        Admin
Name                          Type       Socket   Close     Status
calls                         TELNETD    6001     FALSE     ENABLED
####DATA: auth=off, login_banner= “Welcome to My Net”,
login_prompt=“My Session,drop_on_hangup=on
tftpd                         TFTPD      69       FALSE     ENABLED
####DATA:
telnetd                       TELNETD    23       FALSE     ENABLED
####DATA:
hdmconsole                    TELNETD    23       FALSE     DISABLED
####DATA:
modem_group=”slot1”
```

`enabled` When you add a network service, it is enabled by default. When changing any parameter, you must first *disable* the service (see section below for more information), make your changes, then re-*enable* the service.

For example, for a network service named Telnet user:

```
disable network service telnet user
set network service telnet user data auth=off
enable network service telnet user
```

`server_type` Indicates 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. Use the following command:

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

To enable network service, use the following command:

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

Deleting a Network Service

To delete a network service, use the following command:

```
delete network service <service_name>
```

Using TFTP

Trivial File Transfer Protocol (TFTP) 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 PC as a TFTP client of the hub 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 the RAS 1500.*

*Important: **Do not** transfer binary files. Transferring binary files of any type will cause unexpected results and may cause the RAS 1500 to "hang".*

Using Rlogin and Telnet

You can connect to a specific host on the network using the `rlogin` or `telnet` command. You must first have used the `add dns host` or `add dns server` commands for the RAS 1500 to recognize an Internet Protocol (IP) host name.

`Rlogin` *is not supported into the RAS 1500. You can only use* **`rlogin`** *to communicate out of the 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
```

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 are output to the console port.

Although messages are sent to the Console port by default, you can configure a SYSLOG host to receive and save messages. See Appendix D, "Event Messages" for more information.

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 responds 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

Before you can resolve a host, you must have added a Domain Name Service (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.

Example:

```
add dns server 133.114.121.45 preference 1 name “Our DNS
server
add dns host hahvahd.college-hu.com  address 133.114.121.15
host hahvahd
```

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 the 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 maximum 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 Simple Network Management Protocol (SNMP) station. Use the following command:

```
ping <IP address>
      background [yes|no]
      count [maximum packets]
      data [string]
      interval [seconds]
      self_destroy_delay [minutes]
      size [data size]
      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
```

A ping of a *single* count produces the following, for example:

```
PING Destination: camel Status: ALIVE
```

Setting ping Row Ceiling

The `set ping maximum_rows` command sets the maximum number of rows permissible in the Remote Ping Table. Note that setting this parameter to a number smaller than the current number of rows does not cause any row deletions immediately but following any current ping. 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` and `set login user` commands. This user pings a login host, gets a successful/unsuccessful message, and is disconnected. Use these commands:

```
add user <username> type login
set login user <username> login_host <name or IP_address>
login_service ping
```

Example:

```
add user jack type login
set user jack login_host_name 3.3.3.3 login_service ping
```

Viewing the RAS 1500 System Information

You can use the `show system settings` 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.

Viewing Interface Status, Settings

Several commands are useful to display the active/inactive status and settings of specific interfaces (ports). They include the following:

- `list switched interfaces`
- `list interfaces`
- `show interface settings`
- `show switched interface`

Monitor PPP Activity

The `monitor ppp` command lets you view the following realtime 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.

These commands are fully detailed in Chapter 4, "Router Command Reference."

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 the events to be displayed on the console and syslogged over Telnet sessions by using the `set facility` command. This command is also 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 the following:

- `show memory`
- `show connection settings`
- `show connection counters`
- `show accounting settings`

For a full explanation, see the CLI Command Reference section of this guide.

Show Memory

The `show memory` command displays the system DRAM memory utilization.

Example:

```
SYSTEM MEMORY RESOURCES
Total System Memory Resources:                  3584 KB
Free Memory:                                    2282 KB
Code Size:                                      4598 KB
Initialized Data Size:                          0 KB
Uninitialized Data Size:                        5750 KB
Stack Size:                                     0 KB
```

Show Dial-in Connection Settings, 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` — The default is *default*.
- `Command Prompt` — Displayed when user dials in.
- `Service Prompt` — Prompt after dial-in user logs in (*LOGIN* or *NETWORK* service types available).
- `Message Prompt` — Prompt following service prompt for login/network service administrative user. The choices are *CONNECT, EXIT, HELP, LOGOUT, MANAGE, RLOGIN, and TELNET*

List Dial-in Connections

The `list connections` command displays all connections established on switched interfaces as configured with the `set connections` command. It lists the following:

- `IfName` — Modem slot and interface of current connections.
- `Username` — name of users currently connected.
- `Type` — current type of connections established on modems. They include the following:
  - *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 on the fly
  - *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, for example; *NONE, PPP, SLIP, RLGN, TLNT, PING, ADMN, CLTCP,* and *INVALID*.

- *Start Date* — start date of a connection established on the specified interface.
- *Start Time* — start time of a connection established on the specified interface.

An example is shown below.

CONNECTIONS

IfName	User Name	Type	DLL	Start Date	Start Time
rm0/slot:1/ mod:1	larry	DIALIN	NONE	05-AUG-2041	13:56:1
rm0/slot:1/ mod:2	ginger	SHRMOD	NONE	05-AUG-2041	13:57:2
rm0/slot:1/ mod:3	gina	DIALIN	PPP	21-FEB-1998	10:26:1

3 ROUTER COMMAND OVERVIEW

This chapter contains the following information:

- Command Format
- Entering Commands
- Command Language Structure

Command Format

Many commands are position-independent and multitiered and use keywords. Multitiered commands let you type the base command (for example, `set interface`) and implement many more parameters (host_type, host_address, etc). Position independence does not require all parameters to be specified at once, nor in sequence, to work. But typing a keyword in the base command such as `network` in `set ip network` is mandatory to enable the command. Command syntax is shown in the example below:

```
add ip network <network_name>
   address [IP address]
   {enabled [no | yes] }
   {frame [ethernet_II, snap] }
   {interface [rm0/eth:1] }
```

- `add ip network` is the command; `<network_name>` the required value
- `address` is a required parameter; `[IP address]` the value for the IP address
- `{enabled}` is the network "on" value; choices: `[no or yes]`
- `{frame}` is the encapsulation type; choices: `[ethernet_ii or snap]`
- `interface` is the LAN connection - *rm0/eth:1*

Parameters

- **{** … **}** parameters enclosed by *curly braces* are optional and are provided with *default* values. You do not need to specify these parameters unless you wish to override the default.
- **<** … **>** values enclosed by *arrows* are used by a command or parameter that is position-dependent and does not have keywords. Some of these parameters are required; some are not. Required values are displayed in the command line interface (CLI) when querying a command (typing a question mark) or upon issuing a command where required values were omitted.
- **[** … **]** range of values following keywords are enclosed in *brackets*. Inside the brackets, if you see a:
  - **|** (vertical bar) you may select only *one* from the *key list*: [first | second | third]
  - **,** (comma) you can select *one or more* of the displayed *bitmasks*: [first,second,third,...]
- *Position independent* arguments are shown in a vertical array after the command.

Entering Commands

Commands can be entered in abbreviated form if the portion of the command you type is unique (shown below). You can also use command completion and positional help when entering command strings.

Using Control Characters

- While working in the CLI, system messages may scroll across your screen. To recall the last thing you typed, press the up arrow. This can be helpful if you are unsure exactly where you were when you received the system message.
- If you have typed ahead to enter a series of commands and you want to stop processing your commands, you can press (Ctrl c) to abort any currently executing and stacked commands.
- Commands can be retrieved by typing [Ctrl p] (for previous) and [Ctrl n] (for next). Command retrieval consults the history of previous fully entered commands, defaulting at the last ten commands. If an error occurs while a command is processing, any partial command (up to and including the field in error) is added to the history list.
- Command line editing allows these options: (Ctrl b) or left arrow brings you go back one character; (Ctrl c) deletes the running CLI process; (Ctrl f) or right arrow takes you forward one character; (ESC

b) takes you back one word; (ESC f) takes you forward one word; (Ctrl a) takes you to the beginning of a command; (Ctrl e) takes you to the end of a command, and (Ctrl d) or (Ctrl k) deletes a selected character.

Abbreviation and Command Completion

- Commands can be *abbreviated* if arguments you write are unique. For example, you can type `se us jay pa bird`, short for: `set user jay password bird` is acceptable, but `se us jay m “Fly this coop”` is not unique because `m` can stand for `message` or `modem_group`.

*Identifiers such as **jay** in the above example are not completed.For brevity, some commands in this chapter are abbreviated and annotated (abbr.).*

- Some parameters are omitted in examples because they default to standard values and do not require entry, or are unnecessary for common configuration.
- *Command completion* finishes spelling a unique, abbreviated value for you if you press the TAB key. It is useful when you are in a hurry or uncertain about a command. For example, if you type `add ip n` (TAB), it spells out the keyword `network` without losing your place in the command syntax.

Help

- Help is *general* or *positional*. Type `help <any command keyword>` to get a cursory list of commands and syntax. Type `<any command>` **?** to get more extensive, positional help for a particular field. Help is most useful *during* configuration: query the list of possible parameters by typing **?** and, when you find the value you need, type it without losing your place in the argument. Just leave a space between the keyword and the question mark.

Additional Conventions

- The type of value you enter must match the type requested. Numbers are either decimal or hexadecimal. Text can be either a string that you create, or it may be a list of options you must choose from. When choosing an option, type the text of the option exactly.
- “Double quotation marks” set off user-defined *strings*. If you want white space or special characters in a string, it must be enclosed by **“**double quotation marks.**”**
- Most commands are *not* case sensitive. As a rule, only <*name*> and *[password]* values require typing the correct case.

- Configuration changes are impermanent: they occur immediately but are lost on reboot unless you save them because the **save all** command places configuration changes in FLASH memory. These changes are lost by the SuperStack Remote Access System (RAS) 1500, if power fails before saving them.
- Some commands such as `add ip network` and `reconfigure` do ***not*** take effect immediately.
- Some *delete* commands require that you first *disable* the process or function. For example, before using the commands to delete a network user, interface, or network service, first disable the process or function.
- In most cases, wherever an *IP address* value is required, you can enter a host *name* provided you have configured a Domain Name System (DNS) server or put the name and address into the DNS Local Host Table.
- You can create a script file - a text file containing CLI commands - to simplify repetitive tasks. Use Trivial File Transfer Protocol (TFTP) to transfer the file to the FLASH file system, then use the `do` command to run the script file.

Network Address Formats

Many commands require a network address, to define a link to a remote host, workstation or network. Internet Protocol (IP) and Internet Packet Exchange (IPX) network addresses shown in this document use the syntax described in the following table. IP netmasks can be configured three ways: using the CLI mask signifier (A,B,C or H), using the standard format *(nnn.nnn.nnn.nnn)* or counting the one bits in a range from 8-30 (32 for a host). For help setting bitmasks, see Appendix C, “Addressing Schemes” for a bitmask table.

Address Type	Format	Range
IP_ address	a.b.c.d	0.0.0.0 to 255.255.255.255 (decimal). address 127.x.x.x is reserved for Loopback. address 247.x.x.x or higher is not part of a valid IP Network Class (A, B, C) address 0.0.0.0 is invalid in most contexts.
ip_net_ address	a.b.c.d/mask	255.255.255.255/A,B,C,H or *nnn.nnn.nnn.nnn* or 8-30 bits
ipx_net_ address	xxxxxxxx	hexadecimal

mac_ address	xx:xx:xx:xx:xx:xx	hexadecimal digit pairs
ipx_host address	xxxxxxxx.xx:xx:xx :xx:xx:xx	IPX network address.MAC (Ethernet) address

Interface Ranges

Interfaces can be expressed as variants of the ***x*/slot:*y*/mod:*z*** format, where *x* is the unit type (either *rm0* for the RAS 1500 base unit, *pau0* for the Primary rate Access Unit (PAU), or *pem0* or *pem1* for the RAS 1500 Expansion unit), *y* is the slot number (the PAU always uses **slot:1**), and *z* is a modem number.

You can specify more than one interface in the following way:

```
assign interface rm0/slot:1/mod:[1-x]
```

When connecting a PAU to a base unit, the STACKNET connector determines the number the PAU is assigned. For example, connecting the PAU via STACKNET connector to the base unit’s right most connector gives the PAU a 0 designation (*pau0*), middle connector (*pau1),* left connector (pau2).

If you remove a PAU (without deleting it from the software) and install another PAU, it will take on the designation 10 (for 0) 11 (for 1), and 12 for (2). The left digit continues to increment for every new PAU that is connected to that STACKNET connector.

Important: You cannot ***set*** *interfaces using ranges.* ***Set interface*** *and* ***set switched interface*** *commands require modem-by-modem configuration.*

Names

You can specify names for networks, users, and other system entities. Most names can be up to 64 ASCII characters, unless specified otherwise in the command description. A name can contain white space, or other non-alphanumeric characters, if you enclose the name with double quotes. Names are *case-sensitive.* Some examples are shown in the following table:

Desired name:	**Entered as:**
Larry’s PC	““Larry’s PC””
Server_number_3	Server_number_3

Users

A user entity is a table of parameters that are used when establishing a network connection. The `add user` and `set user` commands define the parameters of a user. The user commands are employed when making wide area network (WAN) (dial-in) connections and for dial-out users. Local users (stored in the User Table) are limited to 300 entries.

Default User

The *default user* is a powerful and efficient tool created at system setup that you can use to change many parameters of users you subsequently configure. It is designed to be utilized as a template for multiple user configuration.

For instance, if you want to configure *all* your users to be *type login, callback*, write:

```
set user default type login,callback
```

The parameters that can be configured across the board are indicated by a (D) when you type `list users`. Be aware that when you use this tool, you change the *default user* factory settings.

You can view the default user settings on your system by typing `show user default`. Remember that configuration changes on an *individual* user basis are done using the appropriate `set` commands.

Command Language Structure

The CLI command language creates, manages, displays, and removes system entities. These entities describe system and network connections and processes. Configured entities are stored in tables such as the IP Routing Table, for example. The following are some common entities:

- *Network* — defines local and remote networks, network connections, hosts, and routers.
- *User* — describes connection parameters, for operation and authorization.
- *Modem Group* — specifies switched interfaces to be managed as a group.
- *Filter* — can be applied to interfaces, connections, and users to control access through the system.
- *Interface* — describes physical devices; for example, ports.
- *Syslog Host* — receives system messages.
- *DNS Server* — translates IP addresses to and from host names.

- *Login Host* — made available for user connections.
- *Route* — describes a path through the network to another system/network.

Table entries are created with an `add` command and removed with a `delete` command. The `add` command specifies the most important parameters of the entry. Additional parameters are usually specified with the `set` command, which is also used to change configured parameters.

The `list` commands display table entries. For example, the command `list modem_groups` displays all defined modem groups.

`show` commands display detailed information about a specific table entry or a set of scalars (non-table items). For example, `show modem_group 3com` displays information on the 3Com modem group. `show all` commands display information. The `show all` commands display all parameters for *all entries* in tables associated with particular commands.

The order of items in a table is usually not relevant, nor is it inherent in the type of entity. Sometimes the order is relevant, and you must specify a *preference* value in the `add` command, indicating where this item belongs in the table. For example, `add dns server <server_name> preference 1` assigns a priority of 1 to this DNS server. The DNS server with the highest preference number is used first. Login hosts also require a preference number.

4 ROUTER COMMAND REFERENCE

This chapter contains the following information:

- Overview
- Add Commands
- Assign Command
- Bye Command
- Copy Command
- Delete Commands
- Dial/dialout Commands
- Disable Commands
- Disconnect Command
- Do Command
- Enable Commands
- Exit Command
- Hangup Commands
- Help Command
- Hide Command
- History Command
- Kill Command
- Leave Command
- List Commands
- Logout Command
- Monitor Commands
- Paused Commands
- Quit Command

- Reboot Command
- Reconfigure Command
- Rename Command
- Reset Commands
- Resolve Command
- RLOGIN Command
- Save Commands
- Set Commands
- Set User Commands
- Show Commands
- Telnet Commands
- Unassign Command
- Verify Command
- Dial-in User Commands
- Telnet Commands
- CLI Exit Commands
- Command Features

Overview

Command Language Structure

The command line interface (CLI) language creates, manages, displays, and removes system entities. These entities describe system and network connections and processes. Configured entities are stored in tables such as the Internet Protocol (IP) Routing Table. The following are some common entities:

- *Network* — Defines local and remote networks, network connections, hosts, and routers.
- *User* — Describes connection parameters for operation and authorization.
- *Modem Group* — Specifies switched interfaces to be managed as a group.
- *Filter* — Applies to interfaces, connections, and users for control access through the system.

- *Interface* — Describes physical devices, for example, ports.
- *Syslog Host* — Receives system messages.
- *DNS Server* — Translates IP addresses to and from host names.
- *Login Host* — Made available for user connections.
- *Route* — Describes a path through the network to another system/network.

Table entries are created with an `add` command and removed with a `delete` command. The `add` command specifies the most important parameters of the entry. Additional parameters are usually specified with the `set` command, which is also used to change configured parameters.

`list` commands display table entries. For example, `list modem_groups` displays all defined modem groups.

`show` commands display detailed information about a specific table entry or a set of scalars (nontable items). For example, `show modem_group 3com` displays information on the 3Com modem group.

The order of items in a table is usually not relevant, nor is it inherent in the type of entity. Sometimes the order is relevant, and you must specify a *preference* value in the ADD command, indicating where this item belongs in the table. For example, `add dns server <server_name> preference 1` assigns a priority of 1 to this Domain Name System (DNS) server. The DNS server with the highest preference number is used first. Login hosts also require a preference number.

Add Commands

Use the ADD command to define the following:

- Networks you connect to
- Hosts you need to access
- SNMP communities
- Users who dial out, dial in, access the network, or use the CLI

add address_pool user <user_name>

```
pool_name <name>
```

Assigns a user to a previously configured address pool. This command is associated with the `add ip pool` command. Also see the `enable ip address_pool_filtering` command.

add appletalk

```
network <network name>
zone
```

Defines an AppleTalk network and the zone(s) that are part of that network.

Parameter	Description
network <network name>	Unique designation you assign for the AppleTalk network that you want to configure. Limit: 32 ASCII characters. Maximum: 5 networks names.
zone <zone name>	Unique designation you assign for the AppleTalk zones that you want to add. A zone name describes the logical network segment on a physical network. The first zone on the list is the "default zone." Limit: 32 ASCII characters. Maximum: 5 zone names.

add bridge access_ mac_address

```
<mac_address>
```

Adds to the list of devices which are allowed to access bridge network(s). A bridge must have been previously defined, using `add bridge network`, for this command to take effect. Using this list, you can limit the access of a device to the bridge by not including the device MAC address in this list. You must also `enable bridge access_mac_address` for this bridge access limiting policy to take effect. Check current access status by using `show bridge settings`.

Parameter	Description
<mac_address>	MAC (Ethernet) address of workstation/host requiring bridge access. Use `arp` command to verify the MAC address for IP, `list ipx routes` for Internet Packet Exchange (IPX), or `list aarp` for AppleTalk.

add bridge network

```
enabled [no | yes]
interface <interface name>
user <username>
```

Defines a bridge network connection to allow your local area network (LAN) users to bridge to LANs across the wide area network (WAN). Bridging is supported over integrated services digital network (ISDN) and Frame Relay. Note that routing takes precedence over bridging, so that bridging does not occur unless you disable routing for the protocols you wish to bridge. The protocols to bridge and other important parameters are specified in the user you use to establish this connection. You must use `add user` to create a network type user for this command and `set network user` to specify the protocol and other parameters related to bridging.

Parameter	Description
enabled	Optional parameter that indicates whether data link Frame Relay is enabled (YES) or disabled (NO). Default is YES.
interface	The interface (port) to be bridged.
user	User to provide parameters needed to set WAN connection.

add datalink frame_relay

```
enabled [no | yes]
interface <interface>
```

Configures the serial WAN port (rm0/wan:1) on the SuperStack Remote Access System (RAS) 1500 for Frame Relay access. Frame relay allows several virtual connections through the one physical WAN port connection to the public network.

Your Internet Service Provider (ISP) must connect to a Frame Relay provider for this feature to be used.

Parameter	Description
datalink frame_relay	Protocol that provides frame/packet switched wide-area networking.
enabled	Optional parameter that indicates whether data link Frame Relay is enabled (YES) or disabled (NO). Default is YES.
interface	The port which data link frame_relay communicates over (rm0/wan:1).

add datalink ppp

```
enable [no | yes]
interface <interface_name>
user <user_name>
```

Configures the serial WAN port (rm0/wan:1) on the RAS 1500 for lease Point-to-Point Protocol (PPP) connection and associates a user profile with the WAN port.

Parameter	Description
datalink ppp	Protocol that allows for the transfer of leased PPP packets over a wide-area network synchronous serial line (leased line).
enabled	Optional parameter that indicates whether data link PPP is enabled (YES) or disabled (NO). Default is YES.
interface	The port which data link PPP communicates over (rm0/wan:1).
user	Username of the host on the on the private network connecting to the RAS 1500. Limit: 32 ASCII characters.

add dns server <IP_address>

```
preference <priority_rating>
name <server_name and domain_name>
```

Adds the IP address of a remote DNS server to the Domain Name Server Table. The preference number specifies the order DNS servers in this table are accessed, with 1 as the highest preference and 10 as the lowest. The first specified server is sent the IP Host Name to be resolved, first *with*, then *without* the default domain name (see `set dns domain_name` for more information about the default domain name). If that server cannot resolve the name, it is sent to the next specified server.

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

Parameter	Description
<IP_address>	IP address of a server in *nnn.nnn.nnn.nnn* format.
preference	Specifies the order in which name servers are used, with 1 as the highest priority. Range: 1-10.
name	Designation (optional) of the name server. Limit: 64 ASCII characters.

add filter <filter_name>

Adds a filter file name to the Filter Table. The Filter Table is a managed list of filter names used by Simple Network Management Protocol (SNMP). A filter file is a text file stored in the FLASH file system that you load from an external source using Trivial File Transfer Protocol (TFTP) or Web file load. `Add filter` also verifies the syntax of the filter file. If syntax verification fails, you receive an error message. The filter is added to the table, but it is not usable. You must correct the filter file in a text editor, use TFTP to export the updated file to the system FLASH file system, and use the `verify filter` command to check the filter syntax. You can view the filters using the `show filter` command and verify that the filter is correct by using the `show file` command.

Filter files are stored as ASCII files in FLASH memory.

Parameter	Description
<filter_name>	Designation of a filter file. Limit: **20 ASCII** characters.

add frame_relay pvc <pvc name> dlci <dlci number> interface user <username>

Configures a user profile for a permanent virtual connection.

For example, the command,

```
add frame_relay pvc chicago dlci 16 interface rm/0/wan:1 user
tom
```

associates the profile of the username “tom,” the data link connection identifier “16,” and the physical WAN port (interface) rm0/wan:1 to the permanent virtual connection “chicago.”

add framed_route user <name>

```
gateway [IP_address or name]
ip_route [IP_name or network_address]
{metric [number]}
```

Adds a framed (static) network to the user profile for dial-up connections. This method of creating a static route does not run Routing Information Protocol (RIP) to learn routes, so you must specify IP route and gateway addresses. For comparison, see `add ip route` command.

Parameter	Description
<username>	Username specified for the framed network. Limit: 64 ASCII characters.
gateway	IP address or name of the gateway used to reach this remote network.
ip_route	IP name or address of the remote network.
metric	Integer representing how far away the route is, in “hops” from other routers. Default: 1. Range: 1-15.

add init_script <script_name>

```
command <command_string>
```

Creates a modem initialization string, and adds it to the Init Script Table. Use `list init_scripts` to view current Init script Table entries. After you use the `set switched interface` command to assign an initialization script to a switched interface, that string is sent to the serial line driver whenever a connection terminates, to ready the modem for the next connection. You need not assign init scripts to modems. The maximum is **32** initialization scripts.

Parameter	Description
<script_name>	Designation of the init script. Limit: 7 ASCII characters.
command	Initialization string (AT commands). It must include **double quotes** and be less than **56 ASCII** characters. The CLI appends a **/R** and **/N** to it.

add ip defaultroute gateway <IP_address or name>

```
metric [hop count]
```

Allows a default route to be configured. The command adds a default route with a gateway on the IP network configured on the RAS 1500 LAN interface (rm0/eth:1). This allows a default route to be configured.

Parameter	Description
<IP_address >	IP address of the gateway router.
metric	An integer representing how far away the default router is, in hops through other routers. Range: 1-15. Default: 1.

add ip network <network_name>

```
address [IP_network_address]
frame [ethernet_ii | snap]
interface  [rm0/eth:1 | internal]
enabled [yes | no]
```

Adds an IP network to the list of IP networks available over the specified interface. When the system starts ups, the RAS 1500 can be configured to automatically create an IP network for default route and minimal SNMP settings.

Internal networks do not support SNAP encapsulation. Also, do not set the same internal IP address for more than one RAS 1500 on the same LAN. (see `set ip unnumbered_link local_address` *for more.)*

Parameter	Description
<network_name>	Name of IP network, consisting of up to **64 unique ASCII** characters. White space must be surrounded by double quotes.
address	IP address of the network, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The Mask Specifier can be A, B, C, or H, or a numeric value from 8 to 30 (32 for 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 for you from the network address.
frame	Frame encapsulation to be used on this IP network. Choices: **Ethernet_ii (Default) and snap**.
interface	Name of the interface which this IP network communicates over. **rm0/eth:1** is the LAN port available, while **internal** is a setting to define a global or "interfaceless" IP address for the RAS 1500 when supporting an ondemand or manual user with RIP over an *unnumbered* LAN-to-LAN connection. The default is the LAN interface (**rm0/eth:1**).
enabled	Optional parameter indicates whether the network is enabled (YES) or disabled (NO). Default: **YES**.

add ip pool <pool_name>

```
initial_pool_address <IP_network_address/subnet>
route [aggregate | no_aggregate]
size <1-4096>
state [public | private]
```

Assigns a specified number of contiguous IP addresses for allocation by the RAS 1500. When dial-in network users are dynamically assigned IP addresses, those IP addresses are allocated from a pool which has the advantage of bundling several IP addresses into one to limit RIP advertisements.

The pool is created as a range, starting from an initial address/subnet mask. As PPP or Serial Line Interface Protocol (SLIP) users dial in, IP allocates an address from this pool and assigns them to the user. IP addresses are automatically allocated on a *public* or *private* basis for users who are not assigned to a pool (public) or for those who are (private). Pools are also advertised as *aggregate* or *nonaggregate routes*. If an IP pool is configured as an *aggregate* address pool, the associated network route is added to the Routing Table immediately and advertised as a *unitary* network route. But if the address pool is defined as *no_aggregate*, individual host routes are added to the Routing Table, *only when a user is dialed in* to use that IP address pool.

The RAS 1500 automatically derives subnet masks for *aggregate* users but a mask can be configured for *no_aggregate* users.

Users assigned to more than one pool receive an address from the last assigned pool in round robin fashion. Also, if the administrator reduces the size of the pool, users whose associated address pool was deleted wont be denied access until after their calls have terminated.

Parameter	**Description**
<pool name>	Designation of the IP pool. Limit: **16 ASCII** characters.
route	Broadcasts the pool as a single network (aggregate) instead of individual host routes (no_aggregate). Default: **No_aggregate**.
initial_pool_address/subnet_mask	First IP network address to be assigned from the specified pool, in the format *nnn.nnn.nnn.nnn*, with or without a mask specifier. The Mask Specifier can be *A, B, C, H*, or a numeric value from *8* to *30* (*32* for host) that describes the number of one bits in the mask. If you do not specify a mask, the RAS 1500 generates the natural netmask from the *initial_pool_address*.
size	Number of allowable IP addresses. Class C values exceeding *x.x.x.*255 increments to *x.x.*1.1. Default: 1. Range: 1-4096.
state	Type of pool created. A *public* pool allocates IP addresses to any caller not assigned a pool. A *private* pool is limited to specified users. Default: **Public**.

add ip route <host_name or IP_network_address>

```
gateway [IP_name or gateway_address]
metric [hop_count]
```

Adds an IP route entry to the IP Routing Table. IP packets destined for networks that match this network are routed to this address. The command `list ip routes` displays all currently defined routes including the static route you create with this command but only if you have specified a *gateway*. Also see the `add ip default route` command.

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

Parameter	Description
<network_ address>	IP address or host name of the remote destination, in the format nnn.nnn.nnn.nnn, entered *with* or *without* a mask specifier. The mask specifier can be A, B, C, or H (host), or 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 self-generates it (based on the network address) for all routes (*ip network address*) except *host* routes, for which you *must* specify a mask. For help counting bits, see *Appendix C: Address Schemes* for a bitmask table.
gateway	IP name or address of gateway used to reach this remote network.
metric	An integer for how distant the route is, in "hops", from the destination to the RAS 1500. Default: 1. Range: 1-15.

add ip udp_bcast_forwarding_port

```
add ip udp_bcast_forwarding_port <port>
```

Identifies the source port number from which User Datagram Protocol (UDP) packets on the private network are forwarded by the RAS 1500. You may use the `list ip udp_bcast_forwarding_port` command to display ports on the private network configured for UDP packet forwarding.

Parameter	Description
<port>	Source port number that used when a user application broadcasts UDP packets. A separate port is used for every application from the host.

add ipx network <network_name>

```
address [ipx_network_address]
interface [rm0/eth:1]
enabled [yes | no]
frame [ethernet_ii | snap | dsap | novell_8023]
```

Adds an IPX network to the list of IPX networks available over the specified interface.

Parameter	Description
<network_name>	Name of IPX network. Unique ASCII string of up to **64** characters.
address	Address of the IPX network.
interface	Name of interface with which this IPX network associates. The default is the first LAN interface (**rm0/eth:1**).
enabled	Optional parameter indicates whether the network is enabled (YES) or disabled (NO). Default: **YES**.
frame	Frame encapsulation to be used on this IPX network. Choices: ■ **Ethernet_II** - contain Type in place of length fields. **Default**. ■ **SNAP** (Ethernet_SNAP) - Sub-Network Access Protocol derived from 802.2. ■ **DSAP** (802.2) - default frame type for NetWare v4.*x.* ■ **Novell_8023** (802.3 raw) - default frame type for NetWare v2.*x* and v3.*x* networks.

add ipx route <ipx_network_ address>

```
gateway [ipx_host_address]
metric [1-15]
ticks [tick_number]
```

Adds an IPX static route to the system IPX Route Table, which defines static routes to remote IPX networks. The command `list ipx routes` displays currently defined static routes.

Parameter	Description
<ipx_net_address>	IPX network address requiring a route.
gateway	IPX address of the host that acts as a gateway. The format is nnnn.xx:xx:xx:xx:xx:xx (network_address.mac_address).
metric	Number of hops through different routers to reach the remote IPX network. Range: 1-15.
ticks	Estimated interval in ticks it takes to deliver a packet to the remote network. There are approximately 18 ticks per second.

add ipx service <service_name>

```
address [internal network address]
gateway [network_number.mac_address]
metric [1-15]
node [internal_node_number]
socket [socket_number]
type [service_type]
```

Adds a static IPX service to the IPX Services Table. You must supply the name, internal ipx network number, node number, socket, and type of service for this service. The user must also supply gateway information to indicate the next router hop. To remove this service, use the `delete ipx service` command. See the `show IPX settings` command for more information.

Parameter	Description
<service name>	Designation of IPX service. Limit: **32** ASCII characters.
address	Internal network number for the IPX service on which this service resides.
gateway	Host address of the router you defined as the gateway.
metric	Integer representing how far away the default router is, in hops through other routers. Range: 1-15.
node	The internal node number (MAC address) of the server on which the service resides. Typically: *00:00:00:00:00:01*.
socket	The port the server listens on. Socket numbers are the joined sender (or receiver) IPX address and service type port number.
type	Type of service: hexadecimal number referring to file server, print server, etc. Refer to the table below.

The following is a list of IPX services available:

Type	Description
04	file server
05	job server
07	print server
09	archive server
0A	job queue
21	NAS SNA gateway
2E	dynamic SAP
47	advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES-NetWare VMS
98	NetWare access server
9A	Named Pipes server
9E	PortableNetWare-UNIX
107	NetWare 386
111	Test server
166	NetWare management
26A	NetWare management
26B	Time synchronization
278	NetWare Directory server

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]
```

Adds up to *ten* login hosts to the Login Host Table. You add login hosts so users of type *login* connecting to an IP host can reference the host by name. The system looks up the address, using the DNS server you define with the `add DNS server` command. Or, you can specify the IP address here. Display the currently defined login hosts with the `list login_hosts` command.

Parameter	Description
<host_name>	Name or IP address that specifies an IP host. Limit: **64 ASCII** characters.
address	*Optional*. address of login host. If you do not specify an address here, the system consults the DNS server to find the address.
preference	Priority of the Login Host. Each host can be assigned a unique preference number for selection by the server. The first preference is 1, the least preference, 10. Range: 1-10.
rlogin_port	*Optional*. Specifies the port number that is used when a user executes the rlogin CLI command, specifying this host. Maximum: 65535. Default: 513.
telnet_port	*Optional*. Specifies the port number that is used when a user executes the telnet CLI command, specifying this host. Maximum: 65535. Default: 23.
clearTCP_port	*Optional.* Specifies the port number that is used when a user application requests a ClearTCP session with this host. Maximum: 65535. Default: 6000.

add modem_group <group_name>

```
interfaces [interface name]
```

Creates a group of interfaces. See also the `set modem_group` command, which configures all interfaces in the modem group. You can also add additional interfaces to this modem group using `assign interface` and remove them with `unassign interfaces`. The default modem group, *all*, contains all installed modems in the RAS 1500 and RAS 1500 Expansion Units. Use the `list modem_groups` command to view a list of modem groups. Use the `show modem_group` to view a list of interfaces assigned to a specific modem group.

Modem groups are a shorthand notation for a list of interfaces. They do not hold interface configuration settings.

The default modem group, "all," cannot be modified.

Parameter	Description
<group_name >	Name of the modem group. Limit the length of this name to eight characters to ensure the name always displays completely in certain list and show commands. Limit: **64 ASCII** characters. Limit: **500 modem groups**.
interfaces	List of interfaces to be assigned to the modem group. The following is the list format: <interface 1>,<interface 2>,... The following is the format of each interface: *x*/slot:*y*/mod:*z* where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number. Example: rm0/slot:1/mod:1,pem0/slot:1/mod:2 Enter interfaces from the same slot in ranges, for example, rm0/slot:1/mod:[1-4],pem0/slot:1/mod:[1-4]

Example:

```
add modem_group dialout interfaces
rm0/slot:1/mod:[1-4],pem0/slot:1/mod:1
```

add nat dynamic user <user_name>

```
count <number of addresses>
public_pool_start<ip_address>
```

Configures, and associates a name with, a specific number of ISP-assigned addresses for Dynamic Network Address Translation (NAT) by the RAS 1500.

Example:

```
add nat dynamic user natd count 4 public_pool_start 2.2.2.2
```

sets (the count of) **"4"** consecutive ISP-assigned addresses beginning with the ISP-assigned address **"2.2.2.2"** to use for Dynamic NAT. In this case, the range includes the ISP-assigned addresses, "2.2.2.2", "2.2.2.3", "2.2.2.4", and "2.2.2.5". **"natd"** represents the name that is assigned for the connection for this configured range.

Each time a user connects to the public network, Dynamic NAT translates the IP address from that user on the private network and maps it to the first available public IP address from the contiguous range of ISP-assigned addresses that you configured by using this command. The RAS 1500 maintains a table of active IP addresses on the public network mapped to user IP addresses on the private network for the connection. Once the connection to the public network is closed, the information in the table is dropped and this IP address is free for the next connection. Each time a user connects to the public network, the next available address from the contiguous range is assigned, and a new table of mapped addresses is established by the RAS 1500.

Note: *NAT can only be used when the ISP has provided more than one IP address. The first and last in the contiguous range of ISP-assigned addresses are "broadcast" addresses and are not available for NAT. The second address in the contiguous range is reserved for the RAS 1500 and also is not available for NAT."*

Parameter	**Description**
<user_ name>	Unique name that you want to assign the connection that uses Dynamic NAT to map ISP-assigned addresses to connections on the private network. Limit: **32** ASCII characters.
count	Total number of ISP-assigned addresses starting with the public_pool_start address that is used by the RAS 1500 for Dynamic NAT mapping.
public_pool_start	The first of the contiguous range of IP addresses assigned by Dynamic NAT mapping.

add nat static user <user_name>

```
private_address <ip_address>
public_address <ip_address>
```

Configures, and associates a name to, a mapping between and IP address on the private network to a specific ISP-assigned address on the public network that uses Static NAT.

Example:

```
add nat static user nats private address 1.1.1.1 public
address 2.2.2.2
```

statically assigns the private address 1.1.1.1 to the ISP-assigned addresses address **"2.2.2.2"** to for Static NAT and names this mapping that uses Static NAT, **"nats"**. In this case, 1.1.1.1 **always** connects to 2.2.2.2. In this example, **"nats"** is the name given to the mapping between the IP address on the private network and ISP-assigned address on the public network configured for this Static NAT.

Each time the IP address on the private network, "1.1.1.1" connects to the public network, Static NAT translates the IP address and connects it to the static assigned addresses, "2.2.2.2". The RAS 1500 maintains a table of active mappings between IP addresses on the private network mapped to statically assigned IP addresses on the public network.

Both Dynamic and Static NAT can be used simultaneously, ***however*** *individual users connecting to the public network must be configured for* ***either*** *dynamic or static NAT. In addition, the IP addresses of users configured for either NAT type, must be* ***consecutive*** *addresses at the* ***beginning*** *or* ***end*** *of the series of addresses in the subnet on the private network.*

Parameter	**Description**
<user_ name>	Unique name that you want to assign the connection that uses Static NAT to map a specific ISP-assigned address to a specific address on the private network.
private_address	The network address of the host on the private network that is designated a specific, static public IP address. This address is always used when connecting to the public network.
public_address	The public network IP address from the contiguous range assigned by the ISP, that is reserved for, and always maps to, the IP address on the private network configured for Static NAT.

add network service <service_name>

```
close_active_connections [true | false]
data [ancillary data options]
enabled [yes | no]
server_type [ClearTCPD | DialOut | SNMPD | TELNETD | TFTPD]
socket [socket_number]
```

This configures a network listener process that provides certain services, including modem sharing, TFTP file access, and SNMP, Telnet, and ClearTCP support. For more information on configuring dial-out service, refer to the System Management Guide. To view the available server types, use the `list available servers` command.

Parameter	**Description**
<service_name>	Name of this type of service. Limit: **64 ASCII** characters.
close_active_ connections	Indicates whether to close any active connections when a service is disabled by the **disable network_service** command. Default: **False**.
data	Ancillary Data. This field contains server-specific configuration data. See table below for configurable ancillary data parameters for Telnet.
enabled	*Optional*. Indicates whether the network is enabled (**YES**) or disabled (**NO**). When you add a network service, it is *enabled* by default.
server_type	Designates the type of service being offered. Services currently available are the following: ■ *ClearTCPD* — daemon enables access to a modem group. Uses Transmission Control Protocol (TCP). ■ *DialOut* — supports dial-out connections to IP or IPX hosts. Uses TCP. ■ *SNMPD* — daemon supports SNMP. Uses UDP. ■ *TFTPD* — daemon supports file transfer service. Uses UDP. ■ *TELNETD* — daemon supports Telnet, either to the CLI or a modem group. Uses TCP.
socket	Port the server listens on. For TFTP, TELNET, and CLEARTCP, it is the TCP or UDP port number. Socket numbers are the joined sender (or receiver) IP address and service type port number. Maximum: 65535. Range: 0-65535.

The next table shows configurable parameters for network service, which are specified with the *data* value.

Ancillary Data Parameter	**Description**
auth	On indicates that login/password authentication should be performed on incoming connections. **Feature not supported for DialOut service and/or DialOut IP.** Format: **auth= [on | off]**. Default: **on**.
drop_on_hangup	Value specifying whether the TCP session is dropped after modem hangs up. *Off* allows connection to remain active. **Feature not supported for DialOut service.** Default: **off**.
login_banner	ASCII string sent to a client when connection is made. It must be quoted and offset by backslashes if spaces are included in the string. Specify carriage return after login banner with **login_banner=string\r\n\. Feature not supported for DialOut service.** Format: **login_banner=string**. Default: **non**.
login_prompt	ASCII string specifying the login prompt sent during authentication. It must be quoted and offset by backslashes if spaces are included in the string. **Feature not supported for DialOut service.** Specify carriage return after login banner with **login_banner=string\r\n\**. Format: **login_prompt=string**. Default: **login**:
modem_group	ASCII string specifying the name of a modem group for whose modems network service is supplied. **This value must be specified when using DialOut service**.
service_type	Indicates whether the service offered is modem sharing or manage. ▪ *Modem sharing* service connects a client to *multiple* modems. ▪ *Manage* service connects a client to the *command line*, to manage the system. Applicable only to Telnet servers; you cannot use ClearTCP to access the system for management. Format: **service_type=manage, dialout**. Default: **manage**.

`Add network service` examples:

To configure a ClearTCP service (not authenticating upon connect) to offer modem sharing on TCP port 6000 using the first modem in the second slot in the RAS 1500, enter the following:

```
add modem_group “hi boston” interface rm0/slot:2/mod:1
add network service modem_sharing server_type cleartcpd
socket 6000 data auth=off,service_type=dialout, modem_group=“hi
boston”
```

*Enclose DATA values including **spaces** with double quotes, for example, data modem_group=”Hi Boston”.*

Do not create more than one DialOut service with the same name on a network.

To configure a Telnet service to offer CLI access on port 6666, doing authentication upon connect (default) and dropping the connection on hangup, enter the following:

```
add network service CLI_access server_type telnetd socket
6666 data drop_on_hangup=on
```

To configure a DialOut service using the modem group LA, enter the following:

```
add network service “Call_LA” server_type dialout data
modem_group=”LA”
```

add pat tcp user <user_name>

```
PRIVATE_ADDRESS <ip_address>
PRIVATE_PORT <number>
PUBLIC_PORT <number>
```

Sets a static address mapping translation for a connection using TCP Port Address Translation (PAT) and associates a username with that connection. TCP PAT translates TCP port numbers and user IP addresses on the private network and maps these addresses to a single ISP-assigned address.

***Note:** PAT can only be used when the ISP has provided only one IP address. This one IP address can change with each connection.*

Parameter	Description
<user_ name>	Unique name you assign to the connection that you want to configure for static TCP PAT. Limit: **32** ASCII characters.
private_address	The source IP address of the user on the private network.
private_port	The source port number on the private network from which TCP packets are transferred.
public_port	The destination port number of the ISP-assigned IP address on the public network.

add pat udp user <user_name>

```
PRIVATE_ADDRESS <ip_address>
PRIVATE_PORT <number>
PUBLIC_PORT <number>
```

Sets a static address mapping translation for a connection using UDP PAT and associates a username with that connection. UDP PAT translates UDP port numbers and user addresses on the private network and maps these addresses to a single ISP-assigned address by changing the source IP port number and IP address.

Parameter	Description
<user_ name>	Unique name you assign to the connection that you want to configure for static UDP PAT. Limit: **32** ASCII characters.
private_address	The source IP address of the user on the private network.
private_port	The source port number on the private network from which UDP packets are transferred.
public_port	The destination port number of the ISP-assigned IP address on the public network.
public_port	The port number of the single ISP-assigned IP address on the public network.

add snmp community <community_name>

```
address [IP_address]
access [ro | rw | adm]
```

Adds to a table of SNMP-authorized users. If you don't want to restrict SNMP access to a particular IP address, specify the address as “0.0.0.0” (public). The community name and IP address of SNMP requests from managers on the network must match the list, which you can see using `list snmp communities`. Also, multiple management stations can manage the RAS 1500 using the same SNMP community name by use of the SNMP Community Address Pool table, which associates a community name with IP addresses.

Parameter	Description
<community_name>	Group name that authorizes SNMP requests.
address	IP address of the remote SNMP manager, in the form: *nnn.nnn.nnn.nnn*
access	Determines what type of access to SNMP MIBs the specified user has. Options: *Read Only (RO)* — User-level objects. *Read Write (RW)* — User-level objects. *Administrator (ADM)* — Administrator allows *read access to all objects* and *write access to all writeable objects*. **RO** is the default on public (0.0.0.0) networks, and **RW is** the default on private networks.

add syslog <IP_name or address>

```
facility [log_auth | log_local0 | log_local1 | log_local2
|log_local3 | log_local4 | log_local5 | log_local6 |
log_local7]
loglevel [critical | unusual | common | verbose]
```

Adds an IP host to the list of IP hosts that receive SYSLOG entries. You can see the current log levels for the system using `list facilities. You can` modify the current loglevel for each facility using `set facility loglevel`.

All SYSLOG messages generated by the Auth *facility are sent regardless of loglevel set. To modify this function, disable the* allow_all_auth_levels *parameter.* All other *RAS 1500 facilities are sent only if their loglevels match the configured syslog loglevel.*

Parameter	**Description**
<ip_name_or_address>	Host name or IP address of the UNIX host that receives SYSLOG information.
facility	The SYSLOG node facility (site) where SYSLOG messages are sent. See choices above. Default: *log_auth*.
loglevel	There are four levels of logging: ■ *CRITICAL* — a serious system error, which may affect system integrity. *Default*. ■ *UNUSUAL* — an abnormal event, which the system should be able to recover from. ■ *COMMON* — a regularly occurring event. ■ *VERBOSE* — a regular periodic event, for example, a routing update message.

add tftp client <IP_name_or_address>

Adds the *tftp client* to the Authorization Table for TFTP access.

Parameter	**Description**
<ip_ name_or_address>	Host name or IP address of a host to be added. An address of 0.0.0.0 allows all clients TFTP access.

add user <user_name>

```
enabled [yes | no]
login_service [cleartcp | ping | rlogin | telnet]
network_service [arap | fcp |frp_1490 | ppp | slip]
password <password>
type [callback, dial_out, login, manage, network,
clid_callback]
```

Adds a user to the Local User Table. You may specify a type for the user, as well as login and network protocols, or you may use the defaults. The `list users` command displays these parameters for all users. See the `show users` command for more information on individual users.

Administrators creating Remote Authentication Dial-In User Service (RADIUS) users should consult Appendix E: Radius Authentication for more information.

Parameter	Description
<user_name>	Name of user to be added, up to **32** ASCII characters. Limit: No more than **200** local users.
enabled	*Optional*. Indicates whether the user is enabled (**YES**) or disabled (**NO**) by this command.
login_service	■ Protocol to be used for a login user. Options: ■ RLOGIN. ■ Telnet (*default*). ■ ClearTCP. ■ Ping — User pings a login host, receives a successful/unsuccessful message and is disconnected.
network_service	Framed protocol to be used by network user. Options: ■ PPP — Point to Point Protocol (*default*). ■ SLIP — Serial Line IP. SLIP is not supported currently for LAN-to-LAN users.
password	User password (optional). Limit: **127** ASCII characters. You can create a null password with *password "".*
type	Type of user - may be one or more types. ■ *Call-back* users are disconnected after authentication and called back. ■ *Dial-out* — modem sharing or WAN users. ■ *Login* uses the login_service specified. ■ *Manage* users have administrative authority. ■ *Network* (*default*) uses network_service specified - a dial in user. ■ *CLID_Callback* — identifies and calls back the user based on the user Automatic Number Identification (ANI).

Arp Command

arp <ip_host_name_or _address>

Learns the IP address (and Media Access Control address — Ethernet address — if on a locally connected network) of a network node via the Address Resolution Protocol (ARP). If the node is not in the ARP cache, an ARP request is sent out.

For example, at the prompt, enter the following:

```
ras1500>>  arp houston
```

The RAS 1500 generates the following output:

```
ras1500>>  ARP: 156.155.132.145 -> 08:00:20:80:43:85
```

Assign Command

assign interfaces <interface names>

`modem_group <group_name>`

Adds interfaces to an existing modem group or modem groups. Use the `show_modem group` command to view a list of interfaces assigned to a specific modem group. Use the `add modem_group` command to add modem groups. Use the `list modem_groups` command to view a list of modem groups.

Parameter	Description
interface name	List of interfaces to be assigned to the modem group. The format of the list is the following: <interface 1>,<interface 2>,... The format of each interface is the following: *x*/slot:*y*/mod:*z* where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Port Expansion Unit; or pau0 for the RAS 1500 Primary Access Unit [PAU]), *y* is the slot number, and *z* is the modem number. Example: rm0/slot:1/mod:1,pem0/slot:1/mod:2 Enter interfaces from the same slot in ranges. Example: rm0/slot:1/mod:[1-4],pem0/slot:1/mod:[1-4] This command cannot exceed **64** ASCII characters.
modem_group	Name of the modem group.

Example:

```
assign interface pem0/slot:1/mod:[1-4] modem_group dialout
```

Bye Command

bye Exit the CLI, but keep this connection open. This command returns you to the Dial-In User or Telnet commands.

Copy Command

copy file <input_file> <output_file> Copies a file within the FLASH file system. This is a flat file system.

Delete Commands

Delete commands remove anything you previously added.

delete address_pool user <name> `pool_name <name>`

Removes a user previously assigned to the specified address pool with the `add address_pool user` command.

delete appletalk network <network name> Deletes the AppleTalk network that you previously added using the `add appletalk network` command. Make sure you disable the network using `disable appletalk network` before deleting it. Use `list appletalk networks` to view added networks.

delete appletalk zone <zone name> Deletes an AppleTalk zone from an AppleTalk network. Make sure you disable the network using `disable appletalk network` before deleting the specified zone. Use `list appletalk zones` or `show appletalk network` to verify the zone that is not in use.

delete bridge access_mac_address <mac_address> Deletes a LAN user access to the bridge connection across the WAN. Use `list bridge access_mac_addresses` to view which addresses are available to delete.

delete bridge network <network name> Deletes the bridge network that you previously added using `add bridge network`. Make sure you have disabled the bridge network, using the `disable bridge network` command, before trying to delete it. Use `list bridge forwarding` to see if there is any activity over the bridge connection.

delete configuration

Removes all your configuration files, reboots the system, and restores system configuration to default values. For your protection, you are prompted to confirm the request.

delete datalink frame_relay

Deletes the configuration of the serial WAN port (rm0/wan:1) on the RAS 1500 that you previously configured for Frame Relay access using the `add datalink frame_relay` command.

delete datalink PPP

Deletes the configuration of the serial WAN port (rm0/wan:1) on the RAS 1500 that you previously configured for lease PPP using the `add datalink PPP` command.

delete dns cache <number>

Removes an entry from the DNS Cache Table. Range: 0 - 65535

delete dns host <host_name>

Deletes the specified host from the DNS Local Host Table. Use `list DNS hosts` to view the DNS Local Host Table. After deletion, requests for that host are processed through a DNS server, instead of locally. Use `list DNS servers` to see which servers are defined.

delete dns ncache <number>

Removes the specified entry from the DNS Negative Cache Table. Range: 0 - 65535

delete dns server preference <preference_ number>

Removes the name server associated with that preference number (preferred rank: 1 [first] -10 [least]) from the table of accessible DNS servers.

delete file <file_name>

Deletes a file from the FLASH file system. Use the `list files` command to see which files are currently stored.

delete filter <filter_name>

Removes the named filter from the Filter Table and deletes the file stored in FLASH memory. Use `list filters` to see filter files stored in FLASH memory.

delete framed_route user <username>

```
ip_route <IP_name or address>
```

Deletes the framed route user you created with the `add frame_route user` command.

delete init_script <script_name>

Removes a modem initialization string from the Init_script Table. Use `list init_scripts` to see which modem initialization scripts you have added.

delete ip defaultroute <IP_address or name>

Deletes the IP default route created with the `add ip defaultroute` **gateway** command. Use the `list ip routes` command to verify edit.

delete ip network <network_name>

Deletes an IP network from the interface that you specified when *adding* the network. Use `list ip networks` to see which networks are associated with which interfaces. Always use `disable ip network` before deleting it.

delete ip pool <pool name>

Deletes an IP pool created with the `add ip pool` command. Use the `list ip pools` command to verify edit.

This command takes effect only after all addresses have been released from the pool. Also, when a IP pool is deleted, be sure to also delete the pool from any associated user profile.

delete ip route <network_name or IP_address/subnet_mask>

`all_learned_routes`

Deletes the specified static/learned IP address or all learned routes (including RIPv1/RIPv2 routes) from the IP Routing Table. The subnet mask value, which is optional, takes the form of A, B, C, and H, or a numeric value from 8 to 32. It also accepts dot format, in which case the value must be 255.0.0.0 or greater and contiguous. Deleting routes causes IP packets destined for those networks to use the default route, which can be viewed using the `list ip routes` command. See `add ip defaultroute gateway` and `add ip route` commands for more information.

delete ip udp_bcast_forwarding_port <port>

Deletes the port number on the private network that identifies the source port from which the UDP packets are being forwarded. Use the `add ip` udp_bcast_forwarding_port command to add the port number on the private network from which UDP packets are forwarded.

Parameter	Description
udp_bcast_forwarding_ port	Port number specified in the IP address of the user on the private network that broadcasts UDP packets. A separate port is used for every application on the user station.

delete ipx network <network_name>

Deletes an IPX network on the interface you specified with the `add ipx network` command. You can `list ipx networks` to see which are available and their status. Use the `disable ipx network` command before deleting the network.

delete ipx route <ipx_network_ address>

`all`

Deletes a specified route or *all* IPX and learned (RIPv1/v2) routes on the interface you created with the `add ipx route` command. The `list ipx routes` command displays the current IPX routes.

delete ipx service <service_name>

`type [service_type]`

Deletes static or learned IPX routes configured with the `add ipx service` command. This command works only if a complete match on all parameters is found.

Parameter	Description
<service name>	Designation of IPX service. Limit: **32** ASCII characters.
type	Type of service: file/server, print, etc., expressed in hexadecimal format (*xxxxxx*).

delete login_host preference <preference_ number>

Removes the login host with the specified preference (priority: 1 [first] -10 [least]) number. See `add login_host <name> preference` command for more information. Use `list login_hosts` to see the login hosts you added and their associated preference numbers.

delete modem_group <group_name>

Removes a modem group from the Modem Group Table. Use the `list modem_groups` command to view a list of modem groups. Use the `show modem_group` to view a list of interfaces assigned to a specific modem group.

The default modem group, all, cannot be modified or deleted.

delete nat dynamic user <user_name>

Deletes the configuration you established for Dynamic NAT through the `add nat dynamic user <username>` command.

delete nat static user <user_name>

Deletes the configuration you established for Static NAT through the `add nat static user <username>` command.

delete network service <service_name>

Deletes the specified network service from the list of available services. You must use `disable network service` before deleting the service. You can see which services are available and active using the `list available servers` and `list network services` commands.

delete pat tcp user <user_name>

```
PUBLIC_PORT <number>
```

Deletes the user on the private network that you previously configured for static TCP PAT through the `add pat tcp user <username>` command.

Parameter	Description
<user_ name>	Username of the host on the private network that use PAT to connect to the public network and transfer TCP packets. Limit: **32** ASCII characters.
public_port	The destination port number of the ISP-assigned IP address on the public network.

delete pat udp user <user_name>

```
PUBLIC_PORT <number>
```

Deletes the user on the private network that you previously configured for static UDP PAT through the `add pat udp user <username>` command.

Parameter	Description
<user_ name>	Username of the host on the private network that uses PAT to connect to the public network and transfer UDP packets. Limit: **32** ASCII characters.
public_port	The destination port number of the ISP-assigned IP address on the public network.

delete snmp community <name>

Removes an SNMP community that was previously added with the `add snmp community` command. You can use `list snmp communities` to see the current entries.

delete syslog <IP_name_or_ address> Removes the specified IP host name or address from the list of addresses that are authorized to receive SYSLOG information. Use `list syslog` to see the currently allowed addresses.

delete tftp client <IP_name or address> Removes the specified IP host name or IP address from the list of addresses authorized to TFTP. Use `list tftp clients` to see the currently allowed addresses.

delete user <name> Deletes a user you previously added to the Local User Table. Use `list users` to see the currently defined user. Use `show user` to see the attributes you assigned to that user using the add user or set user command.

Dial/dialout Commands

dial <user_name> Generates an outgoing call to the location specified by the username. You can use the `list users` command to list the defined users, the services they are defined to work with, and their current status. Limit: **64** ASCII characters.

Disable Commands

Disable commands inactivate a host of processes previously enabled.

disable accounting Disables remote accounting via RADIUS. You can use `show accounting` to see if it is currently running and enable accounting to start accounting.

disable appletalk network <network name> Disables the specified AppleTalk network. A disabled network remains in the network table, but cannot receive or send data. Use `list appletalk networks` to see the currently defined AppleTalk networks and their status.

disable authentication [local | remote] Disallows the following types of authentication:

- *Local* — *User* authentication based on a password specified in the User Table. Local authentication is *enabled* globally by default.

Local authentication takes precedence over remote authentication.

- *Remote* — authentication based on a password stored in a *RADIUS or TACACS+* server.

Issue the `show authentication` command to display settings.

Use the `show critical_event settings` command to view logging configuration and event sinks.

disable dns host_rotation

Disables the RAS 1500 process of randomly choosing a primary IP address and up to eight alternates from the DNS cache.

disable icmp logging

Disables display of the Internet Control Message Protocol (ICMP) to the SYSLOG server. Use the `show icmp` command to view edits.

disable icmp router_advertise

Disables the RAS 1500-generated router advertisements multicast on the same LAN segment as the RAS 1500. Use the `show icmp` command to view edits.

disable interface <interface name>

Disables a specified interface. If a call is active on the interface, it is disconnected. A disabled interface remains in the Interface Table, but does not transmit or receive any data. Use the `list interfaces` command to see the currently defined interfaces and their status.

You can disable multiple interfaces in one command. The following is the list format:

```
disable interface <interface 1>,<interface 2>,...
```

The following is the format of each interface:

x/slot:*y*/mod:*z*

where *x* is the type of unit (rm0 for the RAS 1500 unit, pem0 or pem1 for the RAS 1500 Port Expansion Unit, or pau0 for the RAS 1500 PAU), *y* is the slot number, and *z* is the modem number.

Example:

rm0/slot:1/mod:1,pem0/slot:1/mod:2

Enter interfaces from the same slot in ranges.

Example:

rm0/slot:1/mod:[1-4],pem0/slot:1/mod:[1-4]

Example:

```
disable interface rm0/slot:1/mod:[1-4],pem0/slot:1/mod:1
```

disable ip address_pool_filtering Disables packet filtering on all Internet Protocol (IP) address pools (drops packets for IP addresses within IP pools *not in use).* Use the `show ip settings` command to view edits.

disable ip forwarding Causes the system to stop forwarding any packets over IP networks but the RAS 1500 still operates as a client. Under most circumstances, you never disable forwarding. You may want to disable ip forwarding if you are using the system only as a terminal server since users who Telnet to the system can still connect to remote hosts. Use the `show ip settings` command to view edits.

disable ip network <network_name> Disables the specified IP network. Make sure there is no activity on this network before disabling it.

disable ip rip Disables the RIP routing algorithm on all IP networks. You can use `show ip routing` to see the current status of IP routing. This saves system space by preventing a large RIP database, which is useful for networks connecting over the WAN interface.

disable ip routing Disables all routing protocols on all IP networks. Currently, the only routing protocol is RIP, which means that `disable ip rip` performs the same function. You can use the `show ip routing` command to see the current status of IP routing.

disable ip static_remote_routes Disables all statically defined remote routes on all IP networks, that you previously defined using the `add ip route` command. You can list the current IP routes using the `list ip routes` command.

disable ip udp_broadcast_forwarding Disables the UDP broadcast forwarding feature stopping the RAS 1500 from forwarding UDP broadcast packets. You can use the `enable ip udp_broadcast_forwarding` command to enable the RAS 1500 to forward packets.

disable ipx network <network_name>

Disables the specified IPX network. Use `list ipx networks` to see which IPX networks are defined and their current status.

disable ipx rip network <network_name>

Disables the RIP routing protocol on the specified IPX network. This saves system space by barring a large RIP database from growing, which is useful for networks connecting over the WAN interface. Use the `enable ipx rip network` command to restart RIP on this IPX network.

disable ipx sap network <network_name>

Disables the Service Advertising Protocol (SAP) on the specified network. This saves system space by barring a large SAP database from growing, which is useful for networks connecting over the WAN interface. Use the `enable ipx sap network` command to restart SAP on this IPX network.

disable modem_group <name>

Disables the modem group you enabled with the `enable modem_group` command. The default modem group, *all*, includes all installed modems in the stack. Use the `show modem_group` command to view INACTIVE status of disabled modem groups.

disable network service <service_name>

Disables a network service, such as Telnet or TFTP. If *close_active_connection* was specified as TRUE in the `add network_service` command, all active connections are closed when the service is disabled.

disable security_option remote_user_ administration [dialin | telnet]

Disables CLI access by remote Telnet and dial-in users. All CLI configuration must be done from the console port. You can use `enable security_option remote_user administration` to re-enable remote CLI access.

disable security_option snmp user_access

Disables SNMP access to the system. This prevents remote users from using SNMP and damaging the configuration. You can use `enable security_option snmp user_access` to re-enable full SNMP access.

disable telnet

```
escape
```

Prevents various Telnet client services. Use the **show telnet** command to view settings.

Parameter	Description
escape	All Telnet clients are prevented from using the escape character during a session.

disable user <user_name>

Disables the specified user from being used. This affects dial-in users and WAN connections that depend on that user for parameters. It also causes all active sessions established using that particular user to terminate and does not allow any new sessions to occur using that username. Disabling a user is useful when prohibiting a user access temporarily. Use `list users` and `show user` commands to view edits.

Disconnect Command

disconnect user <name>

Brings down the specified user connection.

Do Command

do <command_ inputfile> output <outputfile>

Runs a script file, stored in FLASH memory, which contains a series of CLI commands. The output parameter is optional.

Enable Commands

enable accounting

Enables remote accounting via RADIUS or TACACS+. Use the `disable accounting` command to halt accounting via RADIUS. Use the `show accounting` command to view edits.

enable authentication local | remote

Permits the following types of authentication:

- *Local* — User authentication based on a password specified in the User Table. Local authentication is enabled globally by default.

Local authentication takes precedence over remote authentication.

- *Remote* — Authentication based on a password specified in a RADIUS or TACACS+ server.

Issue the `show authentication` command to display current settings.

enable bridge access_mac_address

Enables the specified MAC address to use the bridged network connection. You must have previously run `add bridge access_mac_address` before using this command. If a MAC address is not in this table, that station is **not** be able to bridge across the WAN. When bridge access_mac_address is disabled, any user can use the bridge.

Note: *Routing must be disabled for bridging to work.*

enable bridge network <network name>

Enables bridging over the specified network. You must have previously run `add bridge network` to add bridging over this network. Bridge networking is enabled by default, so you need to use this command only if you have previously disabled this bridge.

Note: *Bridging does not occur for a protocol if routing is enabled for that protocol.*

enable bridge spanning_tree

Enable the spanning tree algorithm for the bridge connection. The spanning tree algorithm is required if there is more than one bridge between the same two LAN segments. You can use `list bridge forwarding` to see which bridges are defined and `show bridge network <network_name>` to see which options are enabled on a particular bridge network.

enable datalink frame_relay

```
interface <interface_name>
```

Enables frame_relay as the data link layer protocol to run on the specified interface. You must have previously run `add datalink frame_relay` for this command to work.

enable datalink ppp

```
interface <interface_name>
```

Enables PPP as the data link layer protocol to run on the specified interface. You must have previously run `add datalink ppp` for this command to work. You can list currently defined PPP data link enabled interfaces using `list ppp`.

enable dns host_rotation

Enables the RAS 1500 process of randomly choosing a primary IP address and up to eight alternates from the DNS cache. Use the `show dns` command to view the current setting.

enable dns host_rotation

Enables the RAS 1500 process of randomly choosing a primary IP address and up to eight alternates from the DNS cache. Use the `show dns` command to view the current setting.

enable icmp router_advertise

Enables the RAS 1500-generated router advertisements multicast on the same LAN segment as the RAS 1500. Use the `show icmp settings` command to view the current setting.

enable interface <interface_name>

Enables the specified interface. Enabling an interface allows it to transmit and receive data.Use the `list interfaces` command to see the currently defined interfaces and their status.

You can enable multiple interfaces in one command. The following is the format of the list:

```
enable interface <interface 1>,<interface 2>,...
```

The following is the format of each interface:

x/slot:*y*/mod:*z*

where *x* is the type of unit (rm0 for the RAS 1500 unit, pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number.

Example:

rm0/slot:1/mod:1,pem0/slot:1/mod:2

Enter interfaces from the same slot in ranges.

Example:

rm0/slot:1/mod:[1-4],pem0/slot:1/mod:[1-4]

Example:

```
enable interface rm0/slot:1/mod:[1-4],pem0/slot:1/mod:1
```

enable ip address_pool_ filtering

Permits packet filtering on all IP address pools. Use the `show ip` command to view the current setting.

enable ip forwarding

Allows all IP networks to forward (route) packets. You should use this command only if you previously used the `disable ip forwarding` command. Issue the `show ip` command to view the current setting.

enable ip network <network_name>

Enables the specified IP network, which you previously defined using `add ip network`. You can use `list ip networks` to see the currently defined IP networks, as well as their current status.

enable ip rip

Enables the RIP protocol for all IP networks. RIP protocol is set to NONE by default. You can check the RIP version using `show ip network settings` and modify it using `set ip network`. Use the `show ip routing` command to view the current setting.

enable ip routing

Allows all routing protocols for all IP networks. Currently, this command enables only RIP, so it is functionally the same as `enable ip rip`. Use the `show ip routing` command to view the current setting.

enable ip security_option commands

- `enable ip security_option drop_tcp_fragoffset1`
- `enable ip security_option disallow_all_header_options`
- `enable ip security_option disallow_source_route_options`

Each of the above commands allows global filtering of all IP packets containing the specified datagram fields (described below). This security feature also syslogs the event when the packet is dropped. See the `show packet_logging settings` command for accounting data.

The following datagram fields, when found, cause the packet to be dropped:

- *fragment offset=1* — Packets with an offset equal to one are discarded in accordance with RFC 1858. Some routers that may be used on the same network with the RAS 1500 may be configured to filter out specific traffic. In some cases these routers do not apply the filter correctly for IP packets with an offset of 1. To avoid this circumstance in the filtering mechanism, packets of this type can be discarded. Of the two drop commands, this is the highest level of security. Default: *enabled.*

- *partial TCP headers (offset=1)* — Protocol field in the IP packet header (in this case, TCP). Packets of this type can be discarded. Lower level of security than *All fragmented packets (Drop_all_fragoffset1)*. Default: *enabled.*
- *all header options* — All choices in the IP Options field of the IP header. IP options may be generated as an attack to get past routing tables. To avoid this situation in security, packets of this type can be discarded. Of the two disallow commands, this is the highest level of security. Default: *disabled.*
- *source route options* — Another choice in the IP Options field of the IP header. Particular path the sender chooses to take through the network to reach its destination, as specified in the sender packet IP header. Packets of this type can be discarded, although this is a lower level of security than *All Header Options*. Default: *disabled.*

enable ip static_remote_routes

Enables the statically defined remote routes, which you defined using the `add ip route` command. You can list the currently defined IP routes using `list ip routes`. Use the `show ip routing` command to view edits.

enable ip udp_broadcast_ forwarding

Permits the RAS 1500 to forward UDP packets from source ports on the private network. These ports, from which UDP packets are forwarded, are defined using the `add ip udp_bcast_forwarding_port.`

Normally, to save bandwidth, routers do not forward UDP packets. However, since some applications run by the user on the private network require the forwarding of UDP packets, this command can be enabled or disabled, as needed.

Do not enable the RAS 1500 for UDP broadcast forwarding if your network contains loops.

enable ipx network <network_name>

Enables the specified IPX network, which you previously defined using the `add ipx network` command. You can list currently defined IPX networks using `list ipx networks`.

enable ipx rip network <network_name>

Enables the RIP protocol for the specified IPX network. RIP is normally enabled when you add an ipx network. You can see if RIP is currently enabled (ON) using the `show ipx rip` or `show ipx network` commands.

enable ipx sap network <network_name>

Enables the SAP on the specified network. SAP is normally enabled when you add an ipx network. You can see if SAP is currently enabled (ON) using the `show ipx sap` or `show ipx network` commands.

enable modem_group <name>

Enables the modem group you disabled with the `disable modem_group` command. The default modem group, all, includes all modems installed in the stack. See also the `set modem_group` command, which configures all interfaces in the modem group.

enable network service <service_ name>

Enables the network service that you previously defined with the `add network service` command. You can see which services are currently defined and their state using `list network services`.

enable security_option remote_user_ administration <dialin | telnet>

Allows CLI access by remote Telnet (network) or dial-in users. CLI configuration can be done from the console port and remotely. You can use `disable security_option remote_user administration` or `disable security_option snmp user_access` commands to restrict CLI access to the console port only.

enable security_option snmp user_access

Allows SNMP access to the User Table. This lets remote users use SNMP to access the CLI and reconfigure the RAS 1500. You can use `show security_options` to see the current security values.

enable telnet

`escape`

Allows various Telnet functions. Use the `show telnet` command to view settings.

Parameter	Description
escape	All Telnet clients are permitted to use the escape character during a session. By default the escape character is Ctrl] (right bracket). A user can change that value using set_escape in the Telnet program.

enable user <name>

Allows a user to establish dial in and/or dial out sessions. You must have previously added the user using the `add user` command, where enabled is the default. You can use `list users` to see which users are currently disabled.

Exit Command

exit

Leave the CLI, but keep this connection open. This command returns you to Dial-In user or Telnet commands.

Hangup Commands

Cuts interface or modem group connections.

hangup interface <interface_name>

Disconnects any calls (causes the connection on the specified interface to hangup and leave the interface(s) in an *Enabled* state.

You can use this command on multiple interfaces in one command. The following is the format of the list:

```
hangup interface <interface 1>,<interface 2>,...
```

The following is the format of each modem interface:

x/slot:*y*/mod:*z*

where *x* is the type of unit (rm0 for the RAS 1500 unit, pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number.

Example:

rm0/slot:1/mod:1,pem0/slot:1/mod:2

Enter interfaces from the same slot in ranges.

Example:

rm0/slot:1/mod:[1-4],pem0/slot:1/mod:[1-4]

Example:

```
hangup interface rm0/slot:1/mod:[1-4],pem0/slot:1/mod:1
```

hangup modem_group <name>

Makes the modem group unavailable for dial-in users. This command has the same effect as hanging up the phone. See `add modem_group`, `list modem_groups` and `show modem_group` commands for more information.

Help Command

help <command>

Provides information about possible commands and their formats. Typing `help` alone lists the possible commands. Typing `help <command name>` lists the possible parameters for that command.

Typing part of a keyword (command or parameter) and pressing the T (Tab) completes the keyword. If you have not yet entered enough of the keyword to be unique, pressing T causes the bell to ring.

Typing `?` (question mark) after a command string displays the possible keywords and values for that command.

Hide Command

hide events

Reverses the `show events` command where all events being directed to the console or SYSLOG are also echoed to the Telnet session you are running.

History Command

history

Displays previously entered CLI commands. Recall commands from the history cache by using Ctrl p to recall commands up the list, and Ctrl n to recall commands working down the list. The default depth is 10 commands. The range is 1-500. You can modify history depth using the set command history command.

Example:

```
arp
arp camus
arp carrot
list interfaces
host carrot
history
```

Kill Command

kill <process name> Stops an active process. Use the `list processes` command to view active processes. You can only kill a process that you started, for example, a ping command.

You must type uppercase letters and type the full process name when issuing the ***kill*** *command.*

Leave Command

leave Exits a managed user from the CLI, but keeps the link up. This command returns you to Dial-In user or Telnet commands.

List Commands

Displays information saved as entries in the RAS 1500 tables.

list active interfaces

Displays the operational status, administration status, and name of all active interfaces. The output is the same as that from the list interfaces command, except nonactive interfaces are not displayed. Inactive interfaces are interfaces with no current connections. Oper(ational) status indicates current operating state of the interface, UP or DOWN. Admin(istrative) Status indicates the permanently configured status of the interface, UP or DOWN. For modem interfaces, Oper Status is down only if you disable the modem.

```
Interface Name        Oper Status     Admin Status
loopback              Up              Up
internal              Up              Up
rm0/eth:1             Up              Up
rm0/slot:1/mod:1      Up              Up
rm0/slot:1/mod:2      Up              Up
pem0/slot:2/mod:1     Up              Up
pem0/slot:2/mod:1     Up              Up
```

list appletalk forwarding

Displays the entries in the AppleTalk forwarding table. The table lists the following:

- *Network Address Range* — AppleTalk network address range.
- *NextHop* — Address of next hop router; 0.0 implies entry is a local network.
- *Protocol* — Always Routing Table Maintenance Protocol (RTMP).
- *Modified Time* — Time the entry was last modified.
- *UseCount* — Number of times this entry has been used.
- *Port* — Port number.

list appletalk networks

Displays the configured AppleTalk networks. The table lists the following:

- *Name* — AppleTalk network name.
- *Prot* — Protocol, *always* Appletalk.
- *Int* — Interface this network uses.
- *State* — Possible states:

  - Initializing
  - Configuring
  - Enabling
  - Enabled
  - Disabling
  - Disabled
  - Invalid
  - Terminating
- *Type* — Static or dynamic.
- *Network Address* — Address range of this entry.

list appletalk routes

Displays the entries in the AppleTalk routing table. The table lists the following:

- *Address Range* — Range of addresses used on this route.
- *Next Hop* — AppleTalk address of the next hop router. The entry 0.0 implies the entry is a local network.
- *Port* — Address of the network (route destination).
- *Hops* — How many hops away this network is.
- *Type* — AppleTalk, PPP, Serial-Non Standard, or Other.
- *State* — Condition of the path to this network, listed from best to worst: good, suspect, pretty bad, bad. The state of this network worsens when networking packets from that network fail to arrive. The more packets are missing, the worse the state is.

list appletalk zones

Displays all the AppleTalk zones configured for the entire system. It lists the following:

- *Name* — Zone name you defined using `add appletalk zone`.
- *Addr Range* — Range of addresses used in this zone.
- *State* — State of the zone.
- *Port* — Interface the zone runs over.
- *From* — Address of the router from which the zone and network was learned.

list bridge access_mac_address

Displays the MAC addresses of the systems that have access to the bridge network. Use `add bridge access_mac_address` to add addresses and delete bridge access_mac_address to remove them. The MAC address access list is not used unless you run the `enable bridge access_mac_addresses` command.

list bridge forwarding

Displays the following forwarding and filtering information:

- MAC address - A unicast MAC address for which the bridge has forwarding and/or filtering data.
- Status - one of the following:
  - other - not invalid, learned, self, or mmgt
  - invalid - aged out
  - learned - learned and in use
  - self - statically defined and in use
  - mgmt - unknown but filtering information exists
- RxPkt - Number of packets received from this MAC station.
- RxOctets - Number of bytes (octets) received from this MAC station.
- Fltr - Number of packets received from this MAC station that were filtered out (discarded).
- Fwd - Number of packets received from this MAC station that were forwarded.
- TxPkt - Number of packets forwarded to this MAC station.
- TxOctets - Number of bytes forwarded to this MAC station.

list available servers

Displays the available network servers and supported network services. The choices are Dial-out service, SNMP service, Telnet service, TFTP service, or ClearTCP. The services listed by this command are used in the server_type field of the add network service command.

```
Server      Type      Protocol Module      Description
Type
ClearTCPD   NETWORK   TCP      Telnet      ClearTCPD,
                                           enabling access
                                           to a modem group.
HTTPD       NETWORK   TCP      HTML        An HTTP server
                                           for gathering
                                           statistics.
SNMPD       NETWORK   UDP      SNMPAgent   SNMP agent.
TELNETD     NETWORK   TCP      Telnet      TELNET server.
                                           Either to the CLI
                                           or a modem group.
TFTPD       NETWORK   UDP      TFTP        Server side of
                                           TFTP, for
                                           accessing files.
BOOTPD      NETWORK   UDP      BOOTP       Server side of
                                           BOOTP.
```

list connections

Displays all connections established on switched interfaces. It lists the following:

- *IfName* — Modem slot and interface of current connections.
- *User Name* — Name of users currently connected.
- *Type* — Current type of connections established on modems. They include the following:
  - *On-demand* — User connection established for on-demand purposes.
  - *Dial-back* — User connection established for call-back 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, RL(O)G(I)N, TLNT, PING, ADMN, CL(EAR)TCP.
- *Start Date* - Start date of a connection established on the specified interface.
- *Start Time* - Start time of a connection established on the specified interface.

list critical events

Displays last ten critical status events, the facility at issue, the system time when each occurred, and a description of the event. You can change which events are logged as critical, using the `set facility` command.

```
CRITICAL EVENTS
Event


At 14:51:42, Facility "User Manager", Level "CRITICAL"::
AUTH: No acknowledgment from RADIUS accounting servers,
reached max number


At 13:56:26, Facility "User Manager", Level "CRITICAL"::
Unable to allocate memory: ES_NOT_BUFFER replicate
```

list dhcp proxy leases

Displays IP information a dial-in user receives via a Dynamic Host Configuration Protocol (DHCP) proxy lease. This information includes the following:

- *Interface* — Port, i.e., a modem, port expansion module (PEM), or PAU that the dial-in user is dialing in from.
- *User ID* — *Username* associated with the dial-in user requesting an IP address.
- *Client Address* — IP Address assigned by the DHCP server for temporary use by the dial-in user.
- *Life* — Length of time the lease is active.

- *Lease* — A defined period of time that an IP Address is assigned by the DHCP server for temporary use by the local user. The minimum is 1 second; maximum, 12 hours; default, 4 hours.
- *FSM State* — Defined as “Finite State Machine.” It defines the current condition of the lease.

list dhcp server leases

Displays IP information a local user receives via a DHCP server lease. This information includes the following:

- *IP Address* — IP Address assigned by the DHCP server for temporary use by the user on the private network.
- *Lease* — Defined period of time that an IP Address is assigned by the DHCP server for temporary use by the local user. The minimum is 1 second; maximum, 12 hours; default, 4 hours.
- *HW Address* — MAC address of the user requesting an IP address from the server.
- *Client ID* — *Username* associated with the user requesting an IP address.

list dial_out

Displays dial-out information about current modem interfaces. It lists the following:

- *Index* — Table list.
- *General (Modem Group) Name* — Modem group name for the interface enabling network users access to the communication server interfaces without requiring the user to know the specific name or location of an interface.
- *Specific (Interface) Name* — Particular name associated with this interface enabling a network user to find a particular port for access to a specified service associated with that interface.
- *State* — Condition of the interface regarding dial-out use: InUse, Available, and Unavailable.
- *Type* — Type of network connection: None (if no client attached), IP, or IPX.

- *Address* — Ethernet address of the remote station: IP address for IP, MAC address for IPX. If an IP, IPX, or no client is attached to the RAS 1500 port, this value is all zeros.

```
DIALOUT
CONNECTIONS
              General
              (Modem   Specific
              Group)   (Interface)
Index         Name     Name           State      Type   Address

1             All      rm0/           Available  None   0.0.0.0
                       slot:1/mod:3
```

list dns cache

Displays the following entries in the DNS Cache table:

- *Number* — Row number in DNS Cache Table.
- *Pretty Name* — Name of the Resource Record in the cache that is identified in this row of the table. As described in RFC-1034, the owner of the record is the domain name were the resource record is found.
- *Class* — DNS class of the Resource Record in the cache that is identified in this row of the table.
- *Type* — DNS type of the Resource Record in the cache that is identified in this row of the table.
- *Source* — Host from which Resource Record was received, 0.0.0.0 if unknown.

list dns hosts

Displays the DNS local host and its IP address, which you configured using `add dns host` command.

list dns ncache

Displays entries in the DNS Negative Cache table. They list the following:

- *Number* — Row number in DNS Negative Cache Table.
- *Pretty Name* — Name of the Resource Record in the cache that is identified in this row of the table. As described in RFC-1034, the owner of the record is the domain name were the resource record is found.
- *Class* — DNS class of the Resource Record in the cache that is identified in this row of the table.

- *Type* — DNS type of the Resource Record in the cache that is identified in this row of the table.
- DNS Servers.

list dns servers Displays DNS Name Servers, which you configured using the add dns server command. It lists the following:

- *Preference* — Server priority for DNS service.
- *Name* — Your name for the server.
- *Address* — IP address of server.
- *Status* — Current status (ACTIVE, INACTIVE).

list facilities Displays the system facilities (processes) currently running, plus the default log level. This level is the severity of the error messages that are displayed on the Console port. You can change the log level using the `set facility loglevel` command. By comparison, syslog log levels are specified by the `set syslog <name> loglevel` command.

list files Displays the files currently stored in the FLASH file system. You can remove files using `delete file`, but you can add them using TFTP or the Web configurator.

list filters Displays all the filter names in the Filter Table, which you previously defined using the `add filter` command. You can remove filters using `delete filter`. The command lists the following:

- *Filter Name* — Filter file name.
- *Status* — Current status of the filter. The choices are the following:
  - *Save* — Filter file directed to be written to the current configuration file
  - *Saving* — Filter file is being written to the new configuration file
  - *Normal* — Filter file has been written to the configuration file
  - *Verify Failed* — Filter verification failed
- *Protocols* — Filter protocols supported: IP, IP-RIP, IP-CALL, IPX, IPX-CALL, IPX-SAP, IPX-RIP, LOGIN-ACCESS.

list init_scripts Displays all the entries of Modem Initialization Table, which you previously defined using `add init script`. Initialization scripts are assigned to individual modems using the `set switched interface` command. The default initialization script USR_int carries the AT command ATS0=0. You can modify existing initialization scripts using the `set init_script` command.list init_scripts

list interfaces Displays the installed interfaces, their operational status, and the administration status. If an interface is down under Admin Status, you can use `enable interface` to try to bring it up. The command lists the following:

- *Interface Name* — Name of the interface: *rm0/eth:1* (the LAN interface), *loopback*, *internal*, or *x/slot:y/mod:z* (where *x* is the type of unit (rm0 for the RAS 1500 unit, pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number, for example, rm0/slot:1/mod:1).
- *Oper Status* — Current operating status of the interface: *Up* or *Down*. For modem interfaces, Oper Status is Down only if the modem is disabled.
- *Admin Status* — Permanently configured status of the interface, *Up* or *Down*.

list ip addresses Displays the IP address for each active IP network. It lists the following:

- *Address* — IP address of the interface.
- *Bcast Algo* — Algorithm used to determine which address to broadcast representing the entire network. The choices are the following:
  - *1* — IETF standard: *nnn.nnn.nnn.255 (*default)
  - *0* — BSD standard: *nnn.nnn.nnn.000*
- *Reassembly Max Size* — Maximum allowable size of packet that can be reassembled from a fragmented packet.
- *Interface* — Interface this IP address uses to connect to the system. The choices are *internal, loopback, and rm0/eth:1*

list ip arp Displays the contents of the ARP cache. It lists the following:

- *IP address* — Network address for this entry.
- *Phys address* — MAC address the IP address maps to.

- *Type* — Ethernet interface type: *Dynamic.*
- *IfName* — LAN interface name: *rm0/eth:1.*

list ip interface_block

Displays the IP addresses associated with each system interface. If the interface has a point-to-point connection, the neighbor field contains the address of the remote system. This command lists the following:

- *Address* — IP address of the RAS 1500 interface.
- *Neighbor* — IP address of the remote system.
- *Status* — Status of the connection: *Enabled* or *Disabled.*
- *Interface* — Any valid interface.

list ip networks

Displays all the IP networks you previously defined statically using the add ip network command and any dynamic networks created with a modem-established PPP/SLIP connection to the RAS 1500. It also lists the following:

- *Name* — Network designation.
- *Prot* — IP protocol only.
- *Int* — Name of the LAN interface this network runs on *rm0/eth:1* (the LAN interface), *loopback*, *internal*, or *x/slot:y/mod:z* (where *x* is the type of unit (rm0 for the RAS 1500 unit: pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number; for example, rm0/slot:1/mod:1).
- *State* — State of the network: *Ena(bled)* or *Dis(abled).*
- *Type* — *Static* (user-specified), *Auto* (default) or *Dynamic network.*
- *Network address* — Address of the IP network.

list ip pools

Displays the IP pools you configured with the add ip pool command. It lists the following:

- *Name* — Pool designation.
- *Address* — Initial IP address and subnet mask of specified pool.
- *Size* — Number of IP addresses you made available in the pool.
- *InUse* — Number of IP addresses currently in use within the pool.
- *State* — Conditional status of the IP pool: Public or private.

- *Route* — Indicates whether pool is being broadcast as a single network (*aggregate*) or separate networks (*no_aggregate*).Default: *no_aggregate.*
- *Status* — Indicates current condition of pool. The following are the choices:
  - *Active* — pool is available to assign user IP addresses from.
  - *Remove* — pool size is being modified or the base address of the pool is being modified. No users can be assigned from the pool until operation is completed.
  - *Remove_pending* — pool size is being modified, and an active user is currently using a pool entry that must be removed. Users can be assigned from the pool in this state.
  - *Delete_pending* — pool is being deleted but an active user has been assigned out of this pool and must wait until user hangs up to delete the pool. Users are not assigned from the pool in this state.

list ip routes

Displays all the statically defined IP routes that you previously defined using the `add ip route` command, as well as any routes learned via RIP and system-defined routes (loopback). This reflects information collected from the Forwarding Table.

Aggregate routes are not displayed by this command. See the list ip address pools command for their display.

The command lists the following:

- *Destination* — IP address that the route resolves to.
- *Prot* — LOCAL, RIP, or NetMgr (routes you added).
- *NextHop* — Address of the gateway used to reach this route.
- *Metric* — Number of router hops away this route is from the system.
- *Interface* — Interface that the route uses *Loopback*, *rm0/eth:1*, or *x/slot:y/mod:z* (where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number, for example, *rm0/slot:1/mod:1*).

list ip udp_bcast_ forwarding_port

Displays the port numbers on the private network user IP address previously configured for UDP packet forwarding by the `add ip udp_bcast_forwarding_port` command.

list ipx networks

Displays the IPX networks that you previously defined using the `add ipx network` command. It lists the following:

- *Name* — Designation you assigned this network.
- *Prot* — Protocol; always IPX.
- *Int* — Interface on which each IPX network.
- *State* — *Enabled* or *Disabled.*
- *Type* — *STATIC* or *DYNAMIC.*
- Network Address — network address of this IPX network.

list ipx routes

Displays IPX routes you previously defined using the `add ipx route` command, plus the defined IPX nodes, including any IPX routes learned via RIP. It lists the following:

- *Network address* — Network address of this route.
- *Prot(ocol)* — Protocol used to find this route. Choices: *LOCAL*, *RIP*, *STATIC*, *NLSP*, *OTHER.*
- *NextHopNIC* — Network address of the next router (the next hop to the destination), the MAC address for the local IPX nodes (on the LAN).
- *Gateway* — Address of the gateway to this network.
- *Metric* — Number of hops through routers this network is distant from.
- *Ticks* — Estimated interval in eighteenths of a second for packet delivery to the remote network.

list ipx services

Displays IPX pool addresses previously defined with the `add ipx services` command. It lists the following:

- *Name* — Name of the IPX service.
- *NetNum* — Network number that the service is on.
- *Node* — Name of the IPX node running the service.
- *Socket* — Socket number of the service.
- *Type* — Service type in hexadecimal format.
- *Prot* — Protocol used to find this service. Choices: *SAP*, *LOCAL*, *NLSP*, *STATIC*, *OTHER.*
- *Metric* — Number of hops through routers to reach this service.

list ipx static routes

Displays all IPX static routes previously defined using the `add ipx route` command. It lists the following:

- *Network address(es)* — Network address requiring this route.
- *NextHopNIC* — Network address of the next router in the routing path.
- *Gateway* — Address of the host you defined as the gateway.
- *Metric* — Number of routers a packet must pass through to get to gateway.
- *Ticks* — Delay, in hops, to reach the route destination.

list lan interfaces

Displays installed interfaces — Ethernet (rm0/eth:1), its operational status, administration status, and interface index. If the interface is DOWN under Admin Status, you can use enable interface to try to bring it up. The command lists the following:

- *Name* — LAN interface name: *rm0/eth:1.*
- *Oper Status* — Current operating status of the interface: *Up* or *Down.*
- *Admin Status* — Permanently configured status of the interface, *Up* or *Down.*

list login_hosts

Displays currently defined entries in the Login Host Table that you previously defined using `add login_host`. Values displayed are the following:

- *Preference* — Preference (priority) number assigned to the host.
- *Name* — Name you assigned the login host.
- *Port* — Rlogin, Telnet, and ClearTCP TCP port numbers assigned to that login host.
- *Host Address* — Address assigned to the login host.

list modem_groups

Displays modem groups that you previously defined using the `add modem_group` command and the number of ports in each group. This command also lists the default modem group, all, for example:

```
GROUP          Number of Interfaces
all            24
dialout        4
wan            4
callback       4
```

list nat user <user_name>

Displays settings of actively mapped NAT users. The command lists the following:

- *Address* — Active address mappings between the user on the private network and IP address on the public network.
- *Port* — Active port mappings between the user on the private network and the IP address on the public network.

list network services

Displays all network services you defined using the `add network service` command. It lists the following:

- *Name* — Name of service. Choices: *telnetd* (default), *tftpd* (default), *bootpd* (default), *DialOut*, *SNMP*, *ClearTCP.*
- *Server Type* — Type of network server, for example, *TFTPD* (TFTP daemon).
- *Socket* — TCP port number used (you assign or by default) by the service.
- *Close* — Reveals whether all connections close when you disable this service: true or false. See `add network service` command for details.
- *Admin Status* — Status requested for this service: *Enabled* or *Disabled*. See the `add network service` command for details.

list networks

Displays all defined networks running any protocol. The command lists the following:

- *Name* — Designation of the network that you defined with the `add network` command.
- *Prot* — Protocol of the network: *IP*, *IPX*, or *Appletalk.*

- *Int* — Ethernet interface the network is running on: *rm0/eth:1*, *loopback*, *internal*, *x/slot:y/mod:z* (where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number, for example, *rm0/slot:1/mod:1*).
- *State* — Condition of network: *ENA* (enabled), *ENA** (enabling), *DIS* (disabled), *DIS** (disabling), *INIT* (initialized), *INV* (invalid).
- *Type* — *STAT* (static), *DYN* (dynamic), or *AUTO* (default) network.
- *Network Address* — Address of the network.

list pat user <user_name>

Displays settings of actively mapped PAT users. The command lists the following:

- *Address* — Active address mappings between the user on the private network and IP address on the public network.
- *Port* — Active port mappings between the user on the private network and the IP address on the public network.

list ping systems

Displays results of ping, including data from the Remote Ping Table. For more information, see the `ping` command. The command lists the following:

- *Row* — Row number within the Remote Ping Table. Default: 20.
- *Destination* — Host name or IP address of the target node being tested.
- *Status* — Present state of this row. Possible states include the following:
  - *Complete* — Requested number of pings resolved
  - *Active* — Ping requests in progress
  - *Bad address* — Resolved IP address is illegal
  - *Waiting DNS* — Awaiting DNS resolution
  - *Not Active* — Specified ping row not active
  - *DNS Failed* — Destination address could not be resolved
  - *Alloc Failed* — System failed to allocate resources
- *Count* — Number of pings to be transmitted.
- *Interval* — Number of seconds between ping requests. Default: 1 second.

- *Size* — Size of data to be transmitted, in bytes. Default: 64 bytes.
- *TTL* — Ping message time-to-live (TTL) period. Default: 20 seconds.

Row	Destination	Status	Count	Int	Size	TTL
1	cassatt	Complete	50	1	64	20
2	zaphod	Complete	10	1	64	20
3	camus	Complete	30	1	64	20
4	cyclone	Complete	20	1	64	20
5	hiperlc	Active	40	1	64	20
6		Active	35	1	64	20

list ppp

Displays PPP bundles and links. When multiple physical links are combined to run Multilink PPP (MLPPP) (RFC1717), the group of physical links is called a bundle. The second link (channel) becomes active when the channel_expansion percentage has been exceeded. You can check the percentage using `list ppp` and change it using the `set network user ppp` command. This command lists the following:

- *Bundle Index* — Index number of the physical interface in the bundle.
- *Link Index* — Index number in the list of links.
- *Oper Status* — Current operational status of the link. Opened or Not Opened.
- *Interface Name* — Slot and modem designation of interface belonging to this bundle/link.

Bundle Index	Link Index	Oper Status	Interface Name
4		Opened	
	5	Opened	rm0/slot:2/mod:1

list processes

Displays all processes running on the system. It lists the following:

- *Index* — A reference number in the Process Table.
- *Name* — Designation of the process (for example, Event Handler).
- *Type — SYSTEM, APPLICATION, FORWARDER, or DRIVER.*
- *Status — ACTIVE, PENDING, or INACTIVE.*

list sessions

Displays information regarding the current RAS 1500 connections. It lists the following:

- *Name* — Active session username.

- *Conn(ection) Type* — Active session link type. *LAN*, *WAN*, or *UNKNOWN.*
- *Prot(ocol) Type* — Active session protocol. *PPP*, *SLIP*, *TELNET*, *RLOGIN*, *CLEARTCP*, or *UNKNOWN.*

list snmp communities

Displays the SNMP communities defined using the `add snmp community` command. It lists the following:

- *Community Name* — Community designation for the IP address.
- *IP Address* — IP address of a member of the community.
- *Access* — Allowed access for this community. Choices:
  - *Read/Only* — Read-only access to user-level objects allowed.
  - *Read/Write* — Read and write access to user-level objects and write access to writeable user-level objects allowed.
  - *Administrator* — Read access to all objects and write access to all writeable objects allowed.

list stack

Displays a list of the following information pertaining to units configured to the RAS 1500:

- *Module Name* — Name of the PAU or PEM attached to the RAS 1500 via a stacknet.
- *PN ID* — FireWire hardware address that uniquely identifies the unit being stacked to the RAS 1500. The PAU or PEM being stacked contains a PN ID. Note that if two PEMs are attached, each contains a PN ID.
- *Module Type* — Identifies the unit(s) that you are stacking on the RAS: one or two PEMs, or one PAU.
- *Stacknet Name* — Automatically assigned by the RAS 1500.

list switched interfaces

Displays the installed switched interfaces (modems), their operational status, and the administration status. If an interface is down under Admin Status, you can use `enable interface` to try to bring it up. The command lists the following:

- *Interface Name* — Name of the interface. The format is *x/slot:y/mod:z* (where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the modem number, for example, *rm0/slot:1/mod:1*).

- *Oper(ating) Status* — Current operating state of the interface: *Up* or *Down*. Oper Status is Up only if modem is connected.
- *Admin(istrative) Status* — State of the interface configured by the administrator: *Up* or *Down*.

list syslogs

Displays IP addresses that get SYSLOG entries from the Syslog Table. See `add syslog` for more information and `delete syslog` command to remove entries. This command shows the following:

- *Syslog* — IP address to which syslog entries are sent.
- *Log Level* — Reporting level of entries to send: (e.g.) *UNUSUAL.*
- *M(e)s(sa)g(e)* — current number of messages sent since system bootup.
- *Count* — Number of event messages sent to this SYSLOG sink.
- *Facility* — SYSLOG sink node facility to which the SYSLOG message is sent. The choices are *LOG_AUTH*, *LOG_LOCAL0*, *LOG_LOCAL1*, *LOG_LOCAL2*, *LOG_LOCAL3*, *LOG_LOCAL4*, *LOG_LOCAL5*, *LOG_LOCAL6*, and *LOG_LOCAL7.*

Compare with `list facilities` and `set facilities` commands, which control what gets output to the Console port. See the following table.

SYSLOG SINKS				
SysLog	Log Level	Msg	Count	Facility
157.132.148.109	UNUSUAL	214	50	LOG_AUTH

list tcp connections

Displays information about all TCP (Telnet, RLOGIN, etc.) connections including those set by the user. It lists the following:

- *Local address* — IP address of the local host for this connection.
- *Local Port* — TCP port number used by the local connection.
- *Remote Address* — IP address of the remote host for this connection.
- *Remote Port* — TCP port number used by the remote connection.
- *Status* — State of the connection: *Closed*, *Listen*, *SynSent*, *SynReceived*, *Established*, *FinWait1*, *FinWait2*, *CloseWait*, *LastAck*, *Closing*, *TimeWait*, or *DeleteTCB.*

list tftp clients

Displays IP addresses of all users allowed to use the TFTP to connect to the system. Use the `add network service` command to add TFTP support to the system and the `add tftp client` command to authorize users to connect.

Example:

```
TFTP CLIENT addressES
0.0.0.0
157.122.138.134
234.122.156.134
```

list udp listeners

Displays UDP ports being used by the system. These ports correspond to processes that are receiving UDP data (for example SNMP, User Management, TFTP service). Local IP addresses and port numbers are listed for each UDP port.

```
UDP LISTENERS
Local address        Port
0.0.0.000            69
0.0.0.000            123
0.0.0.000            161
0.0.0.000            520
0.0.0.000            1645
0.0.0.000            2049
0.0.0.000            2050
0.0.0.000            3000
```

list users

Displays all users and attributes you specified using the `add` and `set user` commands. It lists the following:

- *User Name* — User designation you specified using `add user` command.
- *Login Service* — *Telnet*, *RLOGIN*, or *ClearTCP.*
- Network Service — Type of network service: PPP or SLIP. SLIP service is not supported for LAN-to-LAN users.
- Status — Link status: *ACTIVE* (in use), *INACTIVE* (not in use), or *DISABLED* (inactivated).

- Type — Type of configured user. See the `add user` command for more information.

```
USERS
                    Login               Network
User Name           Service             Service       Status        Type
larry               TELNET     (D)      PPP (D)       ACTIVE        LOGIN
                                                                    DIALOUT
                                                                    MANAGE
default             TELNET              PPP           INACTIVE      NETWORK
administrator       TELNET      (D      PPP (D        ACTIVE        LOGIN
                                                                    MANAGE
```

Logout Command

logout Leave the CLI and close this connection. This ends the dial-in user or Telnet session.

Monitor Commands

monitor ppp Allows monitoring of real-time PPP activity. For best results, use this program via Telnet. The RAS 1500 offers two methods to evaluate PPP events:

- Using the `set facility` and `show events` commands to record data via syslogs.
- Using the `monitor ppp` command to employ protocol decoding.

When you issue the `monitor ppp` command, the following menu displays.

```
RAS1500 PPP Monitor

Select a letter for one of the following options:
C) Monitor PPP Call Events.
I) Monitor a specific interface.
N) Monitor the next session that starts up.
U) Monitor a specific user
X) Exit the monitor.
Please Enter Your Choice:
```

To monitor PPP events using this command, first issue a `show events` command as a managed user dialing in. Monitor ppp is limited to checking PPP data streams. The command performs the following types of monitoring:

- **Monitoring PPP call events** — Displays internal PPP states as they change for each interface. Most of these events are displayed as events if the proper logging level is set for PPP. This is the only monitoring option that displays the action of more than one PPP session.
- **Monitoring a specific interface** — Displays all PPP packets transmitted and received on the specified interface. If a session is active on the specified interface, monitoring begins immediately. If not, monitoring begins with the next session on that interface. If one session stops and starts, monitoring continues.
- **Monitoring the next session that starts up** — Displays results for next PPP session created. This option is useful if a user is having difficulty connecting and it is unclear on which interface the user connects because of inclusion in a hunt group. As soon as the next incoming or outgoing PPP call is established, monitoring begins. There is no differentiation on the next session. The user selects to monitor the next session and sees the next session displayed, regardless of the interface or username employed.

Only one monitor may be used for Next Session at any one time.

- **Monitoring a specific user** — Displays any PPP sessions currently active for the specified user. As any new session begins for the user, monitoring also begins. This is the best method to display data from a multilink session.

Since the PPP session does not have a user associated with it until authentication occurs, this method of monitoring does not permit tracing of the authentication negotiation.

- **Exiting the monitor** — Exits the program.

Monitoring Stop/Start

To pause the output, press Escape.

All PPP packets sent or received while the monitor is "paused" are lost and not saved, while waiting for the program to resume. Also, if a call is dropped at any time, you must return to the monitor and start again.

Idle Timer

While monitoring is active and no data is displayed, the program displays an idle message to verify it is active.

Example:

```
….Tracing for user “larry”; Escape to stop…
```

Decode and Hexadecimal Display

Interface, User, and Next Session monitoring display two types of data: *decode* and *hexadecimal*. Decode, the default, displays packets without decompression in a textual, decoded output. Hexadecimal displays packets with decompression in hexadecimal and any ASCII equivalent as soon as they are received or just before transmission. During monitoring, press D for Decode and H for Hexadecimal.

Paused Commands

PING

```
ping <destination IP_name or address>
background [yes | no]
count [maximum packets]
data [string]
interval [seconds]
self_destroy_delay [minutes]
size [data size]
timeout [period]
verbose [yes | no]
```

Sends a ping (ICMP echo request) to a remote IP host. This tool to test connectivity can also be initiated from an SNMP station. 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 returns you to the prompt until results are ready.

Parameter	Description
<IP_name or address>	IP address in dotted notation or host name of remote system.
background	When selected, pings are run in a background process on your screen. Can choose either background or verbose, not both. Default: NO.
count	Number of pings requests to send. Default: 1. Range: 1-1000.

Parameter	Description
data	String value specifying data to be sent. Note: If data length is bigger than ping size, only the first ping size octets are used. If data length is zero, the server uses random data. If data length is smaller than ping size, the data pattern is repeated as many times as necessary to fill up the transmission buffer. Range: 0-255 ASCII characters.
interval	Period in seconds between successive ping requests. Note that the actual interval might be different for any given transmission, because the server does not send a new request before a previous request is complete (replied to or timed-out). Default: 1 second. Range: 1-65535.
self_destroy_delay	Period, with *background* selected, indicating the number of minutes a row in the Remote Ping Table is allowed to be inactive before it is erased by the server. A row is considered inactive any time the ping state is one of the following: ■ *Not Active* — Row is not active. ■ *DNS Failed* — Destination address could not be resolved. ■ *Bad address* — Resolved IP address is illegal. ■ *Completed* — Requested number of iterations is completed. ■ *Alloc Failed* — Failed to allocate resources. Range: 0-65535 minutes. Default: 10 minutes.
size	Size of pinged packet. Note that the actual datagram is larger than this value by 42 octets because it includes the following: ■ *MAC header* (14 octets on Ethernet) ■ *IP header* (20 octets) ■ *ICMP header* (8 octets) Default: 64 bytes. Range: 1-1400.
timeout	Period in seconds before determining that a transmission has not been replied to. Range: 1-60. Default: 20 seconds**.**
verbose	When set to *yes*, data is displayed progressively for each ping (if the count is more than one) Output includes each ping *request* and the elapsed *round trip time* in milliseconds, the ping *destination* and its *status*, the ping *count* you specified, any *timeouts* that may have occurred, and *maximum, minimum, and average round trip times*. Can choose either background or verbose, not both. A round trip time of *-1* indicates ping resolution failed. Default: *NO*.

A ping with the verbose parameter selected displays the following:

```
PING Request: 1 Time (ms): 10
PING Request: 2 Time (ms): 0
PING Request: 3 Time (ms): 0
PING Request: 4 Time (ms): 0
PING Request: 5 Time (ms): 0
PING Request: 6 Time (ms): 0
PING Request: 7 Time (ms): 0
PING Request: 8 Time (ms): 0
PING Destination: camus
Status: ALIVE
Count:10
Timeouts Occured:0
Minimum Round Trip (ms):     0
Maximum Round Trip (ms):10
Average Round Trip (ms):1
```

Quit Command

quit Leave the CLI, but keep this connection open. This command returns you to the Dial-In User or Telnet commands.

Reboot Command

reboot Reboots the system. If you have made any configuration changes, be sure to issue the `save all` command before rebooting. Also see the `delete configuration` command.

Reconfigure Command

reconfigure ip network <network name>

```
address <IP_address>
interface <rm0/eth:1>
frame <ethernet_ii | snap>
```

Automatically reconfigures IP network parameters of an established static IP LAN network. This command changes network parameters without the administrator having to remove the router from service by manually disabling the network, modifying its parameters, and re-enabling it. This command modifies static IP LAN networks only (cannot change interface and frame values for an internal address). Network and interface names are limited to 64 ASCII characters. See the `add ip network` command for more information.

Rename Command

rename file <input_file> <output_file>

Copies files within the FLASH file system. The FLASH file system is a flat file system (no subdirectories). Use the `list files` command to view currently existing files.

Parameter	Description
<input_file>	Name of the original file.
<output_file>	New name for the file.

Reset Commands

Restores the following RAS 1500 settings to their default configuration.

```
reset
modem_group <name>
modems <modem name>
```

Parameter	Description
modem_group	Resets the specified modem group following changes to its configuration. This "hard" reset issues an ATZ! command, closing any active connections on that port.
modems	Resets the specified modems (interfaces) following changes to its configuration. This "hard" reset issues an ATZ! command, closing any active connections on that port. The command also lets you reset multiple modems. You can reset multiple modems in one command. The following is the format of the list: reset modems <modem 1>,<modem 2>,... The following is the format of each modem: x/slot:y/mod:z (where x is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), y is the slot number, and z is the modem number. Example: rm0/slot:1/mod:1).

Example:

```
reset modems rm0/slot:1/mod:[1-4]
```

Resolve Command

resolve name <IP_host_name>

Returns an IP address for the specified host name by sending it to DNS for resolution. If the Domain Name is specified using the `set DNS` command, it is also resolved, otherwise you must specify it as part of the name. This command requires either a DNS local host (add DNS host) or a DNS server entry (add DNS server) to resolve the name. This command is identical to the `host` command.

RLOGIN Command

rlogin <IP_name or address>

```
login_name [login_name]
TCP_port [number]
```

Creates an rlogin client connection to the specified host.

Parameter	Description
<ip_name_or_address>	Either the IP address in nnn.nnn.nnn.nnn notation or the host name of the remote system. Limit: **64** ASCII characters.
login_name	Username needed to login to the remote system.
TCP_port	TCP port number to create the connection to. Default: 513. Maximum: 65535.

Save Commands

Preserves changes you made to the RAS 1500 configuration files.

save all

Saves all changes made during your CLI session. We recommend saving your changes frequently, as with any editor. When a save all is in process, the following message is displayed:

```
Saving ... SAVE ALL
```

When the save is *finished*, the following message is displayed:

```
Saving.....
SAVE ALL Complete.
```

Set Commands

Changes any parameter you specified with an add command, with the exception of certain accounting and authentication commands that are *not* preconfigured by add commands.

set accounting

This field is a KEYWORD. The possible values are the following:

```
primary_port <port_number>
primary_secret <"secret_string">
primary_server [IP_address or host_name]
retransmissions <number>
secondary_port <port_number>
secondary_secret <"secret string">
secondary_server [IP_address or host_name]
start_time [authentication | connection]
timeout [number_seconds]
use_servers [one | both]
```

Configures remote (RADIUS) accounting. Use the `show accounting` command to check these values.

The IP address/port number pair for accounting and backup servers must be unique or conflicts occur. For example, one accounting server designated as both first and second server must have unique port numbers designated for both servers. However, the same port number can be designated on servers with different IP addresses.

Parameter	Description
primary_port	Destination port number of the primary RADIUS server. To ensure correct identification of server response packets, configure a unique IP address/port combination. Range: 0-65,535. Default: 1646.
primary_secret	Password of the Primary RADIUS server. Limit: 16 ASCII characters. Null string: **“”**
primary_server	Initial server to send the accounting information to. To ensure correct identification of server response packets, configure a unique IP address/port combination.
retransmissions	Maximum number of times to retransmit packets to accounting servers if transmissions fail. Default is 400. Range is 0-200.
secondary_port	Port number of the Secondary RADIUS server. To ensure correct identification of server response packets, configure a unique IP address/port combination. Range: 0-65,535. Default: 1646.
secondary_secret	Password of the Secondary RADIUS server. Limit: **16** ASCII characters. Null string: “ ”
secondary_server	Second server to send the accounting information to. To ensure correct identification of server response packets, configure a unique IP address/port combination.
start_time	When accounting begins. You may choose either: ■ *Authentication* — session time in number of seconds after username and password are entered. ■ *Connection* — session time in number of seconds from modem pickup.
timeout	Interval between retransmissions. Default: 60 seconds. Range: 1-60.
use_servers	*one*: send accounting information to the primary server only, the second server acts as backup. *both*: send accounting information to both servers until a response is received from both servers.

set appletalk network <network name>

```
aarp_gleaning [disabled | enabled]
current_zone <string>
ddp_checksums [disabled | enabled]
default_zone <string>
description <string>
desired_mode_address <ap_node_addr>
seed_router [disabled | enabled]
```

Sets parameters for all AppleTalk networks, including the following:

Parameter	**Description**
<network name>	Unique designation you assign for the AppleTalk network that you want to configure. Limit: 32 ASCII characters.
aarp_gleaning	Enables the forwarder to learn hardware addresses from the AARP packets it receives.
current_zone	Designation of zone the router is advertised in.
ddp_checksums	Setting this parameter to TRUE results in checksums being calculated on DDP packets. The checksum is used to detect errors caused by faulty operation within routers on the network.
default_zone	Designation of the default zone for systems on this network.
description	A description of the network. Limit: 32 ASCII characters.
desired_mode_address	AppleTalk address used first when probing for an AppleTalk address at the time the network is enabled.
seed_router	TRUE enables the router to propagate seed (network range, zones) data.

set authentication

```
primary_port <port number>
primary_secret <string>
primary_server <IP_address or name>
retransmissions <count>
secondary_port <port number>
secondary_secret <string>
secondary_server <IP_address or name>
timeout <period>
type <nos | radius>
```

Configures remote (RADIUS) authentication for up to three servers. Use `show authentication` command to check these values.

Parameter	Description
primary_port	RADIUS destination port for the primary authentication server. Default: 1645. Range: 0 - 65,535.
primary_secret	Password of the Primary RADIUS server. Limit: **16** ASCII characters. Null string: **""**
primary_server	IP address or name of the initial server to exchange authentication data with.
retransmissions	Maximum number of times to retransmit packets to one or both servers if transmissions fail. Default: 10. Range: 0-100. Value of 0 infinite retries. We recommend you do not set to 0.
secondary_port	RADIUS destination port for the secondary authentication server. Default: 1645. Range: 0 - 65,535.
secondary_secret	Password of the Secondary RADIUS server. Limit: **16** ASCII characters. Null string: **""**
secondary_server	IP address or name of the second server to exchange authentication data with.
timeout	Interval in seconds between retransmissions. Default: 3 seconds. Range: 1-60.
type	The type of server, either *RADIUS* (default) or *NOS*.

set bridge

```
aging_time
forward_delay
spanning_tree_priority
```

Sets parameters for all bridge networks.

Parameter	Description
aging_time	Interval to wait before aging out MAC addresses that were learned from other LAN segments. The default is 300.
forward delay	Interval that bridge waits before bridging packets. This time is useful for the bridge to listen to packets, look at the MAC addresses, and build a MAC address table. Default is 15 seconds.
spanning_tree_ priority	Priority number determines who is seen as the “root” bridge in a bridge network. The default is 32768.

set clearTCP connect_message <message string>

Configures the string that is sent to ClearTCP clients, when the TCP connection is established. The message string must be enclosed in quotes. The limit is *64 ASCII characters*. See the conventions below to follow when composing the message.

If the string is surrounded by double quotes, you can insert an escape character '\' inside the quoted string. If the string is followed by the characters *b*, *f*, *n*, *r*, *t*, or *v*, the RAS 1500 places special characters in the string, as follows:

- \b = backspace
- \f = formfeed
- \n = newline
- \r = carriage return
- \t = tab
- \v = vertical tab

If the string is followed by an ***x***, the next two characters are interpreted as a hexadecimal constant as follows:

- x0A = 0x0a

If the string is followed by *any other character*, that character is placed in the token.

Other rules state the following:

- a double quote (**"**) places the double quote in the token
- a forward slash '\' places one forward slash in the token

set command

```
history <number>
idle_timeout <interval>
local_prompt <string>
login_required [no | yes]
prompt <string>
```

Configures command line parameters. It lists the following:

Parameter	**Description**
history	Sets depth of the buffer holding command history. Use history command to see current depth and list of your last CLI commands. Default: 10 commands. Range: 1-500.
idle_timeout	Sets Console login connection to close after being idle for the specified interval, if that user is required to log in (login_required value must be set to YES. Range: 0-60 minutes. Default: 5 min. Zero (0) value produces no timeout. Value can be changed only by a manage user.
local_prompt	Sets a separate (temporary) prompt for a command file session. Limit: **64** ASCII characters.
login_required	Sets whether a user on the Console port is required to log in. Value can be changed only by a manage user. Default: No.
prompt	Sets the global (permanent) command prompt for the CLI. Use `show command` to see the currently defined prompt. Limit: **64** ASCII characters.

set connection

```
host_select [round_robin | random] message [message
prompt]service [dialin user prompt]user_name [username]
```

Configures global connection parameters for all *dial-in* users. Issue the `show connection` command to display current settings.

Parameter	**Description**
host_select	Specifies how the system chooses which host to connect the user to. Next host is chosen sequentially (*round_robin)* or randomly *random*. Default: Round_robin.
message	String displayed when a dial-in user is connected and is a manage user. Limit: 64 ASCII characters. Default: message**:.**
service	String that prompts the connected dial-in user who has both login and network access enabled. Limit: 64 ASCII characters. Default: Login/Network user.
user_name	String that serves as the user prompt. The global username “default” is specified if no name is entered. Limit: 64 ASCII characters.

set datalink ppp wan_interface

You can configure an Analog/ISDN fallback link, which will become operative when the RAS 1500 detects a connection problem on the WAN port. When the RAS 1500 detects that the connection problem has abated, it will revert to the original connection.

You can configure whether fallback support is enabled or disabled, and the start and stop timeout for this feature. To configure the *Fallback Support* feature procede as follows:

1 Add a network dialout user, with the **add user <user_name>** command.

You will have to configure this user with the same parameters as the user profile that you want to apply the Fallback Support feature to, but with a different IP address. You are setting this new user up to be the fallback link.

2 Use the following commands to set up the *PPP Fallback Support* feature for a particular WAN interface:

```
set datalink ppp wan_interface
     fallback_support <enabled | disabled>
     fallback_start_threshold <integer>
     fallback_stop_threshold <integer>
     fallback_user <fallback_user_name>
```

The parameters for the Fallback Support configuration are defined in the following table:

parameter	description
fallback_support enabled	enables fallback support for the ppp datalink on WAN interface
fallback_support disabled	disables fallback support for for the ppp datalink on WAN interface
fallback_start_threshold	number of unanswered icp echo requests to wait before bringing up the fallback link, when the RAS 1500 detects a disruption in connectivity on the WAN port Range — 4 to 50 seconds Default: 10
fallback_stop_threshold	the number of successful icp echo responses to wait before bringing down the fallback link, when the RAS 1500 detects a resumption in connectivity on the WAN port Range — 4 to 50 seconds Default: 10

parameter	description
fallback_user_name	the name of the network dialup user you created to act as the fallback link

3 Review your configuration settings by using the **show ppp settings** command.

4 Save your configuration settings using the **save all** command.

set date <date> time <time> or set date <date>

Sets the system date and time. Alternately, the set date command leave the time unchanged. Use show date to see what the current settings are. The format is dd-mmm-[yy]yy. The month should be the first three characters of the month name. The year can be expressed in either 2 or 4 digits - 97 or 1997. The time is expressed in hh:mm:ss format with seconds optional.

set dhcp mode

```
[disabled relay server proxy]
```

Displays the three DHCP modes available to choose from to set in the RAS 1500: disabled, relay, or server.

Note: *The RAS 1500 can be set to use DHCP as a relay* ***or*** *a server, but never as both simultaneously.*

Parameter	Description
disabled	Disables DHCP in the RAS 1500.
relay	Sets the RAS 1500 to implement DHCP as a relay. As a relay, the RAS 1500 passes on a DHCP request for IP information from a local user to a DHCP server.
server	Sets the RAS 1500 to implement DHCP as a server. As a server, the RAS 1500 receives a request for IP information from a local user, processes the request and provides the IP information directly to that user.

set dhcp proxy [server1 | server2]

```
address <ip_address>
```

Sets the RAS 1500 to implement DHCP as a proxy. As a proxy, the RAS 1500 initiates a DHCP request to the DHCP server on behalf of the DHCP dial-in clients. The DHCP server processes the request and sends the IP information back to the dial-in user via the RAS 1500.

Parameter	Description
server1	The primary DHCP server that receives and processes the request for IP information.
server2	The secondary DHCP server that receives and processes the request for IP information if the primary server is busy or unavailable.
address	IP address of the DHCP server.

set dhcp relay [server1 | server2]

```
address <ip_address>
enabled [no | yes]
max_hops
```

Sets the RAS 1500 to implement DHCP as a relay. DHCP relay forwards DHCP requests to the DHCP server. The DHCP server processes the request and sends the IP information back to the dial-in user via the RAS 1500.

Parameter	Description
server1	The primary DHCP server that receives and processes the request for IP information.
server2	The secondary DHCP server that receives and processes the request for IP information if the primary server is busy or unavailable.
address	IP address of the DHCP server.
enabled	Optional parameter that indicates whether DHCP relay is enabled (YES) or disabled (NO). Default is YES.
max_hops	Greatest number of hops configured to locate a DHCP server. The default is 15. The minimum is 1, and the maximum is 255.

set dhcp server

```
dns1 <ip_address>
dns2 <ip_address>
domain <name>
end_address <ip_address>
hostname <name>
lease <lease duration>
mask {this field types does not have a positional help
explanation}
router <ip_address>
start_address <ip_address>
wins1 <ip_address>
wins2 <ip_address>
```

Sets the RAS 1500 to implement DHCP server. As a server, the RAS 1500 provides the information specified by the above parameters in response to a DHCP request.

Parameter	**Description**
dns1	Primary DNS that processes and responds to request for IP information.
dns2	Secondary DNS that processes and responds to request for IP information.
domain	Unique name of DHCP Server. Limit: 32 ASCII characters. To include white space in the name, surround it by double quotes. An example domain name is usr.com.
end_address	The last address that appears in the range of IP addresses assigned by the DHCP Server. The expected format is a.b.c.d. The address must be in the range of 0 to 255. The address 127.x.x.x is reserved for loopback. An address of 248.x.x.x or higher is not part of a valid IP Network Class (A, B, C, or E).
hostname	Name of the DHCP server that processes and responds to the the request for IP information.
lease	A defined period of time that an IP Address is assigned by the DHCP server for temporary use by the local user. Minimum is 1 second. Maximum is 12 hours. The default is 4 hours.
mask	Defines the size of the subnet.
router	The IP address of the router that IP request is processed through if the user making the request is outside local subnet.
start_address	The first address that appears in the range of IP addresses assigned by the DHCP Server. The expected format is a.b.c.d. The address must be in the range of 0 to 255. The address 127.x.x.x is reserved for loopback. An address of 248.x.x.x or higher is not part of a valid IP Network Class (A, B, C, or E).
wins1	Primary WINS (Windows Internet Name Service) server address.
wins2	Secondary WINS (Windows Internet Name Service) server address.

set dial_out user <username>

```
idle_timeout <interval>
recovery_timeout <interval>
security [ yes | no ]
```

Sets user parameters for dial-out connections over modems.

Parameter	Description
idle_timeout <interval>	Interval allowed before an idle connection is closed. If security is on (Yes), timeouts derive from user values. Range: 1 minute to 3 hours. Default: 0 (not activated).
recovery_timeout <interval>	When a connection is closed, the time allowed before session is cancelled. This allows a dial-out user time to reconnect, if, for example, the phone cord is jarred from the jack or the PC reboots. Range: 1 minute to 180 minutes (or 3 hours).
security	Determines whether to require username and password when dialing out. If YES, login authorization is required. Default is Yes.

set dns

```
cache [enabled | disabled | clear]
cache_maxttl [0 - 2147483]
domain_name <string>
ncache [enabled | disabled | clear]
ncache_maxttl [0 - 2147483]
number_retries <1-5>
timeout <interval>
```

Sets the global parameters for DNS. This includes both local DNS hosts (`list DNS host`) and remote DNS servers (`list DNS servers`) and DNS caching and negative caching parameters, in support of DNS host rotation for load balancing. See the associated commands `set login user <name> login_host_name` and Chapter 2, “Administrative Tools,” for more information.

Parameter	Description
cache	Enables or disables DNS caching. Setting to CLEAR flushes the DNS cache. Default: disabled.
cache_maxttl	Maximum time in seconds DNS cache entries remain in the DNS cache before they are flushed. Range: 0 - 2147483.
domain_name	Default domain designation to be used if no domain is specified (by `add dns server` command) in the name to be resolved. Example: usr.com. Limit: **64** ASCII characters.
ncache	Enables or disables negative DNS caching. Setting to CLEAR flushes the DNS negative cache. The negative DNS cache contains entries the DNS server found to be in error. For example, if the host name abc.xyz.com does not exist, the DNS server returns a nonexistent name error.
ncache_maxttl	Maximum time in seconds DNS negative cache entries remain in the DNS negative cache before they are flushed. Range: 0 - 2147483.
number_retries	Number of times the resolve name request is sent to each Name Server if the server fails to respond to a request before the timeout period. Default: 1. Range: 1-5.
timeout	Interval in seconds to wait before deciding a request to a Name Server has timed out. The minimum interval and default is 5 seconds; maximum interval, 245 seconds.

set dns server preference <number>

```
name <server_name and domain_name>
address [IP_address]
```

This command redefines the name of a domain name server, which you previously defined using the `add DNS server` command. Use the `list DNS servers` command to see the currently defined DNS servers.

Parameter	Description
preference <number>	Priority of the name server in name searches from *1* (highest) to *10* (lowest).
server name	Designation - must be unique - given the DNS server. This field is optional, but is useful for keeping track of name servers. You can also supply the domain name. Limit: *64 ASCII characters*.
address	IP address of the DNS server.

set dst off

```
amount_to_correct <time>
day_of_week [friday monday saturday sunday thursday tuesday
wednesday]
month [april august december february january july june march
may november october september]
time_to_correct <time>
week_of_month <1-5>
```

Sets time to adjust for the end of daylight savings time.

Parameter	Description
amount_to_correct	Amount of time defined in hours, minutes, and seconds set to reflect time difference due to the ending of daylight savings time. Entered as HH:MM:SS. The second field is optional.
day_of_week	Day of week daylight savings time ends.
month	Name of month daylight savings time ends.
time_to_correct	Denotes the time to correct to time difference due to the ending of daylight savings time. Entered as HH:MM:SS. The second field is optional.
week_of_month	Week of the month daylight savings time ends. The options are 1, 2, 3, 4, or 5.

***Note:** If you are configuring a RAS 1500 in a zone that observes daylight savings time, you **must** set time commands in the following order: 1) set timezone, 2) set dst, and 3) set time.*

set dst on

```
amount_to_correct <time>
day_of_week [friday monday saturday sunday thursday tuesday
wednesday]
month [april august december february january july june march
may november october september]
time_to_correct <time>
week_of_month <1-5>
```

Sets daylight savings time to on.

Parameter	Description
amount_to_correct	Amount of time defined in hours, minutes, and seconds set to reflect time difference due to the start of daylight savings time. Entered as HH:MM:SS. The second field is optional.
day_of_week	Day of week daylight savings time begins.
month	Name of month daylight savings time begins.
time_to_correct	Denotes the time to correct to time difference due to the start of daylight savings time. Entered as HH:MM:SS. The second field is optional.
week_of_month	Week of the month daylight savings time begins. The options are 1, 2, 3, 4, or 5.

set facility <facility_name> loglevel [level]

Sets the severity reporting level of a facility to display messages on the console (your hard-wired connection to the RAS 1500) or on a PC telnetted to the RAS 1500. Use the `list facilities` command to view the current loglevel is for each facility. Default loglevels for most facilities is *critical*.

Do not confuse `set facility` *and* `set syslog` *commands. The* `set facility` *command determines which messages are generated on the console or to a telnetted PC, depending on the loglevel specified for each facility. The* `set syslog` *command, however, determines which messages are saved, depending on the global loglevel set for the particular SYSLOG host. The* `show event` *command displays event messages on the console if telnetted into the RAS 1500.*

The log levels are the following:

- *Critical* — A serious system error, which may effect system integrity.
- *Unusual* — An abnormal event, which the system should recover from.
- *Common* — A regularly occurring event.
- *Verbose* — A regular periodic event, for example, a routing update message.
- *Debug* — For debugging purposes only.

set frame_relay

Configures

```
conformance
on
PVC
```

set frame_relay pvc <pvc_name>

You can configure an Analog/ISDN fallback link, which will become operative when the RAS 1500 detects a connection problem on the WAN port. When the RAS 1500 detects that the connection problem has abated, it will revert to the original connection.

You can configure whether fallback support is enabled or disabled, and the start and stop timeout for this feature. To configure the *Fallback Support* feature procede as follows:

1 Add a network dialout user, with the **add user <user_name>** command.

You will have to configure this user with the same parameters as the user profile that you want to apply the Fallback Support feature to, but with a different IP address. You are setting this new user up to be the fallback link.

2 Use the following commands to set up the *Fallback Support* feature for a particular pvc:

```
set frame_relay pvc <pvc_name>
     fallback_support <enabled | disabled>
     fallback_start_timeout <integer>
     fallback_stop_timeout <integer>
     fallback_user <fallback_user_name>
```

The parameters for the Fallback Support configuration are defined in the following table:

parameter	description
fallback_support enabled	enables fallback support for this pvc
fallback_support disabled	disables fallback support for this pvc

parameter	description
fallback_start_timeout	the time, in seconds to wait before bringing up the fallback link, when the RAS 1500 detects a disruption in connectivity on the WAN port Range — 10 to 7200 seconds Default: 10
fallback_stop_timeout	the time, in seconds to wait before bringing down the fallback link, when the RAS 1500 detects a resumption in connectivity on the WAN port Range — 10 to 7200 seconds Default: 10
fallback_user_name	the name of the network dialup user you created to act as the fallback link

3 Review your configuration settings by using the **show frame_relay pvc <pvc_name>** command.

4 Save your configuration settings using the **save all** command.

The LMI polling mechanism acts as the backbone for the Fallback feature. You must have the LMI feature activated to use Fallback.

set imodem interface <interface_name>

Configures specific modems on your RAS 1500, PEM, or PAU for ISDN access.

```
at_command <string>
call_type [auto | clear | internet | modemfax | v110 | 120]
directory <stribg>
directory_number1 <string>
directory_number2 <string>
dsx1_line_type [d4 | e1 | e1_crc | e1_crc_multiframing |
e1_multiframing | extended_superframe]
nic_config_type [from_0_to_133ft | from_133_to_266ft |
from_266_to_399ft | from_399_to_533ft | from_533_to_655ft |
longhaul]
spid1 <string>
spid2 <string>
switch [att5ess | aus | australia | dms100 | etsi | germany |
ins64 | italy | japan | newzealand | nt1 | nz | spain | taiwan
| tr6]
tx_line_buildout [db0pt0 | negdb15pt0 | negdb22pt5 |
negdbypt0 | negdbypt0 | negdbyt5]
```

Parameter	Description
<interface_name>	The type of module you want to configure: Router unit, PEM, or PAU for ISDN access.
at_command	Configures modem to dial and answer.
call_type	Identifies that type of connection from the incoming call. The possible call types are auto, clear, internet, modemfax, v110, or v120.
directory	Parameter that allows access to set both directory_number1 and directory_number 2, which are provided by the ISDN access provider.
directory_number1	The primary access number assigned by the ISDN access provider.
directory_number2	The secondary access number assigned by the ISDN access provider.
dsx1_line_type	Defines Digital System Cross Connect Level 1 line types (T1 and DS1), which permit cross connections by patch cords and plugs.
nic_config_type2	
spid1	Service Profile Identifier: a unique number assigned by the telephone company to identify the first B channel in BRI ISDN service.
spid2	Service Profile Identifier: a unique number assigned by the telephone company to identify the second B channel in BRI ISDN service.
switch	Identifies which of the three switch types is used by the telephone company. The 3 possible switch types are 1) AT&T5ESS Custom, 2) National ISDN-1, and 3) NT DMS100 Custom.
tx_line_buildout	.

set init_script <script_name>

```
command <string>
```

Modifies an init_script, that you previously defined using `add init_script`. You can see the currently defined initialization scripts using `list init_scripts`.

Parameter	Description
<script_name>	Designation for a modem initialization string. Maximum size is 7 characters. If you are setting an init_script for a modem pool or interface, the init_script name must already exist.
command	Modem initialization string must be entered with quotes and must be less than 56 characters.

set interface <interface_name>

```
filter_access [on | off]
input_filter <filter_name>
output_filter <filter_name>
```

Sets filter parameters for the specified filter on the specified interface. You can see the available filter files using `list filters`, view the contents of a filter file using `show filter`, and add filter files to FLASH memory using `TFTP`.

Interface filters can be changed without disabling and re-enabling each network on that interface.

Parameter	Description
<interface_name>	Designation of interface you are setting parameters for. Limit: *64 ASCII* characters. Either: *rm0/eth:1* (the LAN interface), ***loopback***, ***internal***, or ***x/slot:y/mod:z*** (where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit; and pau0 for the PAU), *y* is the slot number, and *z* is the modem number. Example: rm0/slot:1/mod:1).
filter_access	Off causes filters specified for an interface with a set interface command to override filters specified with a `set user` command when the filters are of the same type. Default: Off.
input_filter	Name of the filter file you wish to be applied to the input stream coming in on the specified interface. Limit: 20 ASCII characters.
output_filter	Name of the filter file you wish to be applied to the output stream leaving the specified interface. Limit: 20 ASCII characters.

set ip address_assign_ mode

```
dhcp_proxy
ip_pool
```

Configures the RAS 1500 to assign IP addresses either through using the DHCP feature or through the IP pool feature. The RAS 1500 automatically attempts to request the IP address from the IP pool first. If an address cannot be assigned because an IP pool has not been established, the RAS 1500 makes a dchp proxy request to the dhcp server.

Parameter	Description
dhcp_proxy	The RAS 1500 initiates a DHCP request to the DHCP server on behalf of the DHCP dial-in clients. The DHCP server processes the request and sends the IP information back to the dial-in user via the RAS 1500.
ip_pool	A range of IP addresses set by the system administrator and dynamically assigned to remote dial-in clients each time a connection is established.

set ip defaultroute gateway <IP_address or name>

```
metric [hop count]
```

Reconfigures a backup default route. The command changes the address or metric of a *primary* default route with a gateway on the IP network configured on the RAS 1500 LAN interface (rm0/eth:1).

A default route gateway specified with a higher metric acts as the *primary* default route gateway.

If the Ethernet interface goes down, the default route gateway associated with that interface is disabled. If a second default route gateway associated with a still-alive interface exists, that gateway is installed as the primary gateway. If the disconnected Ethernet interface is reconnected, the associated gateway is reinstalled.

Parameter	Description
<IP_address >	IP address of the gateway router.
metric	An integer representing how far away the default router is, in hops through other routers. Range: 1-15**.** Default: 1.

set ip multicast proxy interface <interface_name>

Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with this command.

set ip network <name>

```
broadcast_algorithm [0 | 1]
reassembly_maximum_size [0-65535]
rip_authentication_key [string]
rip_policies_update <rip_policies>
routing_protocol [none | ripv1 | ripv2]
```

Configures the type of broadcast algorithm, the maximum size for reassembling fragmenting packets, the RIP password, RIP export metric, RIP policies, the routing metric, and the routing protocol for the specified interface. The only required parameter for this command is <name>. All other parameters are optional. You can set all of them at once or one at a time. This command can only be used on IP networks previously defined using `add ip network`. You can list the currently defined IP networks using `list ip networks`.

As activated by this command, routing is appropriate on a LAN segment where the default route gateway is not used because the RAS 1500 dynamically adds discovered hosts to its Routing Table. It is also appropriate in a LAN-to-LAN scenario where routing must additionally be activated in user profiles on both sides of the WAN (using the `set network user ip_routing [both|listen|none|send]` command. Since the default is none, routing is not activated until you select ripv1 or ripv2.

You must disable the IP network before setting these parameters, using the `disable ip network` *command, or, use the* `set ip network` *command followed by the* `reconfigure ip network` *command. By issuing a* `show ip network <name> settings` *command, you can determine from the* Reconfigure Needed: *field whether a reconfigure was done.*

RIP Policies

The following RIP policies are supported by the IP route:

- *Send Default — Disabled* by default, causes router to advertise itself as the default router.
- *Send Routes — Enabled* by default. Tells RIP to advertise (broadcast) its routes on the network every 30 seconds - is standard for a gateway router.
- *Send Subnets — Disabled* by default. If this flag is on, only routes with the same network and with subnets on the same network are sent out the interface.

- *Accept Default* — *Disabled* by default. Determines whether router accepts default route advertisements.
- *Split Horizon* — *Enabled* by default. Records the interface over which it received a particular route and does not propagate its information about that route back over the same interface. This prevents network loops.
- *Poison Reverse* — *Disabled* by default. Routes that were excluded due to the use of split horizon are instead *included* with infinite cost (16). The system continues to broadcast the route, but with an infinite cost.

***Note:** To perform poison reverse, you **must also enable** split horizon.*

- *Flash Update* — *Enabled* by default. It is also known as “triggered update”, meaning routes that have their metrics modified are advertised immediately, instead of waiting for the next scheduled broadcast.

The flags described are for backward compatibility with RIP version 1 when RIP version 2 is selected as the routing protocol.

- *Send Compatibility* — Controls the selection of destination MAC and IP addresses. It is *enabled* by default. When enabled, *broadcast* address is used; when disabled, *multicast* address is used.
- *RIP V1 Receive* — Controls the receipt of RIP version 1 updates. When RIP version 1 is the selected routing protocol, this policy is *enabled* by default, which means RIP version 1 packets are received. (When RIP version 2 is chosen, this policy is *enabled* by default, meaning RIP version 1 packets are received.
- *RIP V2 Receive* — Controls receipt of RIP version 2 updates. When RIP v1 is the selected routing protocol, this policy is *enabled* by default, which allows RIPV1 packets to be received. When RIP version 2 is selected, this policy is *enabled* by default, allowing RIPV2 packets to be received. RIPV2 is backward compatible.
- *Silent* — This flag tells RIPv2 not to send updates. It is *disabled* by default.

Parameter	**Description**
<network_name>	Designation of the IP network for which you want to set parameters. Limit: *64 ASCII* characters.
broadcast_algorithm	Algorithm determines which address is used in broadcasts to represent the entire network. Choices: ■ *0* - the BSD standard: nnn.nnn.nnn.000 ■ *1* - the IETF standard: nnn.nnn.nnn.255 (default)
reassembly_maximum_size	Maximum size IP datagram that the system attempts to reassemble, when the datagram has been fragmented to fit in the network packet size. Default: 3464.
rip_authentication_key	ASCII string used for RIPv2 authentication.
rip_policies_update	Allows user to enable or disable RIP policies. See text on the preceding page for description of keywords. A keyword with a *NO_* in front is used to disable the policy. Default indicated by (D). *Note*: For Poison Reverse to work properly, Split Horizon must also be enabled. ■ SEND_Default/NO_SEND_Default(D) ■ SEND_ROUTES(D)/NO_SEND_ROUTES ■ SEND_SUBNETS/NO_SEND_SUBNETS(D) ■ ACCEPT_Default/NO_ACCEPT_Default (D) ■ SPLIT_HORIZON(D)/NO_SPLIT_HORIZON ■ POISON_REVERSE/ NO_POISON_REVERSE(D) ■ FLASH_UPDATE(D)/NO_FLASH_UPDATE ■ SEND_COMPAT(D)/NO_RIPV1_SEND ■ RIPV1_RECEIVE(D)/NO_RIPV1_RECEIVE ■ RIPV2_RECEIVE(D)/NO_RIPV2_RECEIVE ■ SILENT (default is disabled)
routing_protocol	Sets routing protocol to be used on IP network. Choices: *none*, *RIP version 1*, or *RIP version 2*. Default: *None.*

set ip pool <pool name>

```
initial_pool_address <IP_address/subnet>
route [aggregate | no_aggregate]
size [1-4096]
state [public | private]
```

Modifies IP pool parameters set using the `add ip pool` command.

Parameter	Description
<pool name>	Designation of the IP pool. Limit: *16 ASCII* characters.
initial_pool_address/subnet_mask	First IP address to be assigned from the specified pool, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The mask specifier can be 'A, 'B, 'C, 'H, or a numeric value from 8 to 30 (32 for host) that describes the number of one bits in the mask. If you do not specify a mask, the RAS 1500 generates the natural netmask from the *initial_pool_address*.
route	Broadcasts the pool as a single network (aggregate) instead of individual host routes (no_aggregate). Default: No_aggregate.
size	Number of allowable IP addresses. Class C values exceeding x.x.x.255 increment to x.x.1.1. Default: 1. Range: 1-4096.
state	Type of pool created. A *public* pool allocates IP addresses to any caller not assigned a pool. A *private* pool is limited to specified users. Default: Public.

set ip route <IP_hostname or network address>

```
gateway <host name or IP station address>
metric <1-15>
```

Modifies the IP route created using the `add ip route` command.

Parameter	Description
<IP hostname or IP network address>	IP address or host name of the remote destination, in the format *nnn.nnn.nnn.nnn*, entered *with* or *without* a mask specifier. The mask specifier can be A, B, C, or H (host), or 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 self-generates it (based on the network address) for all routes except *host* routes, for which you *must* specify a mask. For help counting the bits, see *Appendix C,* "Addressing Schemes" for a handy bitmask table.
gateway	Host name or IP address of the next hop to the specified IP network address.
metric	Number of hops the destination is removed from the specified IP network address. Range: 1-15.

set ip routing

```
autonomous_system_number [number]
metric_maximum_entries [number]
rip_flags [metrics, send_request]
router_id [IP_address]
```

Sets global parameters for IP routing on the specified IP router address that serves as the gateway to an autonomous system.

IP routing must be disabled before setting these values.

An autonomous system is a connected group of networks run by one or more network operators that has a single and clearly defined routing policy. An autonomous system number is a unique identifier for such a system, but is not currently supported by the RAS 1500. The *maximum* number of IP routes that can be contained in the Routing Table is *10.*

Parameter	**Description**
autonomous_system_number	Value associated with a protocol not currently supported. Disregard this value. Range: 1-65535.
metric_maximum_entries	Most next hop entries the Next Hop Hash Table can hold. Default: 512. Range: 256-65535.
router_id	IP address of the RAS 1500. If the value is not specified, the system uses a user-configured **internal** IP address for this value, or the **eth:1** value if no internal value is specified.
rip_flags	Flags indicate at which level a RIP instance is disabled or configured. Choices: ■ **Metrics** - Specifies how to increment metrics using RFC1058. ■ **Send_request** - Sends a RIP request for routing data when an interface first comes up.

set ipx network <network_name>

```
delay_ticks [number]
diagnostics [disable | enable]
maximum_learning_retries [number]
netbios [enable | disable]
netbios_cache_timer [seconds]
netbios_max_hops [number]
netbios_name_cache [disable | enable]
packet_maximum_size [number]
rip [auto_off | auto_on | on | off]
rip_age_multiplier [number]
rip_broadcast [enable | disable]
rip_gap_timer [number]
rip_packet_size [number]
rip_periodic [disable | enable]
rip_update_interval [number]
sap [auto_off | auto_on | on | off]
sap_age_multiplier [number]
sap_broadcast [enable | disable]
sap_gap_timer [number]
sap_nearest_replies [on | off]
sap_packet_size [number]
sap_periodic [enable | disable]
sap_update_interval [number]
```

Sets configuration of the specified IPX network created with the `add ipx network` command.

Parameter	Description
<network_name>	Designation of the IPX network. Maximum size: 64 characters.
delay_ticks	Interval in number of ticks it takes to reach this IPX network. Default: 1 for LAN networks, 40 for WAN networks. Range: 0 -65535.
diagnostics	Whether to send diagnostic packets to this IPX network. Default: Enabled.
maximum_learning_retries	Number of times this network resends packets to learn its directly connected neighbors. Default: 0.
netbios	Whether to support NetBIOS on dial-out IPX networks. Default: Enabled.
netbios_cache_timer	Interval a NetBIOS system is kept in the cache. Default: 60 seconds.
netbios_name_cache	Whether to cache a list of the other NetBIOS systems on this IPX network. Default: Disabled.
netbios_max_hops	Maximum number of hops this network makes to locate a NetBIOS system. Default: 8**.** Range: 0 - 65535.
packet_maximum_size	Maximum size packet this IPX network supports. Max size: 1600 bytes.
rip	Turns RIP: on**,** off**,** auto_on or auto_off for this network. Default: On.
rip_age_multiplier	Number to multiply the rip_update_interval by, to obtain the value for the aging out the entries in the RIP database. Default: 3.
rip_broadcast	Enables/disables RIP broadcasts. Default: Enabled.
rip_gap_timer	Interval the system waits between sending RIP packets. Default: 1.
rip_packet_size	Size of RIP packets. Default: 446 bytes.
rip_periodic	Enables/disables sending of RIP periodic updates. Default: Enabled.
rip_update_interval	How often RIP should send periodic updates. Range: 1-500 seconds. Default: 60 seconds.
sap	Turns SAP: on**,** off**,** auto_on or auto_off for this network. Default: On.
sap_age_multiplier	Number to multiply the sap_update_interval by, to obtain the value for aging out entries in the SAP database. Range: 1-1080. Default: 3.
sap_broadcast	Enables, disables SAP broadcasts. Default: Enabled.
sap_gap_timer	Interval the system should wait between sending SAP packets. Default: 1.

Parameter	Description

sap_nearest_replies	Whether SAP looks for its nearest neighbors. Default: *YES*.
sap_packet_size	Size of SAP packets. Default: *510 bytes*.
sap_periodic	Enables/disables sending of SAP periodic updates. Default: *Enabled*.
sap_update_interval	How often RIP should send periodic updates. Range: 1-500 seconds. Default: 60 seconds.

set ipx system

```
default_gateway [ipx_host_address]
initial_pool_address [ipx_network_address]
max_hops [number]
name [string]
number [internal network number]
pool_members [number]
```

Sets parameters for dynamic IPX networks. The maximum number of hops allowed in *15*.

Parameter	**Description**
default_gateway	Default router for the dynamic IPX network.
initial_pool_address	First IPX address used to dynamically assign IPX network.
max_hops	Greatest number of hops this network makes to locate an IPX system. Range: 1-64.
name	Designation for the dynamic IPX network.
number	Network address for the dynamic IPX network. This value is required to run various IPX services. See `add ipx service` command for more information.
pool_members	Number of addresses to reserve in the pool of IPX addresses used when dynamically assigning IPX networks. Range: 1-4096.

set login_host preference <preference_ number>

```
rlogin_port [port_number]
telnet_port [port_number]
clearTCP_port [port_number]
```

Sets rlogin, Telnet, or ClearTCP ports for a specified login host. The specified port number is used by the login host to accept connections using that method.

Parameter	Description
<preference_number>	Defines preferred rank in which a login host is used (from first preference of 1 to least preference of 10). Use `list login_hosts` to see the preference number associated with a login host.
rlogin_port	TCP port number you wish to configure for RLOGIN access to the login host. If you do not specify it here, and the user does not specify the TCP port from the CLI `rlogin` command, the default is 513. Limit: 65535**.** Default: 513.
telnet_port	TCP port number you wish to configure for Telnet access to the login host. If you do not specify it here, and the user does not specify the TCP port from the CLI `telnet` command, the default is 23. Limit: 65535**.** Default: **23**.
clearTCP_port	TCP port number you wish to configure for ClearTCP access to the login host. There is no default TCP port number. Limit: 65535**.** Default: 6000.

set modem_group <name>

```
access [dial_in | dial_out | two_way]
clid security [off | on]
connection_type [direct_conn | direct_net | no_prompt |
normal | prompt_user_only]
dial_prefix <string>
host_addresss <ip_address or address>
host_type [prompt | select | specified]
init_script <init_script_name>
login_service [cleartcp | rlogin |telnet]
message <string>
password <password>
prompt <string>
protocol [arap | PPP | slip]
tcp_port <port>
type [login | login_network | network]
user_name <user_name>
```

Configures a previously defined modem group. All the interfaces in the specified modem group are configured with this one command.

Note: *All the parameters that can be set with this command can also be configured using* `set switched interface`*, but this command sets multiple interfaces with one command. Issue the* `show interface settings` *command to view configuration.*

***Note:** Parameters set with this command are associated with the specified interface, not the modem group. Be aware that when you change parameters of interfaces assigned to multiple modem groups, the last change you make to a group containing any associated interface reflects the latest configuration.*

***Note:** When setting connection type, be aware that the direct_net parameter does not support the SLIP protocol. Direct_net requires the use of a negotiated protocol, which SLIP is not.*

Parameter	**Description**
<group_name>	Designation of the modem group. The default modem group is *all*. Limit: *64 ASCII* characters.
clid_security	Enables/disables security for calling line ID for a particular modem group. Default: *off*
access	Sets access type for switched interface. Modem can allow *dial-in*, *dial-out*, or *both* (two-way). Default: *two-way*
connection_type	Sets the connection type for switched interface. Options: ■ *Direct_net* — Uses the protocol parameter setting to create a **network** (virtual node) connection. Employs *username* and *password* specified in this command. Authentication is done by the network protocol such as PPP. Direct_net *does not support* the SLIP protocol. ■ *Direct_conn* — Employs *username* and *password* specified in this command to establish a *login* type connection to the target host. Authentication is accomplished by the target host. If username and password are *not* specified with this choice, user "*default*" is employed. ■ *Normal* — Prompts for both *username* and *password*. *Default*. ■ *Prompt_user_only* — Prompts for *username* only and authenticate with the *password* specified in this command. ■ *No_prompt* — Does not prompt. Authenticates with the *username* and *password* specified in this command. If username and password are **not** specified with this choice, user "*default*" is employed.
dial_prefix	Prefix added to all phone numbers g from this port. Limit: *64 ASCII* characters.
host_address	IP address to connect a dial-in user to, if the host type is specified and connection type is direct_conn or direct_net.

host_type	Identifies how dial in connection is set up. The options are the following: ■ *prompt* — prompted to enter host name or address. *Default*. ■ *select* — a host is chosen from a login host list you specify, configured by the set connection command. ■ *specified* — connected to IP address configured here.
init_script	Name of modem initialization script used. Maximum size: *7 ASCII characters*. If you are setting an init_script for a Modem Pool or Interface the init_script name must already exist. A null string (**“”**) indicates the name is deleted. Default: *USR_int*.
login_service	The login service to use, if the connection type is not direct_net. Options: ■ *Telnet***.** *Default*. ■ *RLOGIN*. ■ *ClearTCP*. ■ *Ping* **— U**ser pings a login host, receives a successful/unsuccessful message and is disconnected.
message	String to display to a dial-in user when connection is set. Limit: *64 ASCII* characters. You can use *$value* to stipulate more parameters in the message line for identification purposes. ■ *$date* - current date according to system uptime. ■ *$callid* - user call identification according to system uptime. ■ *$port* - port occupied by user. The format of each port is *x*/slot:*y*/mod:*z*. where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit; pau0 for the PAU), *y* is the slot number, and *z* is the port (modem) number, for example, rm0/slot:1/mod:1,pem0/slot:1/mod:2. ■ *$hostname* - user host name. ■ *$sysname* - user system name (same as hostname). ■ **$time** - time of call according to system uptime. Note: The message, if it includes spaces, *must* be enclosed in quotations. Use the `show user` command to view the message as configured. See Chapter 2, “Administrative Tools,” for more information.
password	Parameter used if the connection type is no_prompt or prompt_user_only. Limit: *63 ASCII characters*.
prompt	String to present the dial-in user. Limit: *256 ASCII characters*.
protocol	Protocol to connect with, if the connection type is direct_net. SLIP is not supported by direct_net connection type. Default: *PPP*.
TCP_port	TCP port number for the login host. Parameter used when connection type is *direct_conn* or *direct_net*. Limit: *65535*.

type	Specifies type of connection allowed on interface. ■ *Login* port only allows login users. ■ *Network* port only allows network users. ■ ***Login_network*** allows either type. *Default*.
user_name	Designation for the switched interface, used if connection type is no_prompt. Limit: *64 ASCII characters*.

set network service <admin_name>

```
close_active_connections [true | false]
data [string]
server_type [service_name]
socket [socket_number]
```

Sets parameters for network services you configured with the `add network services` command. You can list the configured network services using `list network services`. Service must first be *disabled* for this command to work. For DialOut service, the only Data value supported is *modem_group (*and this value *must* be used when implementing DialOut service). See `add network services` command for more information on Data parameters.

Parameter	**Description**
<admin_name>	Designation you assigned to network service with the add network service command. Limit: *64 ASCII characters*.
close_active_ connections	Indicates whether to close any active connections when a service is shut by `disable network_service`.Default: *False*.
data	Telnet and ClearTCP Ancillary Data. This field contains server-specific configuration data. See table that lists the configurable ancillary data parameters in the `add network service` command.
server_type	Type of network service you wish to assign to this administration name. Available services: ■ *ClearTCPD* - daemon enables access to a modem group on socket 0. Uses TCP. ■ *DialOut* - supports dial-out connections to IP hosts on socket 32773. Uses TCP. ■ *SNMPD* - daemon supports SNMP on socket 161. Uses UDP. ■ *TFTPD* - daemon supports file transfer service on socket 69. Uses UDP. ■ *TELNETD* - daemon supports Telnet, either to the CLI or a modem group on socket 23. Uses TCP.

socket	The port the server listens on. For TFTP, Telnet, and ClearTCP, it is the TCP or UDP port number. Socket numbers are the joined sender (or receiver) IP address and service type port number. Range: 0-65535.

set packet_logging

```
logging [all | radius | none]
packet_size [0-493 bytes]
```

Sets parameters to generate SYSLOG messages for filtered packets. Facility can be configured globally, for specific users who have the Log-Filter-Packet attribute set in the Access-Accept RADIUS configuration or not at all. Use the `show packet_logging` command to view settings.

Parameter	Description
logging	Specifies type of logging generated: ■ *All* - all filtered packets generate a SYSLOG message. ■ *Radius* - the RADIUS attribute, Filter-Log-Packet, to control SYSLOG message generation for a specified user. ■ *None* - no SYSLOG messages are generated. *Default*.
packet_size	Specifies the size of a filtered packet that is included in the actual SYSLOG message. When set to zero (0), the size feature is turned off, causing the entire packet to be included in the SYSLOG message. Default: 0. Range: 0-493 bytes.

set ping maximum_rows <rows in table>

Sets maximum number of rows permissible in the Remote Ping Table. Setting this parameter to a number smaller than the current number of rows causes future row deletions, not immediate. Use the `show ping settings` command to view configuration. Default: 20. Range: 1-1000.

set ppp

```
system_dns_usage <on | off>
nbns_primary <ip address>
nbns_secondary <ip address>
receive_authentication [none | pap | chap | either]
```

Sets global parameters for PPP, which applies to all calls including the call type for which PPP compression is attempted/accepted. Issuing this command overrides the *compression algorithm* parameter set by the `set network user <name> ppp` command.

Users who dial in and receive a compressed_analog connection (MNP5 or V.42bis) do not receive PPP compression. Payload compression is set by the parameter, not header compression as set for a user.

Parameter	Description
system_dns_usage	Enables/disables the RAS 1500 to supply clients with DNS server addresses used in IPCP negotiation. Default: *On*.
nbns_primary	IP address of the primary NetBIOS name server.
nbns_secondary	IP address of the secondary NetBIOS name server.
receive_authentication	The authentication protocol the RAS 1500 uses to authenticate its PPP peer (the peer can employ a protocol of its choice). This value works in conjunction with *authentication_preference*. If the *Any* or *Encrypted_any* value is selected, the authentication protocol tried first from the group can be selected by specifying the *authentication_preference* parameter. Note the following choices: - If *receive_authentication* is set to *any*, *authentication_preference* can be set to Challenge Handshake Authentication Protocol (*CHAP), MS_chap, EAP, proxy_eap, Password Authentication Protocol (PAP), or default* (CHAP). - If receive_authentication is set to *any*, *authentication_preference* can be set to *CHAP, MS_chap, EAP, proxy_eap,* or *default* (CHAP). - If *receive_authentication* is set to *any other value*, the *authentication_preference* setting is ignored. Protocols are negotiated in this order of preference: CHAP, EAP, MS_chap, and PAP. Options are the following: - *None* — No user authentication requested. - *PAP* — Only Password Authentication Protoco allowed with peer. - *CHAP* — Only CHAP (MD5) authentication allowed with peer. - *Either* — Any authentication method can be used.

set snmp community <name>

```
access [ro | rw | adm]
address [IP_address]
```

Modifies parameters for an SNMP community (authorized user or host to which notifications are sent) configured with the `add snmp community` command. The community name and IP address of SNMP requests from managers on the network must match the list, which you can view using `list snmp communities`.

Parameter	Description
<community_name>	Group designation for a pool of management stations that authorize SNMP requests.
access	Determines what type of access to SNMP MIBs the added user has. Options are Read Only (*RO*), Read Write (**RW**), and Administrator (*ADM*). Administrator allows *read access to all objects* and *write access to all writeable objects*. *RO* is the default on public (0.0.0.0) networks and *RW* the default on private networks.
address	IP address of this SNMP management station, expressed in the form *nnn.nnn.nnn.nnn*

set switched interface <interface name>

```
access [dial_in | dial_out | two_way]
at_command <string>
clid_security [off | on]
connection_type [direct_conn | direct_net | no_prompt |
normal | prompt_user_only]
dial_prefix <string>
filter_access [off | on]
host_address <IP_name or address>
host_type [prompt | select | specified]
init_script <init_script_name>
input_filter <filter_name>
login_service [cleartcp | rlogin | telnet]
message <string>
output_filter <filter_name>
password <password>
prompt <string>
protocol [arap | ppp | slip]
tcp_port <port>
type [login | login_network | network]
user_name <user_name>
```

Configures port parameters for the specified switched (modem) interface (for example, rm0/slot:2/mod:1). To display the switched interfaces you have configured, use the `list switched interfaces` command. To view settings for a particular interface, use the `show interface settings` command.

When setting connection type, be aware that the direct_net parameter does not *support the SLIP protocol. Direct_net requires the use of a negotiated protocol, which SLIP is not.*

Parameter	**Description**
<interface_name>	The switched interface to modify. Limit: *64 ASCII characters*. You can specify multiple interfaces in one command. The format of the list is the following: `set switched interface <interface 1>,<interface 2>,...` The format of each modem interface is the following: *x*/slot:*y*/mod:*z* where *x* is the type of unit (rm0 for the RAS 1500 unit, pem0, or pem1 for the RAS 1500 Expansion Unit, and pau for the PAU), *y* is the slot number, and *z* is the modem number, for example, rm0/slot:1/mod:1,pem0/slot:1/mod:2 Enter interfaces from the same slot in ranges. Example: rm0/slot:1/mod:[1-4],pem0/slot:1/mod:[1-4] Example: **`set switched interface rm0/slot:1/mod:1,pem0/slot:1/mod:1`**
access	Sets access type for switched interface. The modem can allow dial-in only, dial-out only, or both (TWO-WAY). Default: *Two-way*.
at_command	String representing any generic AT command. When implemented, output is shown immediately on CLI. See Appendix A, “Modem Command Reference”, for AT command information.

connection_type	Sets connection type for switched interface. Options: ■ *Direct_net* — Uses the protocol parameter setting to create a *network* (virtual node) connection. Employs *username* and *password* specified in this command. Authentication is done by the network protocol such as PPP. Direct_net *does not support* the SLIP protocol. ■ *Direct_conn* — Employs *username* and *password* specified in this command to establish a *login* type connection to the target host. Authentication is accomplished by the target host. If username and password are **not** specified with this choice, user "*default*" is employed. ■ *Normal* — Prompts for both *username* and *password*. *Default*. ■ *Prompt_user_only* — Prompts for *username* only and authenticate with the *password* specified in this command. ■ *No_prompt* — Does not prompt. Authenticates with the *username* and *password* specified in this command. If username and password are *not* specified with this choice, user "*default*" is employed.
dial_prefix	Prefix added to all phone numbers dialing from this port. Limit: *7 characters*.
filter_access	Turns filtering ON or OFF. Default: *Off*.
host_address	IP address to connect a dial-in user to, if the host type is specified, and connection_type is direct_conn or direct_net.
host_type	Identifies how connection is established. Dial-in user is the following: ■ *Prompt* — Prompted to enter a host name or address. ■ *Select* — Connected to a login host, selected from the list of login hosts, determined by the host_select field in the *set connection* command. *Default*. ■ *Specified* — Connected to the configured IP address.
init_script	Name of modem initialization script used. Maximum size: *7 ASCII characters*. If you are setting an init_script for a Modem Pool or Interface the init_script name must already exist. A null string (**""**) indicates the name is deleted. Default: *USR_int*
input_filter	File name of filter screening incoming data.
login_service	Login service to use if the connection_type is *not* direct_net. Options: ■ *Telnet***.** *Default*. ■ RLOGIN. ■ ClearTCP. ■ *Ping* **— U**ser pings a login host, receives a successful/ unsuccessful message and is disconnected.

message	String to display to a dial-in user when connection is set. Limit: *64 ASCII characters*. You can use *$value* to stipulate more parameters in the message line for identification purposes. ■ *$date* — current date according to system uptime. ■ *$callid* — User call identification according to system uptime. ■ *$port* — port occupied by user. The format of each port is the following: *x*/slot:*y*/mod:*z* where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the port (modem) number. Example: rm0/slot:1/mod:1,pem0/slot:1/mod:2 ■ *$hostname* — User host name. ■ *$sysname* — User system name (same as hostname). ■ *$time* — Time of call according to system uptime. *Note*: The message, if it includes spaces, *must* be enclosed in quotations. Use the `show user` command to view the message as configured. See Chapter 2, “Administrative Tools,” for more information.
output_filter	File name of filter screening outgoing data.
prompt	String to present the dial-in user. Default: *login*. Limit: *64 ASCII characters*.
password	Used if connection_type is no_prompt or prompt_user_only. Limit: *63 ASCII characters*.
protocol	Protocol (PPP) to connect with, if connection type is direct_net. SLIP is not supported by *direct_net* connection type. Default: *PPP*.
tcp_port	TCP port number for login host. Value used for *direct_conn* or *direct_net* connection types. Limit: *65635*.
type	Type of connections to allow on the switched interface. ■ *Login* port allows login users only. ■ *Network* port allows network users only. ■ *Login_network* allows either type. *Default*.
user_name	Designation for the switched interface, used if connection type is *no_prompt*. Limit: *64 ASCII* characters.

set syslog <IP_address>

```
facility [log_auth|log_local0| |log_local1|log_local2 |
log_local3|log_local4|log_local5|log_local6|log_local7]
loglevel [critical|unusual|common|verbose]
```

Sets the error reporting level and the destination for SYSLOG entries that are sent to the specified host. You must have previously defined this syslog IP address using the `add syslog` command.

The text below details an example of a SYSLOG message sent when a PPP user logs in but is unable to authenticate.

```
Jun 17 15:46:37 [149.112.214.100.8.2] At 03:48:17, Facility "PPP",
Level "CRITICAL":: PPP User login attempt failed.
Username: ppp1dgdg, if_name: slot:2/mod:1
```

All SYSLOG messages generated by the *Auth* facility are sent regardless of loglevel set. *All other* RAS 1500 facilities are sent only if their loglevels match the configured syslog loglevel.

The four levels of logging are the following:

- *Critical* — A serious system error that may affect system integrity. *Default.*
- *Unusual* — An abnormal event, which the system should recover from.
- *Common* — A regularly occurring event.
- *Verbose* — A regular periodic event, for example, a routing update message.

Parameter	**Description**
<IP_address>	SYSLOG address where information is directed.
facility	SYSLOG facility where output is sent. See choices above. Default: *log_auth*.
loglevel	SYSLOG loglevel to which output is assigned. See choices above.

Do not confuse `set facility` *and* `set syslog` *commands. The set facility determines which messages are generated on the console or to a telnetted PC — depending on the loglevel specified for each facility. The set syslog command, however, determines which messages are saved — depending on the global loglevel set for the particular SYSLOG host.*

set system

```
name [name]
location [location]
contact [contact information]
transmit_authentication_name [keyword]
```

Specifies system information, displayed using *show system*. The transmit authentication keyword (Limit: *64 ASCII characters*) is used when the RAS 1500 receives a challenge. This is typically during LAN to LAN routing, while making a PPP connection to a remote system/router over the WAN. (PPP requires a user at the data link layer, which you supply here.) *Location*, *name*, and *contact* names are limited to *64 ASCII characters*.

Parameter	**Description**
contact	Name of the RAS 1500 administrator.
location	Site of the RAS 1500.
name	Designation of your RAS 1500.
transmit_authentication_name	Remote account name. *Note*: In LAN-to-LAN connections, this name *must* match the username at the far end of the connection.

set tcp maximum_ connections <number>

Sets the total number of TCP connections that the RAS 1500 can support. TCP services include Telnet and ClearTCP. Range: 0-4096.

set time <time>

Sets the system time in Greenwich Mean Time (GMT) and leaves the date unchanged. Use `show date` to view current settings. The format is the following: hh:mm:ss. The seconds field is optional. The `set date <date> time` command also sets the time.

***Note:** if you are configuring a RAS 1500 in a zone that observes daylight savings time, you **must** set time commands in the following order: 1) set timezone, 2) set dst, and 3) set time.*

set timezone

Sets the number and minutes that your timezone is off from GMT. It must be a time between -12 and +14 and must be in the format HH:MM (hour:minutes).

Set User Commands

Set user commands allow you to change the configuration of the following user profiles.

set user <user_name>

```
alternate_phone_number <phone_number>
callback_delay <0-60>
callback_type [dynamic | normal]
caller_ID1 <phone_number>
caller_ID2 <phone_number>
expiration <date>
idle_timeout <0-86400>
input_filter <filter_name>
message <string>
modem_group <name>
output_filter <filter_name>
password <password>
phone_number <phone_number>
session_timeout <0-86400>
type [login,network,callback,dialout,manage]
```

Modifies parameters most of which were configured by the `add user` command.

Parameter	Description
<user_name>	Name of user, previously defined using add user. Limit: 32 ASCII characters.
alternate_phone _number	Number to dial if the first number is busy. Limit: 33 ASCII characters. Note: This value is overridden when a dial-out script specified in the `set dialout user` command is issued.
callback_delay	The interval between dropping the incoming call and initiating the call-back. Default: 0 Range: 1 - 60 seconds.
callback_type	Type of call-back: - *dynamic* — The call-back phone number changes based on the phone number from which the client called. - *normal* — The call-back phone number does not change.
caller_id1 caller_id2	The number that the ANI of an incoming call must match to allow the call. If there is no match to caller_id1 or caller_id2, the call is dropped. Used when clid security is enabled.
expiration	Date after which this user becomes inactive. The format is the following: DD-MMM-[YY]YY. Month is the first 3 letters of the month. Year is either 2 or 4 digits, for example, 96 or 1996.
idle_timeout	Interval to wait before timing out an inactive connection. Default: 0 (not activated). Range: 1 - 86400 seconds**.** Note: change the default to configure this value.

Parameter	**Description**
input_filter	Designation of the filter file in FLASH memory to be applied to the input datastream.
message	String to display to a dial-in user when connection is set. Limit: *64 ASCII characters*. You can use *$value* to stipulate more parameters in the message line for identification purposes. ■ *$date* — current date according to system uptime. ■ *$callid* — User call identification according to system uptime. ■ *$port* — port occupied by user. The format of each port is the following: *x*/slot:*y*/mod:*z* where *x* is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), *y* is the slot number, and *z* is the port (modem) number. Example: rm0/slot:1/mod:1,pem0/slot:1/mod:2 ■ *$hostname* — User host name. ■ *$sysname* — User system name (same as hostname). ■ *$time* — Time of call according to system uptime. *Note*: The message, if it includes spaces, *must* be enclosed in quotations. Use the `show user` command to view the message as configured. See Chapter 2, “Administrative Tools,” for more information.
modem_group	Name of modem group used to make connection to this *dial-out* user. *Important*: This value does *not* apply to a *dial-in* user.
output_filter	Name of the filter file in FLASH memory to be applied to the output datastream.
password	User password (optional). Limit: *127 ASCII characters*. You may enter a null password with *password* ***“”.***
phone_number	Primary phone number to make the connection. Limit: *33 ASCII characters*. *Note*: This value is overridden when a dial-out script specified in the `set dialout user` command is issued.
session_timeout	Interval before timing out a session. Default: *0* (no setting)

type	Type of user added. A user may be one or more types, but call-back and dial-out are mutually exclusive. ■ *Login* users are TCP users who use the login_service specified. ■ *Network* users are framed protocol users, who use the network_service specified. ■ *Call-back* users disconnected after authentication and called back. ■ *Dial-out* users are either modem sharing users or WAN connection users. ■ *Manage* users with system administration authority.

set dialout user <user_name>

```
local_IP_address [IP_network_address]
reply1_script [“string”]
reply2_script [“string”]
reply3_script [“string”]
reply4_script [“string”]
reply5_script [“string”]
reply6_script [“string”]
send1_script [“string”]
send2_script [“string”]
send3_script [“string”]
send4_script [“string”]
send5_script [“string”]
send6_script [“string”]
```

Sets parameters for dial-out users, both WAN and modem. Send scripts are useful under the following conditions:

- **Dial-out sites** — User dials out to a remote location and is connected or prompted for a login.
- **Dial-in/dial-out** — User dials in to the RAS 1500, then dials out to a remote site and is connected.
- **Telnet/dial-out** — User telnets into the RAS 1500, then dials out to a remote site and is connected as a *shared_modem* user.

Script strings are limited to 240 characters that must be enclosed in *double quotes* if they exceed 64 ASCII characters.

These values override phone or alternate phone numbers specified in the `set user` *command.*

Parameter	Description
<user_name>	Name of user, previously defined using `add user` command with dial-out as the type. Limit: *32 ASCII characters*.
local_IP_address	IP address of the user making an IP connection over this dial-out interface.
send & reply scripts	Specify commands required to establish and terminate the remote connection. Scripts must be enclosed in double quotes if more than *64 ASCII characters*. Limit: *240 ASCII characters*.

set dialout user <username> site

```
address_selection [assign | negotiate | specified]
appletalk [enable | disable]
bridging [enable | disable]
default_route_option [enable | disable]
end_time [time]
ip [enable | disable]
ipx [enable | disable]
ipx_address [IPX_address]
range_appletalk_address [1-65279]
remote_ip_address [IP_name or network address/mask_specifier]
send_password [string]
spoofing [enable | disable]
start_time [time]
type [ondemand | timed | continuous | manual]
```

Sets parameters for dial-out users connecting to a remote network.

Parameter	Description
<username>	Name user, previously defined using add user with dial-out as the type. Limit: *32 ASCII characters*.
address_selection	Determines how the IP address is assigned for incoming (client) IP network connections. ■ *Negotiate* — brokers IP address between remote client and local user. ■ *Assign* — chooses address from IP pool, configured using *set ip system*. *Default*. ■ *Specified* — *must* use IP address set in *remote_IP_address* value.
appletalk	Indicates whether the connection supports Appletalk. Set to either Enable or Disable. Default: Enable.

bridging	Indicates whether the connection supports bridging. Set to either Enable of Disable. Default: Enable.
default_route_option	Automatically sets the IP address of a remote default router by negotiation. This parameter takes precedence over a default route (gateway) set by `add framed_route user` or `add ip defaultroute` commands, which require manual IP address entry. Default: Disable.
end_time	For a TIMED user, specifies when to tear down connection. Seconds field is optional.
ip	Determines if this connection supports IP or not. Default: Enable.
ipx	Determines whether this connection supports IPX or not.
ipx_address	The address of the remote network.
range_appletalk_ address	The range of valid Appletalk addresses. Range: 1-65279. Default: 0-0.
remote_IP_address/ mask_specifier	For a remote IP connection, the IP network address assigned to the client, in the format *nnn.nnn.nnn.nnn*, with or without a mask specifier. The mask specifier can be in IP address format (*255.0.0.0* or greater and contiguous) or *A, B, C*, or a numeric value from 8 to 30 that describes the number of one bits in the mask. If setting a user IP address, the mask specifier is set to *H* (for Host) or a numeric value of *32*. If you do not specify a mask, the system generates it for you from the network address. Default: *0.0.0.0./H*.
send_password	Password sent to remote network. *Note*: Passwords you defined with other commands are for dial-in users. Limit: *63 ASCII characters*.
spoofing	Specifies spoofing across the remote connection, to save overhead on the dial-out line connection. Default: *Disable*.
start_time	Period to start a TIMED connection. Seconds field is optional.
type	Describes what type of dial out connection this is: ■ *Ondemand* — makes connection when the system seeks a session with the remote network. ■ *Timed* — makes connection at a set time. ■ *Continuous* — always keeps connection up. ■ *Manual* — starts connection manually with CLI. *Default*

set framed_route user <name>

```
gateway [IP_address]
ip_route [IP_address]
metric [number]
```

Specifies a framed (static) network to the user profile for dial-up connections. See also `add framed_route user` and `add ip route` commands.

Parameter	Description
<username>	Username specified for the framed network.
gateway	IP address of the gateway used to reach this remote network.
ip_route	IP address of the remote network.
metric	Integer representing how far away the route is, in “hops” from other routers. Range: 1-15.

set login user <username>

```
host_type [prompt | select | specified]
login_host_ip_address [IP_ name or address]
login_host_name [IP_ name or address]
login_service [rlogin | telnet | cleartcp | ping]
tcp_port [number]
terminal_type [string]
```

Sets parameters for users whose type is LOGIN.

Parameter	Description
<username>	User to set parameters for, earlier defined using add user with login as type. Limit: *32 ASCII characters*.
host_type	Options are the following: ■ *Prompt* — Dial-in user is prompted to enter an IP host or address. ■ *Select* — User is connected to a host, which is chosen from the list of login hosts you defined using `add login_host`. The method of selecting the host is set using the `set connection` command (RANDOM or ROUND ROBIN). *Default*. ■ *Specified* — Dial-in user connects to the login host set by the *login_host_ip_address* of this command.
login_host_IP_address	IP address or host name of the remote host.
login_host_name	Designation of host to be resolved at time of connection.
login_service	Service used to login to the remote host. Choices: ■ Rlogin. ■ *Telnet. Default*. ■ ClearTCP. ■ *Ping* **— U**ser pings a login host, receives a successful/unsuccessful message and is disconnected.
tcp_port	TCP Port number the remote host expects this login to use. Limit: *65535*.
terminal_type	Terminal type used for the remote connection, for example, VT100. Limit: *64 ASCII characters*.

set network user <name>

```
address_selection [assign | negotiate | specified]
appletalk [disable | enable]
bridging [diable | enable]
default_route_option [disable | enable]
filter_zones [disable | enable]
header_compression [none | tcpip]
ip [disable | enable]
ip_routing [both | listen | none | send]
ipx [disable | enable]
ipx_address [address]
ipx_routing [all | listen | none | respond | send]
ipx_wan [disable | enable]
mtu <0-8192>
nat_option [disable | enable]
network_service [arap | fcp | fcp | fr_1490 | ppp |slip]
pat_default_address <ip_address>
range_appletalk_address <ap_add_range>
remote_ip_address <Ip_name or net_address
rip [ripv1 | ripv2]
rip_authentication_key <string>
rip_policies_update <rip_policies>[send_default | send_routes
| send_subnets | accept_default | split_horizon |
poison_revere | flash_update | send_compat | ripv1_receive |
ripv2_receive | silent]
send_password <password>
spoofing [disable | enable]
transmit_authentication <name>
```

Specifies parameters for IP users whose *type* is network.

Parameter	Description
name	name of the user, whose type must be **network**.
address_selection	Specifies the method by which an IP address is assigned to the client: ■ *assign* — Selects addresses from the IP address pool. ■ *negotiate* — Brokers an IP address between the local remote client and the RAS 1500. This option is not available with SLIP. ■ *specified* — The administrator sets the IP address, using the `remote_ip_address` parameter.
appletalk	Enables or disables the AppleTalk protocol. Default: *Enable*.
bridging	Enables or disables bridging. Default: *Enable*.

default_route_option	Enables or disables the default route option. If enabled, the system sets the IP address of a remote default router by negotiation. This parameter takes precedence over a default route set by the `add framed_route user` or `add ip defaultroute` command. Default: *Disable*.
filter_zones	Enables or disables filtering for AppleTalk zones. Default: *Enable*.
header_compression	Sets TCP/IP compression or no header compression. Default: *TCPIP*.
ip	Enables or disables IP. Default: *Enable*.
ip_routing	Sets IP routing options: ■ *Listen* — Listens for RIP packets destined for networks. ■ *Send* — Sends RIP packets destined for the remote network. ■ *Both* — Listens for RIP packets destined for networks and sends RIP packets to the remote network. ■ *None* — Ignores all RIP packets. This is the default setting.
ipx	Enables or disables IPX. Default: *Enable*
ipx_address	Sets the address of the IPX remote network. When configuring for an unnumbered IPX network, set this value to *fffffffc*. Default: *00000000*
ipx_routing	Sets IPX routing options: ■ *Listen* — Listens for RIP/SAP packets destined for networks. ■ *Send* — Sends RIP/SAP packets destined for remote networks. ■ *Respond* — Replies to requests with RIP or SAP data. This is the default setting. ■ *All* — Listens, sends, and responds with RIP/SAP packets. ■ *None* — Ignores all routing packets.
ipx_wan	Enables or disables a negotiation protocol for IPX networks. If enabled, two IP networks use this protocol to negotiate an IPX network number for the WAN connection. Default: Disabled.
mtu	Maximum Transfer Unit - largest data packet size (bytes) allowed. Default: 1514. Range: 64-8192.
network_service	Type of network service. Default: PPP.
ppp	See the `set network user <name> ppp` command, below.
range_appletalk_address	Sets the AppleTalk network address range. Range: 0-65279.

remote_ip_address	For a remote IP connection, the IP network address assigned to the client, in the format *nnn.nnn.nnn.nnn*, with or without a mask specifier. The mask specifier can be in IP address format (*255.0.0.0* or greater and contiguous) or *A, B, C*, or a numeric value from 8 to 30 that describes the number of one bits in the mask. If setting a user IP address, the mask specifier can also be H (for Host) or a numeric value of *32*. If you do not specify a mask, the system generates it for you from the network address. Default: *0.0.0.0./H*.
rip	Specifies the RIP, either RIPV1 or RIPV2. Default: *RIPv1*.
rip_authentication_key	Authorizes RIP updates using a stored password. Maximum string length: *64 ASCII characters*.
rip_policies_update	Allows user to enable or disable RIP policies. See below for a description of keywords. A keyword with “NO_**”** preceding it disables the policy. The default is indicated by (*D*). *Note*: For Poison Reverse to work properly, Split Horizon must also be enabled. SEND_DEFAULT/NO_SEND_DEFAULT(D) SEND_ROUTES(D)/NO_SEND_ROUTES SEND_SUBNETS/NO_SEND_SUBNETS(D) ACCEPT_DEFAULT/NO_ACCEPT_DEFAULT(D) SPLIT_HORIZON(D)/NO_SPLIT_HORIZON POISON_REVERSE(D)/NO_POISON_REVERSE FLASH_UPDATE(D)/NO_FLASH_UPDATE SEND_COMPAT(D)/NO_RIPV1_SEND RIPV1_RECEIVE(D)/NO_RIPV1_RECEIVE RIPV2_RECEIVE(D)/NO_RIPV2_RECEIVE SILENT (default is disabled)
send_password	Password sent to the remote network. Limit: **1***5 ASCII characters*.
spoofing	Spoofing across remote connect to save overhead on dial-out line. Default: *Disabled*.

set network user <user_name> fcp

```
channel_expansion <percent>
compression_algorithm [none | stac]
max_channels <number>
```

Sets parameters for users whose *type* is network and who connect over an interface running fcp.

Parameter	Description
<username>	Name user, previously defined using add user with network as the type. Limit: *32 ASCII characters*.
channel_expansion	When the line usage of the first channel exceeds this percentage, FCP adds the second channel. Specifying 100% disables the second and additional channels.
compression_ algorithm	Determines whether compression is negotiated on this FCP link.
max_channels	Sets how many channels to use for FCP.

set network user <username> ppp

```
channel_decrement [percent]
channel_expansion [percent]
compression_algorithm [ascend | auto | microsoft | none |
stac]
expansion_algorithm [constant | linear]
max_channels <0-38>
min_size_compression <0-2048>
nbt_keepalive_timeout <0-65536>
receive_acc_map <hex_number>
reconnect_type [master | peer | slave]
reserve [enable | disable]
reset_mode_compression [auto | every_packet | every_error]
spoofed_protocols
suspend_timer [0-65536]
transmit_acc_map <hex_number>
```

Sets parameters for users whose *type* is network and who connect over an interface running MLPPP. Adding a network PPP user to the User Table *automatically* enables MLPPP, which serves to group multiple links into a bundle to combine the communications capacity of both links. This applies to ISDN service, where there are two bearer channels, and your provider allows combining both channels on demand.

Since default values for channel decrement and expansion are 0, *to employ ondemand allocation, change the settings to suit your anticipated bandwidth traffic. We recommend settings of* 20 (decrement) *and* 60 (expansion).

To ensure MLPPP is up on both ends of the connection, do not change the max_channels default value of 2, *otherwise MLPPP may fail.*

Parameter	**Description**
<username>	Name user, previousl**y defined using add user with network as the type. Limit:** 32 ASCII characters.
channel_decrement	When line usage on the second channel drops below this percentage, PPP drops the second or more channel. Default: 0. Recommended: 20. Range: 1-100%.
channel_expansion	When the line usage of the first channel exceeds this percentage, PPP adds the second channel. Specifying 100% disables the second and additional channels for MLPPP. Default: 0. Recommended: 60**.** Range: 1-100%.
compression_algorithm	Specifies the proprietary compression algorithm PPP uses via negotiation. Choices: *ASCEND*, *MICROSOFT*, *STAC*, and *NONE*. Default: *AUTO***.** *Note*: This value can be *overridden* by using the `set ppp ccp_modemtype` [digital,compressed_analog, uncompressed_analog, none, all] command. If you know the type of traffic your connection handles, using this command is beneficial.
expansion_algorithm	Specifies which type of expansion algorithm to handle bandwidth allocation. ■ *CONSTANT* — A long-term measurement and allocation of traffic bandwidth best for constant datastreams, such as file transfer. *Default*. ■ *LINEAR* — A short-term measurement and allocation of traffic bandwidth. This is best for bursty traffic, such as interactive users.
max_channels	Sets how many channels to use for MLPP. This value either invokes PPP to negotiate for MLPPP with the remote system (*more than 1*) or does not try to negotiate for MLPPP (*1*). The actual number of channels used is determined by channel_decrement and expansion parameters. MLPPP is on by default with a value of *2*. *Note*: To ensure that MLPPP is running on both ends of a connection, do not lower the default value of 2, otherwise MLPPP may fail.
min_size_compression	Data packet size that PPP decides is big enough to start compression. Smaller data packets are not compressed. Range: 0-2048 bytes. Default: 256.
nbt_keepalive_timeout	
receive_acc_map	Determines whether the system uses the asynchronous control character map to filter out incoming data. Default: 000000.
reconnect_type	
reserve	
reset_mode _compression	Determines how often PPP examines packets to decide when to renegotiate the optimum compression algorithm. Default: *AUTO*.

Parameter	Description
spoofed_protocols	
suspend_timer	
transmit_acc_map	Determines whether the system uses the asynchronous control character map to filter out outgoing data. Default: *FFFFFFFF*.

Show Commands

Display detailed information about a specific table entry or a set of scalars (nontable items).

show accounting or show accounting settings

Displays RADIUS accounting settings. You can modify these using the `set accounting` command.

- *Use Servers* — Specifies how accounting information is sent to the accounting servers.
- *Primary Server* — IP address of the primary accounting server.
- *Primary Server Port* — Destination port of the primary accounting server.
- *Secondary Server* — IP address of the secondary accounting server.
- *Secondary Server Port* — Destination port of the secondary accounting server.
- *Retransmission Timeout* — Number of seconds between retransmissions.
- *Retransmissions* — Maximum number of times to retransmit packets to accounting servers if transmissions fail.
- *Accounting Start Time* — Point at which accounting begins.

```
ACCOUNTING SETTINGS:
Use_Servers                           BOTH
Primary Server is:                    134.125.211.10
Primary Server Port is:               1646
Secondary Server is:                  134.125.211.20
Secondary Server Port is:             1646
Retransmission  Timeout:              60
Max Retransmissions                   100
Accounting Start Time                 CONNECTION
Status is:                            ENABLED
```

show accounting counters

Displays statistics stored by RADIUS accounting servers.

- *Number Of Local Users* — Number of LAN users RADIUS is tracking.
- *Number of Active Users* — Sum of users RADIUS is tracking.
- *UDP Packets Received* — Number of packets received from RADIUS.
- *UDP Packets Retransmitted* — Number of packets sent to RADIUS.

```
ACCOUNTING COUNTERS:
Number Of Local Users:                              12
Number of Active Users:                             0
UDP Packets Received:                               0
UDP Packets Retransmitted:                          0
```

show appletalk counters

Displays current settings for AppleTalk, which you can modify using the `set appletalk` command. It displays the following:

- *Table Lookups* — Number of times a node performed an address lookup in its address mapping table.
- *Table Hits* —
- *Queries Received* —
- *Replies Received* —
- *Extended Replies Received* —
- *Zone Conflict Errors* —
- *Obsolete Packets Received* —
- *Lookup Requests Received* —
- *Zone Conflict Errors* —
- *Zone Conflict Errors* —

```
APPLETALK AARP COUNTERS
Table Lookups                                  0
Table Hits                                     0
Queries Received:                              0
Replies Received:                              0
Extended Replies Received:                     0
Zone Conflict Errors:                          0
Obsolete Packets Received:                     0
NBP COUNTERS
Look Up Requests Received:                     0
```

```
APPLETALK AARP COUNTERS
Look Up Replies Received:                  0
Broadcast Requests Received:               0
Forward Requests Received:                 0
Look Up Replies Sent Out:                  0
Registration Failures:                     0
Input Errors:                              0
ECHO COUNTERS
Requests:                                  0
Replies:                                   0
Requests Sent Out:                         0
RTMP COUNTERS
Requests Sent Out:                         0
Version Mismatches:                        0
Errors Received:
```

show appletalk or show appletalk settings

Displays current settings for AppleTalk, which you can modify using the `set appletalk` command.

Example:

```
APPLETALK SETTINGS:
ARAP:
ON
Max ARAP Sessions:                               16
Max Compressed ARAP Sessions:                    16
ARAP Zone:
ARAP Node Net Range:                             0 -0
Max ARAP Nodes Reserved:                        16
Min ARAP Nodes Reserved:                         0
Allow ARAP Password Change:                      TRUE
Max Password Length:                             16
Min Password Length:                             4
Number of ARAP Password Retries:                 16
Force Manual ARAP Password Entry:               FALSE
Max Routing Table Size:                          256
Max Forwarding Table Size:                       256
```

show authentication or show authentication settings

Displays the RADIUS and local user authentication settings, which you can modify using the `set authentication` command. It lists the following:

- *Local Authentication is — Enabled* (default)/*Disabled.*
- *Remote Authentication is — Enabled* (*default*)/*Disabled.*
- *Primary Server is* — IP address of the primary RADIUS server.
- *Primary Server Port is* — Port number of the primary server. Default: *1645.*
- *Secondary Server is* — IP address of the secondary RADIUS server.
- *Secondary Server Port is* — Port number of the secondary server. Default: *1645.*
- *Retransmission Timeout* — Interval between retransmissions. Default: *3 seconds.*
- *Max Retranmissions* — Number of retransmissions before failure reported. Default: *10 seconds.*

```
AUTHENTICATION SETTINGS
Local Authentication is                     ENABLED
Remote Authentication is:                   ENABLED
Hint Assigned is:                           DISABLED
Primary Server is                           122.122.122.134
Primary Server Port is                      1645
Secondary Server is:                        0.0.0.0
Secondary Server Port is:                   1645
Retransmission  Timeout:                    3
Max Retranmissions:                         10
```

show authentication counters

Displays the RADIUS and local user authentication counters. It lists the following:

- *Local Successful Authentications* — Number of times user/password pair matched.
- *Local Failed Authentications* — Number of times user/password pair did not match.
- *Remote Successful Authentications* — Number of times RADIUS accepted the user on this server.
- *Remote Failed Authentications* — Number of times RADIUS rejected user on this server.

- *Remote No Responses* — Number of times RADIUS failed to answer an authentication request (with an error message) on this server.

```
AUTHENTICATION COUNTER
Local Successful Authentications        5
Local Failed Authentications            0
Remote Successful Authentications:      5
Remote Failed Authentications           0
Remote No Responses:                    1
```

show bridge or show bridge network <network name> settings

Displays information about the specified bridge network. You use add bridge network to define bridge networks. It lists the following:

- *Interface* — Interface this bridge is using.
- *Network address*— Index number for this bridge network.
- *Frame type* — BRIDGE is the default.
- *Status* — Enabled or disabled are options.
- *User Name*.

show clearTCP or show clearTCP settings

Displays the ClearTCP message (Default: *Connected*) when a ClearTCP client session is connected to the remote TCP host. It can be modified using the `set clearTCP connect_message` command.

Example:

```
CLEARTCP SETTINGS
ClearTCP Connection Message:              Connected
```

show command or show command settings

Displays the settings for CLI commands. See `set` command to modify settings. Prompts can hold a maximum of 64 ASCII characters. It lists the following:

- *History depth* - Number of CLI commands issued by the RAS 1500 that display when the up or down arrow keys are pressed
- *Global prompt* —
- *Local prompt* — Designation of prompt for a temporary CLI session.
- *Console login required* — Whether login to the console is required.
- *Console idle timeout* — Interval before a console session is timed out.

- *Current idle timeout* —

```
History Depth:                  10
Global Prompt:                  ras1500>>
Local Prompt                    ras1500>>
Console Login Required:         NO
Console Idle Timeout:           5
Current Idle Timeout:           0
```

show configuration or show configuration settings

Displays a variety of system information including system, network, protocol, interface, forwarding, routing, DNS, host, and data link parameters.

show connection or show connection settings

Displays the settings for dial-in connections, which can be modified using the set connection command. It lists the following:

- *Host Selection Method* — ROUND-ROBIN or RANDOM.
- *Global User Name* — USR_NETS is the global username, used when no other is available.
- *Service Prompt* — Displayed when a dial-in user is connected.
- *Message Prompt* — Prompts the user for login or network service.

```
CONNECTION SETTINGS
Host Selection Method:                      ROUND-ROBIN
Global User Name:                           default
Service Prompt:                             Login/Network User:
Message Prompt:                             manage:
```

show connection counters

Displays the counters kept for dial-in connections. It lists the following:

- *Number of Calls* — Number of incoming calls.

```
COUNTER FOR CONNECTIONS
Number of Calls:                            1
```

show critical_event or show critical_event settings

Displays where the log files for critical event messages are stored in FLASH memory. It lists the following:

- *Critical Event Sink* — Where critical events are logged, default is @file:/./log-file.local.

- *Critical Event Backup* — where critical events are logged, if the first destination fails. Default: @file:/./old-log-file.local

show date

Displays the system *date, time,* and *uptime*. The time is expressed in GMT. Example:

```
System Date                             13-JAN-1999 19:25:11
Timezone Offset from GMT                -6:00
(hours:minutes)
System UpTime:                          1d 00:12:30
```

show dhcp mode

Displays the configured mode type: disabled, server, relay, or proxy.

show ddp

Displays current AppleTalk statistics.

Example:

```
APPLETALK DDP FORWARDING COUNTERS
Forwarding Requests:                        0
Bad Routes:                                 0
DDP Broadcast Errors:                       0
DDP Hop Count Errors:                       0
```

```
APPLETALK DDP COUNTERS
Outbound Requests:                          0
DDP Outbound Shorts:                        0
DDP Outbound Longs:                         0
DDP Inbound Receives:                       0
DDP Inbound Local Datagrams:                0
DDP No Protocol Handlers:                   0
DDP Too Short Errors:                       0
DDP Too Long Errors:                        0
Short DDP Errors:                           0
Checksum Errors:                            0
```

show dhcp proxy counter

Displays the settings configured for DHCP proxy in the following format:

```
Discover Tx:        0
Select Request Tx:0
Init/Reboot Request Tx:        0
```

```
Renew Request Tx:              0
Rebind Request Tx:             0
Decline Tx:                    0
Release Tx:                    0
Inform Tx:                     0
Offer Rx:                      0
Ack Rx:                        0
Nak Rx:                        0
```

show dhcp proxy settings

Displays the current statistics of the DHCP proxy mode in the following format:

```
DHCP PROXY CONFIGURATION SETTING

Server1 Address:               0.0.0.0
Server2 Address:               0.0.0.0
```

show dhcp relay

Displays the settings configured for DHCP relay in the following format:

```
Server1
   Address:   0.0.0.0
   Max Hops: 0
   Status:    DISABLED

Server2
   Address:   0.0.0.0
   Max Hops: 0
   Status:    DISABLED

COUNTERS
Server1
   Request Sent to Server:          0
   Responses Received from Server:  0
   Responses Received w/Error:      0

Server2
   Request Sent to Server:          0
   Responses Received from Server:  0
   Responses Received w/Error:      0

Client
   Requests discarded:              0
```

show dhcp server counters

Displays the current statistics of the DHCP relay mode in the following format:

```
Lease Requests received:0
Lease Accepts received:0
Lease Renewals received: 0
Lease Refusals received:            0
Lease Releases received:            0
Unrecognized packets received:      0
Lease Offers transmitted:           0
Lease Confirmations transmitted:    0
Renewal Refusals transmitted:       0
Requested address out of range:     0
Requested address in use:           0
No free addresses:                  0
```

show dhcp server settings

Displays the settings configured for DHCP server in the following format:

```
Status:            DISABLED
Start IP Address:  000.000.000.000
End IP Address:    000.000.000.000
IP Mask:           000.000.000.000
IP Router:         000.000.000.000
Lease (seconds):   4800
Host Name:         unit
Domain Name:       dummy.net
DNS #1:            000.000.000.000
DNS #2:            000.000.000.000
WINS #1:           000.000.000.000
WINS #2:           000.000.000.000
```

show dial_out

Displays the current settings for the dial-out server. You can modify the settings using the `set dialout` command.

```
DIALOUT SETTINGS
Security - Login Required:                YES
Idle Timeout (User):                      5
Recovery Timeout (Workstation):           5
```

show dns or show dns settings

Displays settings for all DNS servers, which you can modify using the `set DNS` command. It lists the following:

- *Domain Name* — Default domain name to be used if no domain is specified in the name to be resolved.

- *Number Retries per Server* — Number of times the resolve name request is sent to each Name Server, if the server fails to respond to a request before the timeout period.
- *Timeout Period in Seconds* — Number of seconds to wait before deciding a request to a Name Server has timed out.
- *Cache Max TTL* — Maximum TTL period in seconds for resource records in this cache.
- *Negative Cache Max TTL* — Maximum TTL period in seconds for negative cached authoritative errors.
- *Caching* — Indicates whether function is Enabled or Disabled.
- *Negative Caching* — Indicates whether function is Enabled or Disabled.
- *Host Rotation* — Indicates whether function is Enabled or Disabled.

```
DNS SETTINGS
Domain Name                eden-3com.com
Number Retries per         1
Server:
Timeout Period in          5
Seconds:
Cache Max TTL:             2147483
Negative Cache Max TTL     2147483
Caching:                   ENABLED
Negative Caching:          ENABLED
Host Rotation:             ENABLED
```

show dns cache <1-65535>

Displays an entry in the DNS Cache Table. It lists the following:

- *Pretty Name* — Fully qualified name (resource record) the host connects to (at this row in the table). See RFC-1035, section 2.3.3 for more information.
- *Class* — DNS class of the resource record at this row in the table.
- *Type* — DNS type of the resource record at this row in the table.
- *TTL* — Time-To-Live period in seconds of the resource record.
- Elapsed TTL — Period in seconds since resource record was received.
- *DNS Server* — Host from which resource record was received, 0.0.0.0 if unknown.

- *Data* — RDATA portion of a cached RR. The value is in the format defined for the particular DNS class and type of the resource record. See RFC-1035, section 3.2.1 for more information.
- *(Error) Status* — Status column for the resolver cache table. Since only the agent (DNS resolver) creates rows in this table, the only values that a manager may write to this variable are Active and Destroy.

```
DNS CACHE ENTR
Pretty Name:  canary.mass-3com.com
Class:        1
Type:         1
TTL:          24761
Elapsed TTL   228
DNS Server    123.133.143.176
Data:
              92 73 78 c7
Status:       Active
```

show dns counters

Displays various counters for DNS. It lists the following:

- *Total Queries Received* — Sum of DNS queries received.
- *Total Response Sent* — Sum of DNS responses sent.
- *Responses from Client Processing* — DNS responses from local DNS Host Table.
- *Responses from Server Processing* — DNS responses from the DNS Server Table.
- *Success Responses from Server* — Successful responses to DNS requests.
- *Error Response sent* — Sum of failures to DNS requests, specifics shown below.

SPECIFIC ERROR COUNTERS

- *Format Errors* — Number of Format Error responses received by DNS.
- *Problems with Name Server* — Internal server error.
- *NonExistent Name* — Number of times the requested name could not be resolved.
- *Server refused the request* — Server was able to accept a request.

- *Server does not implement request* — Server was able to accept a request.
- *Corrupted Responses* — Response did not decrypt.
- *Timeouts* — Number of time outs waiting for the server to respond.
- *Response could not be sent* — The requester had terminated.
- *Nonauthoritative Data Responses* — Number of requests made by the resolver for which a nonauthoritative answer (cached data) was received.
- *Nonauthoritative No Data Responses* — Number of requests made by the resolver for which a nonauthoritative answer - no such data response (empty answer) was received.
- *Martians* — Number of responses received that were received from servers that the resolver does not think it asked.
- *Received Responses* — Number of responses received to all queries.
- *Unparseable Responses* — Number of responses received that were unparseable.
- *Fallbacks* — Number of times the resolver had to fall back to its seat belt information.
- *Good Caches* — Number of resource records the resolver has cached successfully.
- *Bad Caches* — Number of resource records the resolver has refused to cache because they appear to be dangerous or irrelevant. For example, resource records with suspiciously high TTLs, unsolicited root information, or those that don't appear to be relevant to the question the resolver asked.
- *Good Negative Caches* — Number of authoritative errors the resolver has cached successfully.
- *Bad Negative Caches* — Number of authoritative errors the resolver was unable to cache because the appropriate Resource Record was not supplied or looked suspicious.

show dns ncache <1-65535>

Displays an entry (row) in the DNS Negative Cache Table. It lists the following:

- *Pretty Name* — Fully qualified name (resource record) the host connects to (at this row in the table).
- *Class* — DNS class of the resource record at this row in the table.

- *Type* — DNS type of the resource record at this row in the table.
- *TTL* — Time-To-Live period in seconds of the resource record.
- *Elapsed TTL* — Period in seconds since resource record was received
- *DNS Server* — IP address of the fully qualified name.
- *Error Code* — Type of authoritative error indicated in the table. Types include the following:
  - *Nonexist(ent Name)* — Authoritative name error.
  - *No Data* — Authoritative response with no error and no relevant data.
  - *Other* — Some other cached authoritative error. At present, no such errors are known to exist.
- *(Error) Status* — Status column for the resolver negative response cache table. Since only the agent (DNS resolver) creates rows in this table. Types include the following: *Active*, *Destroy***.**

```
DNS NEGATIVE CACHE ENTR
Pretty Name   foo.mass-3com.com
Class:        1
Type:         1
TTL:          43200
Elapsed TTL:  207
DNS Server:   153.234.24.145
Error Code:   NONEXIST
Status:       Active
```

show events

Displays all events being directed to the console to also be echoed to the Telnet or dial-in session you are running. Any number of users can employ this function. The `hide events` command ends this directive. Events are configured with the `set facility` command.

show file <input_file_name>

Displays the contents of an ASCII file.

Example:

```
ras1500>> show file easyfilter.fil
     #filter
     #IP:
      #10 reject src-address = 220.159.132.13;
      #20 accept src-address != 220.159.132.13
      #30 reject udp-src-port = 69;
      #40 reject tcp-src-port = 23;
      #50 reject udp-dst-port = 69
      #60 reject tcp-dst-port = 23;
```

show file <input_file_name> hex

Displays the contents of a hexadecimal file.

For example (log-file.local):

```
000000  43453035  43453031  41742031  363a3537  CE05CE01At
                                                16:57
0010    3a31342c  20466163  696c6974  79202255  14, Facility
                                                "User
0020    73657220  4d616e61  67657222  2c204c65  Manager",
000030  76656c20  22435249  54494341  4c223a3a  Level
                                                "CRITICAL":
000040  20415554  483a204e  6f206163  6b6e6f77  AUTH: No
                                                acknow
000050  6c656467  656d656e  74206672  6f6d2052  ledgement
                                                from
000060  41444955  53206163  636f756e  74696e67  RADIUS
                                                accounting
000070  20736572  76657273  2c207265  61636865  servers,
                                                reached
000080  64206d61  78206e00  43453032  41742031   max
                                                n*CE02At
000090  373a3136  3a31342c  20466163  696c6974  17:16:14,
                                                Facility
0000a0  79202255  73657220  4d616e61  67657222  "User
                                                Manager",
```

show filter <filter_name>

Displays the filter rules for all protocols specified in this file. The file name specified MUST be a filter file (filter.fil). See the `show filter protocol` command, below.

*A newly created filter file does not appear when this command is issued until the file is added to the Filter Table with the **add filter** command.*

For example (easyfilter.fil):

```
RULES FOR FILTER /./easyfilter.fil SHOW PROTOCOLS: ALL
#filter
IP:
10 reject src-address = 234.149. 82.139;
20 accept src-address != 234.149. 82.139;
30 reject udp-src-port = 69;
40 reject tcp-src-port = 23;
50 reject udp-dst-port = 69
60 reject tcp-dst-port = 23;

IP-RIP
10 accept network = 244.49. 82.0;
20 deny
```

show filter <filter_name>

`protocol [atalk, atalk-arap, atalk-call, atalk-rtmp, atalk-zip, br-eth, br-eth-call, ip, ip-call,ip-rip, ipx, ipx-call, ipx-rip, ipx-sap, login-access]`

Displays filter rules based on protocol options specified. The filter name MUST be a filter file (filter.fil), as listed using `list filters`. Also see the `show filter` command above. It lists the following:

- *ATALK* — AppleTalk data filter rules.
- *IP* — IP data filter rules.
- *IP-CALL* — IP call filter rules.
- *IP-RIP* — IP RIP advertisement filter rules.
- *IPX* — IPX data filter rules.
- *IPX-CALL* — IPX call filter rules.
- *IPX-RIP* — IPX RIP advertisement filter rules.
- *IPX-SAP* — IPX SAP advertisement filter rules.
- *LOGIN-ACCESS* — Login access filter rules.

show frame_relay pvc <pvc_name> settings

Displays current Frame Relay status and configuration for *pvc <pvc_name>*.

show icmp or show icmp settings

Displays incoming login-access information including whether ICMP logged and ICMP Router Advertise are enabled. You can turn multicasting of ICMP router advertisements on or off with the `enable` or `disable icmp_router_advertise` command.

```
ICMP SETTINGS
ICMP Logging:                                    ENABLED
ICMP Router Advertise:Enabled                    ENABLED
```

show icmp counters

Displays input and output counters for ICMP messages.

Traceroute-generated packets received by the RAS 1500 do not increment the ICMP error counts Time Exceeded and Destination Unreachable. Also, a number of ICMP error messages are sent to SYSLOG hosts. The Receive Destination Unreachable event is sent to the console.

It lists the following:

INPUT COUNTERS

- *Messages* — ICMP packets received.
- *Errors* — ICMP packets received with errors.
- *Destination Unreachable* — Sum of ICMP messages received when a router cannot forward a packet to its specified destination. *Error messages* are s*ent to the console and CLI.*
- *Time Exceeded* — Sum of ICMP messages generated by a router when time has exceeded or a timeout has occurred while waiting for a packet segment. Error messages sent to SYSLOG host.
- *Parameter Problems* — Sum of ICMP messages generated by a router when it encounters an error. *Error messages sent to SYSLOG host.*
- *Source Quench* — Sum of ICMP messages informing a host it should slow data transmission to ease congestion. *Error messages sent to SYSLOG host.*
- *Redirects* — Sum of ICMP messages concerning a router advertising a host of a better next hop. *Error messages not logged.*
- *Echos* — Sum of ICMP request messages received, signifying transport system success.
- *Echo Replies* — Sum of ICMP reply messages received, indicating transport system success.

- *Timestamps* — Sum of ICMP request messages received seeking time from another machine for clock synchronization and estimated transit time purposes. *Error messages sent to SYSLOG host.*
- *Timestamp Replies* — Sum of ICMP timestamp reply messages.
- *address Masks* — Sum of ICMP address Mask Reply messages. *Error messages sent to SYSLOG host.*
- *address Mask Replies* — Sum of ICMP request messages concerning the ability of a host to gather network information. *Error messages sent to SYSLOG host.*
- *Advertise* — Sum of router advertisements received by the RAS 1500.
- *Solicit* — Sum of host-generated router queries received by the RAS 1500. *Error messages sent to SYSLOG host.*

OUTPUT COUNTERS

- *Messages* — Total of ICMP messages transmitted.
- *Errors* — ICMP packets transmitted with errors.
- *Destination Unreachable* — Sum of these messages sent. *Error messages sent to SYSLOG host.*
- *Time Exceeded* — Sum of these messages sent. *Error messages sent to SYSLOG host.*
- *Parameter Problems* — Sum of these messages sent. *Error messages sent to SYSLOG host.*
- *Source Quench* — Sum of these messages sent.
- *Redirects* — Sum of these messages sent. *Error messages sent to SYSLOG host.*
- *Echos* — Sum of ICMP Echo (request) messages sent.
- *Echo Replies* — Sum of these messages sent.
- *Timestamps* — Sum of these messages sent.
- *Timestamp Replies* — Sum of these messages sent.
- *address Masks* — Sum of these messages sent.
- *address Mask Replies* — Sum of these messages sent. *Error messages sent to SYSLOG host.*
- *Advertise* — Sum of router advertisements sent by the RAS 1500. *Error messages sent to SYSLOG host.*

show interface <interface_name> or show interface settings

Displays settings for the specified modem or Ethernet interface. The interface name can be either *rm0/eth:1* (the LAN interface) or *x/slot:y/mod:z* (where x is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), y is the slot number, and z is the modem number.

Example:

`rm0/slot:1/mod:1`).

This command displays the following:

- *Description* — Name of the interface driver. *Ethernet* or *Modem* drivers.
- *Type* — Kind of physical serial interface.

  Example: *RS232* or *Ethernet-CSMACD.*
- *Speed* — Estimate of the interface's current bandwidth in bits per second.
- *High Speed* — Estimate of the interface's current bandwidth in units of 1,000,000 bits per second, exceeding 20 million bits/second.
- *Administrative Status* — Permanently configured state of the interface. Choices: *Up* or *Down.*
- *Operational Status* — Current state of the interface. Choices: *Up* or *Down.*
- *Link Up/Down Traps* — Permanently configured value indicating whether linkUp/linkDown traps should be generated for this interface. Choices: *ENABLED* (default) or *DISABLED.*
- *Promiscuous Mode* — When set to *FALSE* (default), this interface accepts packets/frames addressed only to this station. When set to *TRUE*, the station accepts all packets/frames transmitted on the network.
- *Connector Present* — When set to *TRUE* (default) the interface sublayer has a physical connector and *FALSE* (default) when otherwise.
- *Filter Access* — This switch allows user filters to override the specified interface filter. If set to *OFF* (default), user filters do not override the interface filters. If set to *ON*, user filters override the interface filter.
- *Last Change* — Last configuration change made to the interface, measured in system time.

- *Input Filter* — Name of the input filter enabled for the specified interface.
- *Output Filter* — Name of the output enabled filter for the specified interface.
- *Host Type* — Type of host this dial-in user is currently connected to. Choices: *PROMPT*, *SELECT*, and *SPECIFIED*. Default: *SELECT.*
- *Connection Type* — Kind of connection this interface is configured for. Choices: *DIRECT_CONN*, *NORMAL*, *DIRECT_NET*, *NO_PROMPT*, and *PROMPT_USER_ONLY*. Default: *NORMAL.*
- *Port Type* — Type of physical port configured. Choices: *NETWORK*, *LOGIN*, and *LOGIN_NETWORK* (default).
- *User Name* — Name of connected user. This value is set only if the port is configured not to prompt for username.
- *Access* — Direction of calls currently configured on this interface. Choices: *DIAL_IN*, *DIAL_OUT*, or *TWO_WAY* (default).
- *Dial Prefix* — A number defining the prefix to the phone number.
- *Init Script* — Initialization script currently in use. Default: *USR_int.*
- *TCP Port* — TCP port number you associate with the login service. Default: 0. Range: 0-65535.
- Protocol — Currently connected protocol type. Choices: *PPP* or *SLIP*. Default: PPP.
- *Prompt* — Dial-in prompt you set for this interface. Limit: *64 ASCII characters*.
- Login —
- *Message* - Salutation you specified for this interface. Limit: *64 ASCII characters.*
- *Host address* - IP address of the host specified for this interface.
- *Login Service* - Type of login service you configured for this interface. Choices: *Telnet*, *rlogin*, and *ClearTCP*. Default: *Telnet*.

show interface <interface_name> counters

Displays counters for the specified interface. The interface name can be either *rm0/eth:1* (the LAN interface), *loopback*, *internal*, or *x/slot:y/mod:z* (where x is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), y is the slot number, and z is the modem number.

Example:

`rm0/slot:1/mod:1`).

This command displays the following:

INPUT COUNTERS

- *Octets* — Number of bytes received.
- *Ucast* — Number of Unicast packets received.
- *MultiCast* — number of multicast packets received.
- *BroadCast* — Number of broadcast packets received.
- *Discards* — Number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
- *Errors* — For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a number of inbound transmission units that contained higher-layer protocol.
- *Unknown Prot* — Number of unknown protocols in packet.

OUTPUT COUNTERS

- *Octets* — Number of bytes transmitted.
- *Ucast* — Number of Unicast packets transmitted.
- *MultiCast* — Number of multicast packets transmitted.
- *BroadCast* — Number of broadcast packet transmitted.
- *Discards* — Number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
- *Errors* — For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
- *Out QLen* — Length of the output packet queue (in packets).

show ip or show ip settings

Displays system-wide IP information:

- *IP System Host address* — IP address of the RAS 1500.
- *IP Forwarding* — Status of forwarding of IP packets.
- *IP Address Pool Filtering* — Status of pool filtering.
- *UDP Broadcast Forwarding* — Status of UDP broadcast forwarding.
- *IP Address Assign Mode* — Source of IP address assignment.

```
IP System Host address:                     134.225.22.1760
IP Forwarding:                              ENABLED
IP Address Pool Filtering:                  ENABLED
UDP Broadcast Forwarding                    ENABLED
IP Address Assign Mode                      IP_POOL
```

show ip counters

Displays system-wide IP network statistics:

INPUT COUNTERS

- *Total Input Datagrams* — Sum of IP datagrams received.
- *Bad Headers* — Number of datagrams with bad headers.
- *Bad addresses* — Number of datagrams with bad addresses.
- *Forwarded Packets* — Number of packets forwarded.
- *Bad Protocol* — Number of packets received with bad protocol.
- *Discarded* — Number of packets discarded.
- *Successfully Delivered* — Number of packets successfully received.

OUTPUT COUNTERS

- *Total Output Datagrams* — Sum of datagrams transmitted.
- *Discarded* — Number of datagrams discarded.
- *Bad Routes* — Number of datagrams with a bad route.
- *Fragments Needing Reassembly* — Number of fragmented datagrams.
- *Datagrams Successfully Reassembled* — Number of fragmented datagrams successfully reassembled.
- *Reassembly Failures* — Number of fragmented datagrams unsuccessfully reassembled.

- *Datagrams Successfully Fragmented* — Datagrams successfully fragmented before transmission.
- *Fragmentation Failures* — Failed datagram fragmentations before transmission.
- *Total Fragments* — Sum of fragments transmitted.

show ip network <network_name> or show ip network settings

Displays parameter settings for the specified IP network. See the `set ip network` command on for more details.

- *Interface* — Interface this IP network runs on.
- *Network address* — Network address and subnet mask of the RAS 1500.
- *Frame Type* — Frame type used by the RAS 1500. Choices: *ETHERNET_II* or *SNAP*.
- *Mask* — Subnet mask of the RAS 1500.
- *Station* — Station address of the RAS 1500.
- *Broadcast Algorithm* — Broadcast algorithm used for this network. Default: *IETF*.
- *Max Reassembly Size* — Maximum packet size allowed to be reassembled from fragments.
- *IP Routing Protocol* — Routing protocol used. Default: *None.*
- *IP RIP Routing Policies* — Routing policies used by RIP.
- *IP RIP Authentication Key* — Text string used for RIPv2 authentication.
- *Status — Enabled, ACTIVE, INACTIVE, Disabled.*
- *Reconfigure Needed — FALSE or TRUE.* When displaying the value TRUE, this setting notifies the administrator that the network should be reinitialized for a newly configured parameter to take effect. Using the reconfigure command allows the network to automatically re-enable without having to manually disable and enable the network. The value *FALSE* indicates no network editing has occurred and no reconfiguration is required.
- *IP Routing Metric* — Routing metric configured for this network. Range: 1-16. Default: 1.

```
SHOW IP  NETWORK ipnet SETTINGS
Interface:                              rm0/eth:1
Network address:                        165.134.145.124/22
Frame Type                              ETHERNET_I
Status:                                 ENABLED
Reconfigure Needed:                     FALSE
Mask                                    255.255.252.0
Station:                                165.134.145.124
Broadcast Algorithm:                    IETF
Max Reassembly Size:                    3464
IP Routing Protocol:                    RIPV2
IP Routing Metric:                      1
IP RIP Routing Policies                 SEND_ROUTES
                                        SPLIT_HORIZON
                                        FLASH_UPDATE
                                        SEND_COMPAT
                                        RIPV1_RECEIVE
                                        RIPV2_RECEIVE
IP RIP Authentication Key
```

show ip routing or show ip routing settings

Displays parameter settings for the specified IP network. Statistics are gathered from parameters configured by the `set ip routing` command. It lists the following:

- *IP Router Administrative Status* — Whether status is enabled or not. Default: *Enabled.*
- *IP Static Remote Routes* — Whether static routes are enabled or not. Default: *Enabled.*
- *LAN Host address* — IP address of the RAS 1500.
- *IP Autonomous System Number* — System number assigned. Default: *1.*
- *IP Max Table Size* — Maximum number of IP Routing Table entries allowed. Default: *1,415.*
- *IP Max Metric Entries* — Maximum metric entries allowed. Default: *512.*
- *IP RIP* — Whether RIP is enabled or not. Default: *Enabled.*
- *IP Number RIP Interfaces* — Number of RIP interfaces.
- *IP Number RIP Neighbors* — Number of IP RIP neighbors.

- *IP RIP Flags* — Type of IP RIP flags enabled.

```
IP ROUTER SETTING
IP Router Administrative Status          Enabled
IP Static Remote Routes                  Enabled
IP LAN Host address:                     165.134.145.124
IP Autonomous System Number              1
IP Max Table Size:                       1450
IP Max Metric Entries:                   512
IP RIP:                                  Enabled
IP Number RIP Interfaces:                0
IP Number RIP Neighbors:                 0
IP RIP Flags:                            METRICS
                                         SEND_REQUEST
```

show ip security or show ip security settings

Displays state (*enabled* or *disabled*) of IP security settings. The settings shown below are defaults. See the `enable ip security_options` commands for more information.

```
IP SECURITY SETTINGS
Drop All Fragoffset1:           ENABLED
Drop TCP Fragoffset1            ENABLED
Disallow All Header Options     DISABLED
Disallow Source Route Options:  DISABLED
```

show ip udp_broadcast_forwarding

Displays state (*enabled* or *disabled*) of IP upd_broadcast_forwarding. The default for udp_broadcast forwarding is "disabled."

show ipx or show ipx settings

Displays settings for dynamic IPX networks. You can modify these values using the `set ipx system` command. It lists the following:

- *Default Gateway* — Default IPX router address.
- *Name* — Designation for dynamic IPX networks.
- *Network Number* — Network number for dynamic IPX networks.
- *Max Open Sockets* — Maximum allowed number of open sockets to remote IPX networks.
- *Max Hops* — Maximum allowed hops to remote IPX networks.
- *Priority* — Preferred ranking of dynamic IPX networks.

- *Dynamic address Pool Begin* — Starting IPX address.
- *Number of Dynamic Pool Members* - Number of addresses to reserve for dynamic IPX address assignments.

```
IPX SETTINGS
Default Gateway:                0.00:00:00:00:00:
                                00
PPP IPX Network address:        00000000
Name:                           IPXNET
Network Number:                 0
Max Hops:                       15
Priority:                       1
Dynamic address Pool Begin:     23
Number of Dynamic Pool          200
Members:
```

show ipx counters

Displays counters for all IPX network activity. It lists the following:

INPUT COUNTERS

- *Total Packets Received* — Sum of IPX packets received.
- *Header Errors* — Sum of incoming packets discarded due to errors in their headers, including any IPX packet sized less than a minimum of 30 bytes.
- *Unknown Sockets* — Sum of incoming packets discarded because the destination socket was not open.
- *Discarded* — Sum of incoming packets discarded due to reasons other than those accounted for by Header Errors and Unknown Sockets.
- *Checksum Errors* — Sum of IPX packets received with wrong checksums.
- *Delivered Locally* — Sum of IPX packets delivered locally, including packets from local applications.
- *No Route to Destination* — number of times no route to a destination was found.
- *Too Many Hops* — Sum of incoming packets discarded for exceeding the hop count.
- *Filtered Out* — Sum of incoming packets filtered out.

- *Decompression Errors* — Sum of incoming packets discarded due to compression errors.

OUTPUT COUNTERS

- *Total Packets Transmitted* — Sum of IPX packets transmitted.
- *Forwarded Packets* — Sum of IPX packets forwarded.
- *Local Transmits* — Sum of IPX packets transmitted to local hosts.
- *Local Malformed Transmits* — Sum of IPX packets supplied locally containing structural errors.
- *Discarded* — Sum of outgoing packets discarded.
- *Filtered Out* — Sum of packets filtered out before transmission.
- *Compression Errors* — Sum of outgoing packets discarded due to compression errors.
- *Socket Open Failures* — Sum of outgoing packets discarded because a socket was not available.

show ipx network <network_name> or show ipx network settings

Displays parameter settings for the specified IPX network. You can modify most of these values using the `set ipx network` command. It lists the following:

- *Interface* — Interface this IPX network uses, *rm0/eth:1.*
- *Network address* — Network address of this IPX network.
- *Frame Type* — Frame type used by the interface (*ETHERNET II*, *NOVELL_8023*, *SNAP*, or *DSAP*).
- *Maximum Packet Size* — Maximum allowable packet size for this IPX network. Default: *1500*.
- *Status* — Operational state of the network. Default: *ENABLED.*
- *Network Delay (ticks)* — Time in number of ticks it takes to reach this IPX network. Default: *1.*
- *Network Learning Retries* — Number of times this network resends packets to discover its directly connected neighbors.
- *Diagnostics* — Sending of diagnostic packets. Default: *ENABLED.*
- *NetBIOS* — Support. Default: *ENABLED.*
- *NetBIOS Name Caching* — Support. Default: *DISABLED.*

- *NetBIOS Cache Timer (sec)* — Interval a NetBIOS system is kept in the cache. Default: *60.*
- *NetBIOS Maximum Hops* — Greatest number of hops this network makes to locate a NetBIOS system. Default: *8.*
- *RIP State* — Status: *ON*, *OFF*, *AUTO ON*, or *AUTO OFF*. Default: *ON.*
- *RIP Pace* — Fastest pace, in packets per second, at which RIP packets may be sent on this circuit (not settable via the CLI).
- *RIP Update (sec)* — Interval, in seconds, after which RIP periodic updates are transmitted. Default: *60.*
- *RIP Age Multiplier* — Number the rip_update_interval is multiplied by to obtain the update value. Default: *4.*
- *RIP Max Packet Size* — Largest allowable size of a RIP packet. Default: *446.*
- *RIP Broadcast* — Support. Default: *ENABLED.*
- *RIP Periodic* — Support. Default: *ENABLED.*
- *SAP State* — Support: ON or OFF. Default: *ON.*
- *SAP Pace* — Fastest pace, in packets per second, at which SAP packets may be sent on this circuit (not settable via the CLI). Default: *1.*
- *SAP Update (sec)* — Interval, in seconds, after which SAP periodic updates are transmitted. Default: *60.*
- *SAP Age Multiplier* — Number the sap_update_interval is to multiplied by to obtain the update value. Default: *4.*
- *SAP Packet Size* — Greatest allowable size of a SAP packet. Default: *510.*
- *SAP Broadcast* — Support. Default: *ENABLED.*
- *SAP Periodic* — Support. Default: *ENABLED.*
- *SAP Nearest Server Reply* — SAP seeks nearest neighbors: *YES* or *NO*. Default: *YES.*

show ipx network <network_name> counters

Displays statistics for the specified IPX network. It lists the following:

- *RIP Out Packets* — Sum of RIP packets transmitted.
- *RIP In Packets* — Sum of RIP packets received.
- *SAP Out Packets* — Sum of SAP packets transmitted.
- *SAP In Packets* — Sum of SAP packets received.

```
SHOW IPX  NETWORK ipxnet2 COUNTERS:
RIP Out Packets:                          53
RIP In Packets:                           30
SAP Out Packets:                          1
SAP In Packets:                           160
```

show ipx rip or show ipx rip settings

Displays information about RIP for IPX. It lists the following:

- *State* — ON or OFF.
- *Incorrect RIP Packets* — Number of RIP packets that do not make sense.

show ipx rip counters

Displays the Sum of incorrect RIP packets.

show ipx sap or show ipx sap settings

Displays information about SAP for IPX. It lists the following:

- *State* — ON or OFF.
- *Incorrect SAP Packets* — Number of SAP packets that do not make sense.

show ipx sap counters

Displays the Sum of incorrect SAP packets.

show memory

Displays the RAS 1500 Dynamic Random Access Memory (DRAM) usage. It lists the following:

- *Total System Memory Resources* — Total amount of usable memory for router applications.
- *Free Memory* — Amount of memory not in use.
- *Code Size* — Amount of memory used by code.
- *Initialized Data Size, Uninitialized Data Size, Stack Size* — Static data areas.

```
SYSTEM MEMORY RESOURCE
Total System Memory Resources:       14879 KB
Free Memory:                          13275 KB
Code Size:                           2913 KB
Initialized Data Size:               1839 KB
Uninitialized Data Size:              449 KB
Stack Size:                           32 KB
```

show modem_group <name>

Displays the switched interfaces that belong to the specified modem group and their status.

Example:

```
MODEM GROUP boston INTERFACES 3
Interfac                             Status
rm0/slot:2/mod:1                     ACTIVE
rm0/slot:2/mod:2                     ACTIVE
rm0/slot:2/mod:3                     ACTIVE
```

show network <name> or show network settings

Displays the configured settings for the specified network. For an example, see the output from the `show ip network` command above.

show network <name> counters

Displays the statistical counters for the specified network. However, IP does not maintain network counters.

```
SHOW IPX  NETWORK ipxnet COUNTERS:
RIP Out Packets:                     2484
RIP In Packets:                      113484
SAP Out Packets:                     2266
SAP In Packets:                      699788
```

show packet_logging or show packet_logging settings

Displays settings for packet size and logging. See the `set packet_logging` command for more information.

Example:

```
PACKET LOGGING SETTING
Logging Packet Type:                    NONE
Logging Packet Size:                    0
```

show ping or show ping settings

Displays general ping settings you specified using the `ping` and `set ping maximum_rows` commands.

Example:

```
Maximum Rows in Table                   20
```

show ping row <row_number> or show ping row <row_number> settings

Displays settings for the specified row in the Remote Ping Table. Range: 1-1000. These settings reflect the configuration you specified using the ping command.

Example:

```
PING SETTINGS for ROW: 1 DESTINATION:
ilysium
Status:                                        ACTIVE
Resolved IP address:                           155.155.121.143
Count:                                         100
Interval                                       1
Size:                                          64
Timeout:                                       20
Self Destroy Delay:                            10
```

show ping row <row_number> counters

Displays counters for the specified row in the Remote Ping Table. These settings reflect the configuration you specified using the `ping` command. This command displays the following:

- *Status* — Present state of this row. Possible states include *notReady*, *notInService*, and *active*.
- *Count* — Number of pings to be transmitted in this sequence.
- *Requests Sent* — Number of pings sent when this row became active.

- Replies Received — Number of pings received when this row became active.
- *Timeouts Occurred* — Number of requests timed-out since this row became active.
- *Last Round Trip* — Round trip time in milliseconds experienced by the last request-reply iteration. A round trip value of -1 indicates failed resolution.
- *Minimum Round Trip* — Minimum ping round trip time in milliseconds, not including timed out requests.
- *Maximum Round Trip* — Maximum ping round trip time in milliseconds, not including timed out requests.
- *Average Round Trip* — Average ping round trip time in milliseconds, not including timed out requests.
- *Creation Time* — Time this row was created in terms of system up time.
- *Activation Time* — Time this row was last activated in terms of system up time.
- *Last Changed Time* - Time any object in this row was last changed in terms of system up time.

```
PING COUNTERS for ROW: 1 DESTINATION:
ilysium
Status:                                       ACTIVE
Count:                                        100
Requests Sent:                                32
Replies Received                              32
Timeouts Occured                              0
Last Round Trip (ms)                          40
Minimum Round Trip (ms)                       40
Maximum Round Trip (ms):                      50
Average Round Trip (ms)                       40
Creation Time:                                0d 22:36:33
Activation Time                               0d 22:36:33
Last Changed Time                             0d 22:37:11
```

show ping server <host name or IP_address> counters

Displays ping server counters associated with the ping server you specified in the `add ping service_loss_system` command.

Average Time is expressed in milliseconds. Also, a value of -1 indicates the ping system failed. See `show ping server settings` *below for more information.*

```
PING SERVER COUNTERS for      cassava
SERVER
Status                        ENABLED
Time Since Contacted:         -1
Pings Sent                    0
Pings Received                0
Timeouts                      0
Unreachables:                 0
Average Time (ms)             0
```

show ping server <host name or IP_address> or show ping server settings

Displays ping server settings you specified with the `add ping service_loss_system` command A value of -1 indicates failure of ping system. It lists the following:

- *Status* — Whether this system is being pinged regularly or not. Default: *Enabled.*
- *Frequency* — Interval between each ping request. Default: *30 seconds.*
- *Misses Allowed* — Number of ping messages that can be missed before the modems are busied out. Default: *1.*
- *Time Out* — How long a ping request can be outstanding before it is considered to have failed. Default: 2.
- *Reachable* — Whether the ping server is connected.
- *Time Since Contacted* — Number of seconds since the server was reached.
- Address — Address of system.

```
PING SERVER SETTINGS for      cassava
SERVER
Status                        ENABLED
Frequency:                    30
Misses Allowed                1
TimeOut                       10
Reachable                     UNTRIED
address:                      0.0.0.0
```

show ppp on interface <interface name>, or show ppp on interface <interface name> settings

Displays PPP settings on the specified WAN interface when interface is active. The interface name can be either *rm0/eth:1* (the LAN interface), *loopback*, *internal*, or *x/slot:y/mod:z* (where x is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), y is the slot number, and z is the modem number.

Example:

`rm0/slot:1/mod:1`).

The command displays the following:

SETTINGS for PPP BUNDLE 1

- *Operational Status* — Opened or Not Opened.
- *Number Active Links* — Number of links active on this PPP bundle.
- *User Profile* — User whose parameters were used in creating links.
- *Local MMRU* — MRU the remote entity uses when sending packets to local PPP entity. Default: *1514.*
- *Remote MMRU* — MRU the local entity uses when sending packets to remote PPP entity. Default: *1514.*
- *Local Endpoint Class* — Type of address used as the identifier - IEEE MAC address.
- *Local Endpoint Length* — Maximum length of the local Endpoint Discriminator address. Default: *6.*
- *Local Endpoint ID* — MAC address of local Endpoint Discriminator.
- *Remote Endpoint Class* — Value of remote Endpoint Discriminator Class, which indicates the type of address being used as the identifier.
- *Remote Endpoint Length* — Maximum length of remote Endpoint Discriminator address.
- *Remote Endpoint ID* — IP address of remote Endpoint Discriminator.

SETTINGS for PPP BUNDLE 1 COMPRESSION

- *Operational Status* — Opened or Not Opened.
- *Compression Protocol* — Protocol used by the local PPP entity when it compresses the local PPP entity to the remote PPP entity. Default: *VJ-TCP.*

SETTINGS for PPP LINK

- *Operational Status* — Opened or Not Opened.
- *Interface Index* — Index number of the interface used.
- *Local MRU* — MRU the remote entity uses when sending packets to local PPP entity. Default: *1514.*
- *Remote MRU* - MRU the local entity uses when sending packets to remote PPP entity. Default:*1514.*
- *Local to Peer ACC Map* — Value of the ACC Map used for sending packets from the local PPP entity to the remote PPP entity.
- *Peer to Local ACC Map* — ACC Map used by the remote PPP entity when transmitting packets to the local PPP entity.
- *Local To Remote Protocol Compression* — Indicates whether the local PPP entity uses Protocol Compression when transmitting packets to the remote PPP entity. Default: *Enabled*.
- *Remote To Local Protocol Compression* — Indicates whether the remote PPP entity uses Protocol Compression when transmitting packets to the local PPP entity. Default: *Enabled*.
- *Local To Remote ACC Compression* — Indicates whether the local PPP entity uses address and Control Compression when transmitting packets to the remote PPP entity. Default: *Enabled.*
- *Remote To Local ACC Compression* — Indicates whether the remote PPP entity uses address and Control Compression when transmitting packets to the local PPP entity. Default: *Enabled.*

SETTINGS for PPP LINK - AUTHENTICATION

- *Operational Status* — Opened or Not Opened.
- *Local To Remote Compression Protocol* — Protocol used by the local PPP entity when it compressed the remote PPP entity. Default: *CHAPMD5.*

- *Remote To Local Compression Protocol* — Protocol used by the remote PPP entity when it compressed the local PPP entity.

```
SETTINGS for PPP BUNDLE                     20
Operational Status:                         Opened
Number Active Links:                        1
User Profile:                               n1
Local MMRU                                  1514
Remote MMRU:                                1514
Local Endpoint Class:                       IEEE MAC address
Local Endpoint Length:                      6
Local Endpoint ID:                          00:00:00:03:00:65
Remote Endpoint Class:                      Null Class
Remote Endpoint Length:                     0
Remote Endpoint ID:                         Class=0x1:Length=
                                            0x0

SETTINGS for PPP BUNDLE 20
COMPRESSION
Operational Status:                         NotOpened
Compression Protocol:                       NONE

SETTINGS for PPP BUNDLE 20 IP
PROTOCOL
Operational Status:                         Opened
Local To Remote Compression                 VJ_TCP
Protocol:
Remote To Local Compression                 VJ_TCP
Protocol:
Local Max Slot ID:                          15
Remote Max Slot ID:                         15
Local IP address:                           172.152.42.72
Remote IP address:                          192.112.226.200

SETTINGS for PPP LINK 20 - 8
Operational Status:                         Opened
Interface Index                             8
Local MRU:                                  1514
Remote MRU:                                 1514
Local to Peer ACC Map:                      a0000
Peer to Local ACC Map:                      0
```

```
SETTINGS for PPP BUNDLE                   20
Local To Remote Protocol                  ENABLED
Compression:
Remote To Local Protocol                  ENABLED
Compression:
Local To Remote AC Compression:           ENABLED
Remote To Local AC Compression:           ENABLED

SETTINGS for PPP LINK 20 - 8
AUTHENTICATION
Operational Status:                       Opened
Local To Remote Authenticate              CHAPMD5
Protocol:
Remote To Local Authenticate              NONE
Protocol:
```

show ppp on interface <interface name> counters

Displays statistics for PPP running on the specified interface when interface is active. The interface name can be either *rm0/eth:1* (the LAN interface), *loopback*, *internal*, or *x/slot:y/mod:z* (where x is the type of unit (rm0 for the RAS 1500 unit; pem0 or pem1 for the RAS 1500 Expansion Unit), y is the slot number, and z is the modem number.

Example:

`rm0/slot:1/mod:1`).

It lists the following:

COUNTERS for PPP BUNDLE

- *Operational Status* — Not opened or Opened.
- *Number Active Links* — Sum of active links using this PPP bundle.
- *Transmit Packets* — Sum of packets transmitted over this bundle.
- *Bytes from Upper Layer* — Sum of bytes received from an upper layer application for transmission over this bundle. This counter represents all data handed down to the PPP application BEFORE compression occurs.
- *Bytes to Lower Layer* — Sum of bytes sent to a lower layer application for transmission over this bundle. This counter represents all data to be handed down to the lower layer application AFTER compression occurs.

- *Received Packets* — Sum of packets received from a lower layer application over this bundle.
- *Bytes to Upper Layer* — Sum of bytes to be handed up to an upper layer application over this bundle.
- *Bytes from Lower Layer* — Sum of bytes received from a lower layer application over this bundle.
- *Total Bad Headers* — Sum of packets with incorrect PPP Header (address, Control, PID Field).

COUNTERS for PPP LINK

- *Operational Status* — Not Opened or Opened.
- *Received Packets* — Too Long; sum of frames judged too long.
- *Transmit Frames* — Sum of frames received from the PPP application for transmission over this link.
- *Bytes from Upper Layer* — Sum of bytes handed down from an upper layer application for this link.
- *Bytes to Lower Layer* — Sum of bytes received from a lower layer application for this link.
- *Received Frames* — Sum of frames received on this link.
- *Bytes to Upper Layer* — Sum of bytes handed up to an upper layer application over this link.
- *Bytes from Lower Layer* — Sum of bytes received from a lower layer application over this link.

show ppp, or show ppp settings

Displays global settings for PPP. You can modify DIAL-IN Users Authentication using the `set ppp receive_authentication` command. Modify the system transmit authentication name by using the `set system` command. It lists the following:

- *DIAL-IN Users Authenticate PAP or CHAP* — Indicates whether PPP requires dial-in users to authenticate strictly via *PAP*, *CHAP*, *ANY*, *EAP-MD5*; with *ANY*, *NONE*, or *ENCRYPTED-ANY (CHAP, EAP-MD-5, MS-CHAP),* or *RADIUS-EAP-PROXY*. Default: *None.*
- *System Transmit Authentication Name* — Remote account keyword used by PPP at the data link layer for WAN connections.

- *Primary NBNS Server address* — IP address for the primary NetBIOS Name Server (NBNS) server. In the absence of a user-specific NBNS address, this is sent in IPCP negotiation.
- *Seconday NBMS Server address* — IP address for the secondary NBNS server. In the absence of a user-specific NBNS address, this is sent in IPCP negotiation.
- *Use system DNS Configuration* — Indicates, when enabled, that PPP takes DNS addresses from the RAS 1500 DNS table in the absence of user-configured DNS addresses. Choices: SYSTEM, PPP, or NONE.

```
PPP AUTHENTICATION
DIAL_IN Users Authenticate PAP or       EITHER
CHAP:
System Transmit Authentication Name:    RAS1500
Primary NBNS Server address:            0.0.0.0
Secondary NBNS Server address:          0.0.0.0
Use system DNS Configuration:           SYSTEM
```

show security_option, or show security_option settings

Displays status of SNMP user access, security service, and administration by remote users. You can modify SNMP user access using the `enable` or *disable security_option snmp* commands. You can modify administration by remote user using the `enable` or `disable security_option remote_user` commands. It lists the following:

- *SNMP User Access* — *Enabled* (default) or *Disabled.*
- *Administration by Remote Telnet User* — *ON* (default) or *OFF.*
- *Administration by Remote Dial-in user* — *ON* (default) or *OFF.*

```
SECURITY OPTION SETTINGS
SNMP User Access:                       ENABLED
Administration by Remote TELNET User:   ON
Administration by Remote Dialin User:   ON
```

show slice

Displays slice settings.

show slip, or show slip settings

Displays SLIP configurations. Indicates, when enabled, that SLIP framing can be offloaded to the modem card (if the modem card is capable of doing it) and the start message (which appears when the SLIP connection comes up). Default: *enabled*.

See the `add slip session_start_message` command for information on writing the message.

Example:

```
SLIP offloading         Enabled
SLIP Session Start      SLIP connection starting. Your ss
Message:                %client_ip \n
```

show snmp counters

Displays many SNMP statistics. It lists the following:

INPUT COUNTERS

- *Packets* — Number of SNMP packets received.
- *Bad Versions* — SNMP messages for an unsupported SNMP version.
- *Bad Community Names* — SNMP messages that used an unknown SNMP community name.
- *Bad Community Uses* — SNMP messages that represented an SNMP operation not allowed by the SNMP community named in the message.
- *ASN.1 Parse Errors* — Sum of ASN.1 or BER errors.
- Too Big Errors — SNMP protocol data units (PDUs) for which the value of the error-status field is `tooBig'.
- *No Such Name Errors* — SNMP PDUs where error-status field is `noSuchName'.
- *Bad Value Errors* — SNMP PDUs where error-status field is 'badValue'.
- *Read Only Errors* — SNMP PDUs where the error-status field is `readOnly'.
- *General Errors* — SNMP PDUs where the error-status field is 'genErr'.
- *Total Request MIB Objects* — Sum of MIB objects retrieved successfully as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
- *Total Set MIB Objects* — Sum of MIB objects altered successfully as the result of receiving valid SNMP Set-Request PDUs.
- *Get Request PDUs* — Sum of SNMP Get-Request PDUs accepted and processed.
- *Get Next Request PDUs* — Sum of SNMP Get-Next PDUs accepted and processed.

- *Set Request PDUs* — Sum of SNMP Get-Next PDUs accepted and processed.
- *Get Response PDUs* — Sum of SNMP Get-Response PDUs accepted and processed.
- *Trap PDUs* — Sum of SNMP Trap PDUs accepted and processed.

OUTPUT COUNTERS

- *Packets* — Sum of SNMP packets transmitted.
- *Too Big Errors* — Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is 'tooBig.'
- *No Such Name Errors* — Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is 'noSuchName.'
- *Bad Value Errors* — Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is 'badValue.'
- *General Errors* — Sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is 'genErr.'
- *Get Request PDUs* — Sum of SNMP Get-Request PDUs sent from SNMP.
- *Get Next Request PDUs* — Sum of SNMP Get-Next PDUs sent from SNMP.
- *Set Request PDUs* — Sum of SNMP Set-Request PDUs sent from SNMP.
- *Get Response PDUs* — Sum of SNMP Get-Response PDUs from SNMP.
- *Trap PDUs* — Sum of SNMP Trap PDUs sent from SNMP.

show system or show system settings

Displays system information. It lists the following:

- *System Descriptor* — Company designation of the RAS 1500 including build date.
- *Object ID* — Identifies this system to SNMP managers.
- *System UpTime* — Time the system has been running since last boot.
- *System Contact* — Name of person responsible for system. Modify using `set system` command.
- *System Name* — Modify using `set system` command.
- *System Location* — Site where system is located. Modify using set `system` command.

- *System Services* — For example, Internet EndToEnd Applications.
- *System Transmit Authentication Name* — System-wide keyword for PPP on the WAN, modified using `set system` command.
- *System Version* — Loaded release version of the system software.

```
System Descriptor:   SuperStack Remote Access System 1500,
                     Version: 1.5.9, 144,
                     Built on Jan 26 1999 at 12:10:38.
Object ID:           1.3.6.1.4.1.429.2.24
System UpTime:       1d 20:55:36
System Contact:
System Name:
System Location:
System Services:     Internet EndToEnd Applications
System Transmit      RAS1500
Authentication
Name:
System Version:      X1.5.9
```

show tcp, or show tcp settings

Displays system-wide TCP settings. It lists the following:

Most of these settings cannot be edited.

TCP SETTINGS

- *Retransmission Algorithm* - Type of algorithm used. Default: *Van Jacobson.*
- *Minimum Timeout* — Minimum retransmission timeout interval. Default: *0.*
- *Maximum Timeout* — Maximum retransmission timeout interval. Default: *240000 seconds*.
- *Maximum Connections* — Sum of TCP connections allowed. Default: *1024.*

```
TCP SETTINGS
Retransmission Algorithm:   Van Jacobson
Minimum Timeout:            0
Maximum Timeout:            240000
Maximum Connections:        48
```

show tcp counters

Displays system-wide TCP statistics.

TCP COUNTERS

- *Active Opens* — Number of times TCP connections have made a direct transition to SYN-SENT state from CLOSED state.
- *Passive Opens* — Number of times TCP connections have made a direct transition to SYN-RCVD state from LISTEN state.
- *Attempt Fails* — Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
- *Resets* — Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
- *Currently Established* — Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
- *Input Segments* — Sum of segments received.
- *Output Segments* — Sum of segments sent, including those on current connections but excluding those containing only retransmitted octets.
- *Retransmitted Segments* — Sum of segments retransmitted.

show telnet or show telnet settings

Displays the status of the Telnet escape and trying message features (*ENABLED* (default) or *DISABLED*). It is set using disable/enable telnet escape.

```
TELNET SETTINGS
TELNET Escape:                   ENABLED
```

show time or show timezone

Displays the system date, time, and uptime. The present time is expressed in GMT.

Example:

```
System Date                        10-JAN-1999 19:25:11
Timezone Offset from GMT           -6:00
(hours:minutes):
System UpTime:                     1d 00:12:30
```

show udp, or show udp counters

Displays statistics for UDP datagrams. It lists the following:

INPUT COUNTERS

- *Total Input Datagrams* — Sum of UDP datagrams received.
- *Input but No Port* — Sum of received UDP datagrams for which there was no application at the destination port.
- *Input with other Errors* — Sum of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

OUTPUT COUNTERS

- *Total Output Datagrams* - Sum of UDP datagrams sent.

show user <name>

```
settings
```

Displays the parameters defined for the specified user.

- *Settings* - Displays settings for the specified user with the exception of disabled IP, IPX, Tap Status, and Tunnel Type parameters.

The type of information displayed depends on the type of user you specify. Issue the `list users` command to see which users are defined, and what *type(s)* user each is. An example of a login/manage follows. Note that this user may not be typical. Defaults are indicated by (D).

```
INFORMATION FOR USER: administrator
Status:                     ACTIVE
Type:                       LOGIN
                            MANAGE
Expiration:                 NONE
Message:                    Welcome to the RAS 1500
PPP Callback Type:          Normal  (D)
Phone Number:
Alternate Phone Number:
Caller ID1:
Caller ID2:
Callback delay:             5       (D)
Input Filter:
Output Filter:
Modem Group:                all     (D)
Session Timeout:            0       (D)
Idle Timeout:               0       (D)

PARAMETERS FOR LOGIN USERS:
Login Service:              TELNET  (D)
TCP Port:                   23      (D)
Terminal:                   vt100   (D)
Login Host Name:            barney
Login Host:                 0.0.0.0 (D)
Host Type:                  SELECT  (D)
```

Telnet Commands

Telnet commands are available to users who dial in and whose type is network (*type* parameter in `add user` command), whose host_type is prompt (*host_type* parameter in `set login user` command), and whose login_service is Telnet (*login_service* parameter in `set login` user command).

telnet <IP_name or address>

Establishes a Telnet client session with the specified IP host name or address. For the system to resolve the host name, you must add the host name and address to the DNS Local Host Table, or you must define a DNS server.

telnet <IP_name or address> TCP_port <number>

Establishes a Telnet client session with the specified IP host name or address using the specified TCP port number. It works just like the Telnet command, except you also specify the TCP port number to be used. Default TCP port number: *23*. Maximum: *65535.*

Unassign Command

unassign interface <interface_name_list >

`modem_group <group_name>`

Removes the specified interface from the list of interfaces you previously assigned to the specified modem group. You specify interfaces for a modem group when you add a modem group, using `add modem_group interface`. You can also add interfaces to that modem group using `assign interface modem_group`. You can see which interfaces you have assigned to an existing modem group using the `show modem_group` command.

Verify Command

verify filter <filter_name>

Verifies the syntax of a filter file, which has been previously added to the table. If you update a filter file and TFTP it to the FLASH file system, and the file already exists in the Filter Table, you use this command to verify the file syntax. You can use list filters to see which files are currently in the Filter File Table and what the status of each is.

Dial-in User Commands

Telnet commands are available to users who dial in and whose type is login (type parameter in add user) and whose host_type is prompt (host_type parameter in set login user).

exit

Logs you out of your login session.

help

Displays the available Dial-in user commands.

logout

Logs you out of your login session.

manage
This is only shown if your user type is defined as manage. It puts you into the CLI, so you can execute full CLI commands and configure the system. Use the exit command to exit the CLI.

rlogin <ip_name_or_address>
Establishes an rlogin client session with the specified IP host name or IP address. You must have run add DNS host or add DNS server for the system to recognize an IP host name.

rlogin <host name or ip address> login_name <login name> tcp_port <tcp port number>
Establishes an rlogin client session with the specified IP host name or IP address using the specified TCP port number. The default rlogin TCP port number is 513. You must have run add DNS host or add DNS server for the system to recognize an IP host name.

telnet <ip_name_or_address>
Establishes a Telnet connection to the specified IP address or host name. You must have run add DNS host or add DNS server for the system to recognize an IP host name.

telnet <ip_name_or_address> tcp_port <number>
Sets a Telnet connection to the specified IP address or host name with the specified TCP port number. The default port number is *23*. You must have a domain name server specified or have added the host name via `add DNS host` and `add DNS server` commands for the system to recognize an IP host name.

You should run RIP when setting up a global IP network if you intend to support TCP services such as Telnet, rlogin, and ClearTCP. Without RIP on the internal network, you do not learn of remote networks if the Ethernet interface is disabled.

Telnet Commands

The following commands are available to Console port users who Telnet from the Console port. Such users can access these commands by using the Telnet escape command: Ctrl] (right bracket). This function is not supported for login users.

close
Ends the active Telnet connection.

help
Describes the available commands.

send <string> Transmits a Telnet control character. The available commands are the following:

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	Synchronize
ESC	Escape

set escape <string> Allows changing the Telnet escape character from Ctrl] (right bracket] to something else. Control characters are specified using the carat character followed by the character. For example, to set the Telnet escape character to Ctrl x, enter the following:

```
set escape ^ x
```

status Displays the IP address of the remote host you are Telnetted to and the value of the Telnet escape character.

CLI Exit Commands

These commands are available to dial-in (modem) and Telnet (LAN) users so they can disconnect from the CLI.

bye, exit, leave, quit Leaves the CLI, but keeps this connection open. These commands return you to the dial-in user or Telnet commands.

logout Leaves the CLI and closes this connection. This ends the dial-in user or Telnet session.

Command Features

The command language has several built-in features that make it easier to use. When abbreviating commands, it is sometimes difficult to remember commands and their syntax. Using command completion and positional helps to remind you of the commands and their parameters while you are typing a command string.

Command Line Edit

Command line edit allows nondestructive cursor movements on a command already typed.

Entry	Action
(Ctrl b) or left arrow	go back one character
(Ctrl f) or right arrow	go forward one character
(Esc b)	go back one word
(Esc f)	go forward one word
(Ctrl a)	go to beginning of command
(Ctrl c)	escape from CLI process
(Ctrl e)	go to end of command
(Ctrl d) or (Ctrl k)	delete character

Command Retrieval

Command retrieval retrieves commands from the history of previous commands entered. You can display the current command history using the history command. You can change the number of commands kept in the command history buffer using the set command history command.

Entry	Action
(Ctrl p) or up arrow	recall previous command in history list
(Ctrl n) or down arrow	recall next command in history list

Positional Help

Positional help displays the list of possible parameters when you type `?` (question mark) after any command or parameter. It redisplays the line you typed, without the `?`, so you can enter the parameter you wish to use. This helps you find the parameter you need, so you can add it to your command without retyping the entire command string. Be sure to leave a space between the keyword and the question mark to use positional help.

Command Completion

The TAB key provides command completion. If you press the TAB key before you finish typing a command or parameter, the rest of the command or parameter is displayed (completed), and you can continue entering the command. If the command or parameter is ambiguous, the bell sounds, and the display does not change.

Output Pause

When output to your screen pauses because more than 24 lines are waiting for display, you can press ENTER to display one more line of output, ESC to display one more page of output or q to quit the command.

Command Kill

To discontinue the current command action and flush any commands that have been typed ahead, use (Ctrl c).

A

Modem Command Reference

This appendix includes:

- Modem Command Overview
- Basic AT Commands
- Ampersand Commands
- Percent Commands
- Asterisk Commands
- Tilde Commands
- Octothorp Commands
- S-Register Commands
- Using S-Register Commands

Modem Command Overview

This appendix lists the modem (AT) commands supported by the SuperStack Remote Access System (RAS) 1500. To issue these commands through the RAS 1500 CLI, use the `set switched interface router` command and its at parameter. For example, to reset the modem (specifically, modem one, in slot one, in the RAS 1500 unit), type the following command at the CLI prompt:

```
set switched interface rm0/slot:1/mod:1 at z!
```

For more information about the `set switched interface` command, see Chapter 4, “Router Command Reference.”

Basic AT Commands

The following table lists the basic AT commands supported by the RAS 1500.

Table 3 Basic AT Commands

Command	Description
&$	HELP, Ampersand Commands
%$	HELP, Percent Commands
~$	HELP, Tilde Commands
*$	HELP, Asterisk Commands
#$	HELP, Octothorp Commands
A/	Repeat Last Command
AT	Command Mode Prefix
A	Answer Call
B	B0 V.32 originate mode
C	C1 Transmitter On
Dn	Dial a Telephone Number n=0..9#*TPR,;”W!()-
DL	Dial Last Phone Number
DSn	Dial Stored Phone Number
D$	HELP, Dial Commands
E	E0 No Command Echo E1 Echo Command Chars
H	H0 On Hook (Hang Up) H1 Off Hook
I	I0 Product Code I3 Modem Identification I4 Current Settings I5 Flash Settings I6 Link Diagnostics I7 Product Configuration 19 DNIS Configuration 11 Extended link screen 12 ISDN Configuration 15 CID Status
K	K0 Call Duration Mode K1 Real Time Clock
Q	Q0 Result Codes Sent
Sr=n	Sets Register "r" to "n"
Sr?	Query Register "r"

Table 3 Basic AT Commands

Command	Description
S$	HELP, S Registers
T	Tone Dial
V	V0 Numeric Responses
X	X0 Basic Result Codes X1 Extended Result Codes X2-X7 Advanced Result Codes
Z	Software Reset
Z!	Modem Reset
$	HELP, Command Summary

Ampersand Commands

The following table lists the ampersand (&) commands supported by the RAS 1500.

Table 4 Ampersand Commands

Command	Description
&A	&A0 Disable /ARQ Result Codes &A1 Enable /ARQ Result Codes &A2 Enable /Modulation Codes &A3 Enable /Extra Result Codes
&F	&F0 Load Factory Configuration
&G	&G0 No Guard Tone &G1 550 Hz Guard Tone &G2 1800 Hz Guard Tone
&K	&K0 Disable Data Compression &K1 Auto Data Compression &K2 Enable Data Compression &K3 Selective Data Compression
&L	&L0 Normal &L1 Reserved
&M	&M0 Normal Mode &M4 ARQ/Normal Mode &M5 ARQ Mode

Table 4 Ampersand Commands

Command	Description
&N	&N0 Highest Link Speed
	&N1 300 bps
	&N2 1200 bps
	&N3 2400 bps
	&N4 4800 bps
	&N5 7200 bps
	&N6 9600 bps
	&N7 12000 bps
	&N8 14400 bps
	&N9 16800 bps
	&N10 19200 bps
	&N11 21600 bps
	&N12 24000 bps
	&N13 26400 bps
	&N14 28800 bps
	&N15 31200 bps
	&N16 33600 bps
	&N17 28000 bps
	&N18 29333 bps
	&N19 30666 bps
	&N20 32000 bps
	&N21 33333 bps
	&N22 34666 bps
	&N23 36000 bps
	&N24 37333 bps
	&N25 38666 bps
	&N26 40000 bps
	&N27 41333 bps
	&N28 42666 bps
	&N29 44000 bps
	&N30 45333 bps
	&N31 46666 bps
	&N32 48000 bps
	&N33 49333 bps
	&N34 50666 bps
	&N35 52000 bps
	&N36 53333 bps
	&N37 54666 bps
	&N38 56000 bps
	&N39 57333 bps
	&N40 58666 bps
	&N41 60000 bps
	&N42 61333 bps
	&N43 62666 bps
	&N44 64000 bps

Table 4 Ampersand Commands

Command	Description
&T	&T0 End Test &T1 Analog Loopback (ALB) &T4 Grant Remote DLB &T5 Deny Remote DLB
&U	Minimum link speed (see &N)
&W	Store Configuration
&Y	&Y0 Destructive &Y1 Destructive/Expedited &Y2 Nondest./Expedited &Y3 Nondest./Unexpedited
&Zn=s	Store Phone Number
&Zn=L	Store Last Phone Number
&Zn?	Query Phone Number

Percent Commands

The following table lists the percent (%) commands supported by the RAS 1500.

Table 5 Percent Commands

Command	Description
%B	Store V110 Rate %B0 110 bps %B1 300 bps %B2 600 bps %B3 1200 bps %B4 2400 bps %B5 4800 bps %B6 9600 bps %B7 19200 bps %B8 38400 bps %B9 57600 bps %B10 115200 bps
%C	%C0 Defer Configuration
%CIn=s	Store Initialization String (n=1-4)
%CIn?	Query Initialization String (n=1-4)
%CNn=s	Store DNIS Number (n=1-3)
%CNn?	Query DNIS Number (n=1-3)

Asterisk Commands

The following table lists the asterisk (*) commands supported by the RAS 1500.

Table 6 Asterisk Commands

Command	Description
*B1=	*B1=0 Disable Keypad Element *B1=1 Enable Keypad Element *B1=2 Auto Keypad Element
*B2=	*B2=0 Disable Sending Complete *B2=1 Enable Sending Complete *B2=2 Auto Sending Complete
*B3=	*B3=0 Disable Report Busy *B3=1 Enable Report Busy
*B4=	*B4=0 No LLC / No BC Disable *B4=1 No LLC / No BC Enable
*B5=	*B5=0 Send LLC Disable *B5=1 Send LLC Enable
*B6=	*B6=0 Disable Data/Voice *B6=1 Enable Data/Voice
*B7=	*B7=0 Auto Data/Voice Rate *B7=1 64K Data/Voice Rate *B7=2 56K Data/Voice Rate
*B8=	*B8=0 Auto Voice Encoding *B8=1 A-Law Voice Encoding *B8=2 u-Law Voice Encoding
*I1=s	MSN String
*I2=	*I2=0 Disable MSN Send *I2=1 Enable MSN Send
*I3=	*I3=0 Disable MSN Check *I3=1 Enable MSN Check
*I4=s	Subaddress String
*I5=	*I5=0 Auto Subaddress Type *I5=1 NSAP Subaddress Type *I5=2 User Subaddress Type
*I6=	*I6=0 Disable Subaddress Send *I6=1 Enable Subaddress Send
*I7=	*I7=0 Disable Subaddress Check *I7=1 Enable Subaddress Check

Table 6 Asterisk Commands

Command	Description
*L	*L0 End Test *L1 DChannel Local Loopback *L2 BChannel 1 Local Loopback *L3 BChannel 2 Local Loopback *L4 DChannel Remote Loopback *L5 BChannel 1 Remote Loopback *L6 BChannel 2 Remote Loopback
*M=	*M=0 Auto Mode (Depends on ISDN Switch) *M=1 Point to Multi Point Mode *M=2 Point To Point Mode
*P1=s	Directory Number 0
*P2=s	Directory Number 1
*S1=s	Service Profile Identifier 0
*S2=s	Service Profile Identifier 1
*T1=xx	Terminal Equipment Identifier 0
*T2=xx	Terminal Equipment Identifier 1
*U1=	Originate Mode HDLC Protocol Selection *U1=0 None *U1=1 V.120 *U1=2 X.75 *U1=3 Async-to-Sync PPP
*U2=	Originate Mode Non-HDLC Protocol Selection *U2=0 None *U2=1 V.110
*U3=	Originate Mode Analog Modem/Fax Selection *U3=0 None *U3=1 Analog Modem/Fax
*V1=	Voice Bearer Capability Selection *V1=0 Auto Mode (Depends on ISDN Switch) *V1=1 3.1Khz Audio *V1=2 Speech
*V2=	Data Bearer Capability *V2=0 Autodetect *V2=1 V.120 Rate Adaption only *V2=2 V.110 Rate Adaption only *V2=3 Modem/Fax Emulation only *V2=4 Clear Channel only *V2=5 Async-to-Sync PPP only *V2=6 X.75 only

Table 6 Asterisk Commands

Command	Description
*W=	ISDN Switch Protocol Type *W=0 AT&T 5ESS Custom *W=1 NT DMS100 Custom *W=2 National ISDN-1 *W=3 ETSI *W=4 German 1TR6 *W=5 Australia *W=6 Italy *W=7 Japan INS64 *W=8 New Zealand *W=9 Spain *W=10 Taiwan
*X0=	X.75 Frame Size in Bytes *X0=1-2048
*X1=	X.75 Window Size in Frames *X1=1-7
*Z	Restart BRI Port
*Z?	Query BRI port reset state

Tilde Commands

The following table lists the tilde (~) commands supported by the RAS 1500.

Table 7 Tilde Commands

Command	Description
~Sn	n=serial number

Octothorp Commands

The following table lists the octothorp (#) commands supported by the RAS 1500.

Table 8 Octothorp Commands

Command	Description
#CID=	#CID=0 Disable Caller ID #CID=1 Enable Caller ID
#CID?	Query Current Setting

S-Register Commands

The following table lists the S-register commands supported by the RAS 1500.

Table 9 S-Register Commands

Register	Function
S0	Ring to Answer On
S1	Counts # of Rings
S2	Escape Code Char
S3	Carriage Return Char
S4	Line Feed Char
S5	Backspace Char
S6	Wait Time/Dial Tone (sec)
S7	Wait Time/Carrier (sec)
S8	Comma Time (sec)
S9	Carrier Detect Time (1/10sec)
S10	Carrier Loss Time (1/10sec)
S11	Dial Tone Spacing (msec)
S12	Escape Code Time (1/50sec)
S13	Bitmapped. 1 = Reserved 2 = Do Originate in Auto Answer 4 = Reserved 8 = Reserved 16 = Reserved 32 = Reserved 64 = Disable MNP Level 3 128 = Modem Reset
S14	Bitmapped. 1 = Escape Code Hang Up 2 = Result Code Orig Only
S15	Bitmapped. 1 = Reserved 2 = Disable Online Fallback 4 = Reserved 8 = Reduced Non-ARQ TX Buffer 16 = Disable MNP Level 4 32 = Reserved 64 = Unusual MNP-Incompatibility 128 = Reserved

Table 9 S-Register Commands

Register	Function
S16	Test Modes 1 = Analog Loopback 2 = Dial Test 4 = Test Pattern 8 = Remote Digital Loopback 16 = Reserved 32 = Reserved 64 = Reserved 128 = Reserved
S17	Reserved
S18	&Tn Test Timeout (sec)
S19	Inactivity Timeout (min)
S20	Reserved
S21	Reserved
S22	Reserved
S23	Reserved
S24	Reserved
S25	Reserved
S26	Reserved
S27	Bitmapped. 1 = V21 Mode 2 = Disable TCM 4 = Disable V32 8 = Disable 2100hz 16 = Disable MNP Handshake 32 = Disable V.42 48 = Disable V.42 Detect Phase 64 = Reserved 128 = Unusual SW-Incompatibility
S49	Reserved
S50	Reserved
S51	Bitmapped. 1 = MNP/V.42 Disabled in V.22 2 = MNP/V.42 Disabled in V.22bis 4 = MNP/V.42 Disabled in V.32 8 = Reserved 16 = Reserved 32 = Reserved 64 = Disable Selective Reject 128 = Reserved
S52	MNP Link Request Timeout (0-14sec)

Table 9 S-Register Commands

Register	Function
S53	Reserved
S54	Bitmapped. 1 = Disable 2400 symbol rate 2 = Disable 2743 symbol rate 4 = Disable 2800 symbol rate 8 = Disable 3000 symbol rate 16 = Disable 3200 symbol rate 32 = Disable 3429 symbol rate 64 = Disable V.8 Call Indicate 128 = Disable V.8 Mode
S55	Bitmapped. 1 = Disable 8S-2D trellis code 2 = Disable 16S-4D trellis code 4 = Disable 32S-2D trellis code 8 = Disable 64S-4D trellis code 16 = Reserved 32 = Reserved 64 = Reserved 128 = Reserved
S56	Bitmapped. 1 = Disable Non linear coding 2 = Disable TX level deviation 4 = Disable Pre-emphasis 8 = Disable Pre-coding 16 = Disable Shaping 32 = Disable V34+ 64 = Disable V.34 128 = Reserved
S57	Reserved
S58	Reserved
S59	Reserved
S60	Reserved
S61	Short form rules
S62	Number of ANI digits
S63	Number of DNIS digits
S64	Reserved
S65	Reserved
S66	Reserved

Table 9 S-Register Commands

Register	Function
S67	Bit Mapped. 1 = Enable V.110 in Automode 2 = Fix Connection Rate for Digital Calls 4 = Connect at 64k (else 56k) 8 = Reserved 16 = Enable Data Link Delay 32 = Reserved 64 = Reserved 128 = Reserved
S68	Bit Mapped 1 = Disallow

Using S-Register Commands

S-Registers are addresses of places in memory where various timing parameters, redefinitions of selected ASCII characters, and other configuration settings are stored.

Initially, the S-Register settings for each of the templates are the same. As with any setting stored in NVRAM, however, you can overwrite an S-Register stored value.

Changing an S-Register

If you change an S-Register setting and want to save the change, follow the setting with &W. If you do not follow an S-Register setting with &W, the setting is retained only until the next reboot or power off.

To change a setting for an S-Register in the current configuration, use the commands:

Table 10 Changing an S-Register

To set the S-Register value using	Command	Example
Decimal numbers(3Com recommends this option)	ATSr=n, where r is an S-Register and n is a decimal number between 0 and 255.	ATS50=2
Bit-mapped registers	ATSr.b=n, where r is the bit-mapped S-register, b is the bit (0-7), and n is 0 or 1 (off or on).	ATS50.1=1

Bit-Mapped S-Registers

Understanding Bit-Mapped S-Registers

Certain S-Registers are bit-mapped. Bit-mapped registers appear in RAS 1500 documentation as the following: ATS56.1=1 and ATS68.4=0. A bit-mapped S-Registers uses one number to describe a collection of settings. Bit-mapping allows modem developers to pack a lot of information in a small space.

When RAS 1500 displays the value of an S-Register, you see a decimal value between 0 and 255. RAS 1500, however, understands the decimal value as a collection of binary digits (bits).

Setting Bit-Mapped S-Registers

You can set bit-mapped S-Registers using either bits or decimal values. While it may be simpler for you to set the bits individually, RAS 1500 displays the S-Register settings in decimal form.

Bits and decimal values

For bit-mapped S-Registers, eight bits are assigned. Each bit is either on (1) or off (0). Eight bits create 256 unique combinations of 1s and 0s. Each of the eight bits is assigned a number corresponding to its position as in the following example:

b b b b b b b b

7 6 5 4 3 2 1 0

Each bit can be assigned a value corresponding to its number. Use the following table to understand the relationship of bits to the decimal value.

Table 11 Bit-mapped S-Register Explanation

Value	Bit	Visual representation
S78=1	S78.0=1	0 0 0 0 0 0 0 1
S78=2	S78.1=1	0 0 0 0 0 0 1 0
S78=4	S78.2=1	0 0 0 0 0 1 0 0
S78=8	S78.3=1	0 0 0 0 1 0 0 0
S78=16	S78.4=1	0 0 0 1 0 0 0 0
S78=32	S78.5=1	0 0 1 0 0 0 0 0
S78=64	S78.6=1	0 1 0 0 0 0 0 0
S78=128	S78.7=1	1 0 0 0 0 0 0 0

B MODEM DISCONNECT AND RESULT CODES

- Result Codes
- Disconnect Codes

Result Codes

The following result codes are supported by the SuperStack Remote Access System (RAS) 1500:

Table 12 Result Codes

Message	#	Message	#
NO DIAL TONE	006	14400/ARQ	026
BUSY	007	4800/HST	028
NO ANSWER	008	9600/ARQ/V32	037
NO ANSWER	009	4800/V32	038
2400	010	4800/ARQ/V32	039
RINGING	011	7200/V32	040
VOICE	012	12000/V32	041
9600	013	12000/ARQ/V32	042
CONNECT/ARQ	014	16800	043
1200/ARQ	015	7200/ARQ/V32	044
2400/ARQ	016	14400/V32	045
9600/ARQ	017	14400/ARQ/V32	046
4800	018	16800/ARQ	047
4800/ARQ	019	75/1200	048
7200	020	1200/75	049
12000	021	ABORT	050
12000/ARQ	022	INCOMING CALL	051
7200/ARQ	024	PHONE OFF HOOK	052
14400	025	OFF HOOK RESTRICTED	054

Table 12 Result Codes

Message	#	Message	#
16800/ARQ/HST	057	26400	103
COMMAND DENIED	058	26400/ARQ	104
WAITING	061	26400/VFC	105
DIALING DIABLED	062	26400/ARQ/VFC	106
DATA	063	28800	107
+FCO	065	28800/ARQ	108
16800/V32	083	28800/VFC	109
16800/ARQ/V32	084	28800/ARQ/VFC	110
19200	085	21600/V34	111
19200/V32	087	21600/ARQ/V34	112
19200/ARQ	088	24000/V34	113
19200/ARQ/V32	090	24000/ARQ/V34	114
21600	091	26400/V34	115
21600/V32	093	26400/ARQ/V34	116
21600/ARQ	094	28800/V34	117
21600/ARQ/V32	096	28800/ARQ/V34	118
21600/VFC	097	2400/VFC	119
21600/ARQ/VFC	098	2400/V34	120
24000	099	2400/ARQ/VFC	121
24000/ARQ	100	2400/ARQ/V34	122
24000/VFC	101	4800/V34	124
24000/ARQ/VFC	102	4800/ARQ/VFC	125
4800/ARQ/V34	126	56000 (ISDN)	162
7200/VFC	127	56000/ARQ (ISDN)	163
7200/V34	128	56000/DIGITAL (ISDN)	164
7200/ARQ/VFC	129	56000/ARQ/DIGITAL (ISDN)	165
7200/ARQ/V34	130	64000 (ISDN)	166
9600/VFC	131	64000/ARQ (ISDN)	167
9600/V34	132	64000/DIGITAL (ISDN)	168
9600/ARQ/VFC	133	64000/ARQ/DIGITAL (ISDN)	169
9600/ARQ/V34	134	CHANNEL IN USE	170

Table 12 Result Codes

Message	#	Message	#
12000/VFC	135	CHANNEL IN USE	171
12000/V34	136	CHANNEL IN USE	172
12000/ARQ/VFC	137	CHANNEL IN USE	173
12000/ARQ/V34	138	CHANNEL IN USE	174
14400/VFC	139	CHANNEL IN USE	175
14400/V34	140	CHANNEL IN USE	176
14400/ARQ/VFC	141	CHANNEL IN USE	177
14400/ARQ/V34	142	CHANNEL IN USE	178
16800/VFC	143	CHANNEL IN USE	179
16800/V34	144	32000	180
16800/ARQ/VFC	145	32000/ARQ	181
16800/ARQ/V34	146	32000/x2	182
19200/VFC	147	32000/ARQ/x2	183
19200/V34	148	36000	184
19200/ARQ/VFC	149	36000/ARQ	185
19200/ARQ/V34	150	36000/x2	186
31200	151	36000/ARQ/x2	187
31200/ARQ	152	40000	188
31200/V34	153	40000/ARQ	189
31200/ARQ/V34	154	40000/ARQ/x2	191
33600	155	44000	192
33600/ARQ	156	44000/ARQ	193
33600/V34	157	44000/x2	194
33600/ARQ/V34	158	44000/ARQ/x2	195
48000	196	38666	220
48000/ARQ	197	38666/ARQ	221
48000/x2	198	38666/x2	222
48000/ARQ/x2	199	38666/ARQ/x2	223
32000	200	40000	224
32000/ARQ	201	40000/ARQ	225
32000/x2	202	40000/x2	226
32000/ARQ/x2	203	40000/ARQ/x2	227
33333	204	41333	228

Table 12 Result Codes

Message	#	Message	#
33333/ARQ	205	41333/ARQ	229
33333/x2	206	41333/x2	230
33333/ARQ/x2	207	41333/ARQ/x2	231
34666	208	42666	232
34666/ARQ	209	42666/ARQ	233
34666/x2	210	42666/x2	234
34666/ARQ/x2	211	42666/ARQ/x2	235
36000	212	61333	236
36000/ARQ	213	61333/ARQ	237
36000/x2	214	61333/x2	238
36000/ARQ/x2	215	61333/ARQ/x2	239
37333	216	64000	240
37333/ARQ	217	64000/ARQ	241
37333/x2	218	64000/x2	242
37333/ARQ/x2	219	64000/ARQ/x2	243

Disconnect Codes

To view Disconnect Codes, view the ATI6 screen.

Listed below are all Disconnect Codes and the numeric equivalent.

Table 13 Disconnect Codes

Verbal Reason	Numeric
Escape Sequence	001
ATH Command	002
Carrier Loss	003
Inactivity Timer	004
MNP Incompatibility	005
Reserved	006
Link Password Mismatch	007
Retransmit Limit	009
LD Received	010
Loop Loss	011
Invalid Speed	012

Table 13 Disconnect Codes

Verbal Reason	Numeric
Unable to Retrain	013
No Dial Tone	015
Key Abort	016
Busy	017
No Answer	018
Voice	019
No Answer Tone	020
No Carrier	021
Reason Not Determined	022
V42 SABME Timeout	023
V42 Break Timeout	024
V42 Disconnect CMD	025
V42 Id Exchange Failed	026
V42 Stepup No Good	027
V42 Invalid Code Word	028
V42 String Length to Long	029
V42 Invalid Command Code	030
No Failure Disconnect	031
V32 Cleardown Disconnect	032
RCU Dies In Mid Security	033
Remote RCU access Denied	034
loop lost durrinc connect est	035
DS0 issued idle pattern	036
Prompting Not Enabled	037
No Prompting In Sync	038
Non ARQ Mode	039
Mode Incompatible	040
No Prompting In NON-ARQ	041
PKT BUS - Generic Error	045
PKT BUS LINK ERR - (TX Pre ACK)	046
PKT BUS LINK ERR - (TX Tardy ACK)	047
PKT BUS - Transmit Bus Timeout	048
PKT BUS - Receive Bus Timeout	049

Table 13 Disconnect Codes

Verbal Reason	Numeric
PKT BUS LINK ERR - (TX TAL)	050
PKT BUS Link ERR - (RX TAL)	051
PKT BUS - Transmit Master Timeout	052
PKT BUS - Clock Missing	053
PKT BUS - Received LS while Link Up	054
PKT BUS - Out of Sequence Frame	055
PKT BUS - Bad Frame	056
PKT BUS - ACK Wait Timeout	057
PKT BUS - Received ACK sequence Err	058
PKT BUS - Received OverFlow RNR Fail	059
PKT BUS - Received Msg Buf Overflow	060
Received Disconnect command from Gateway Card	061
Token passing timeout	062
MNP protocol violation	064
More than 128 Unacked LM-Is	067
Resources for call are unavailable	068
Reserved	069
PRI request timeout	070
Abort analog destination over ISDN	071
Normal user call clear	072
Normal unspecified event	073
Bearer incompatibility	074
Unspecified protocol error event	075
Abnormal Disconnection	076
No cause value available	077

C

ADDRESSING SCHEMES

This chapter contains the following information:

- IP Addressing Basics
- Supernetting
- IP Subnet Mask Address Table

IP Addressing Basics

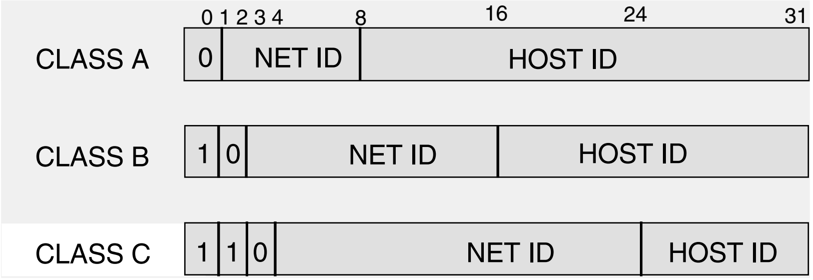
Administrators generally use three address classes in IP, with address ranges as follows:
Class A - 0-127; Class B - 128 - 191; and Class C - 192 - 248.

IP addresses are 32 bits long and generally written in dotted decimal notation: four decimal values separated by periods, followed by a forward slash and the associated subnet mask. For example, 192.77.203.5/255.255.255.0.

The same 32 bits can be divided in a number of different ways to indicate networks and subnetworks of different sizes. Imagine that the node addresses are no longer the physical addresses of your network interface cards, but arbitrary numbers that are mapped to those physical addresses later. You could then accommodate varying network structures from a small number of network segments with huge numbers of nodes to large numbers of networks with only a few nodes.

In the figure below, notice that the position of this line is determined by the position of the first zero bit in the address.

Figure 1 Address Class Map



Subnetting

A large IP network can be subdivided into smaller subnetworks. This is done using a subnet mask (in this text, often called netmask), which tells a routing device how to further subdivide the Host ID portion of an IP address.

A subnet mask is a 32 bit value which is written in dotted decimal notation. It contains a number of bits set to 1 (indicating the network portion of an address) followed by a number of bits set to 0 (indicating the host portion of an address).

For example, a netmask of 255.255.255.0 on a Class B network indicates that the network is divided into 254 subnetworks of 254 nodes each (0 and 255 are reserved numbers). 128.5.63.28 is host 28 on subnetwork 63 of that network. The natural network itself is 128.5.0.0 (Class B network).

Notice that by using subnet masks, you can define a natural hierarchy in which the addresses themselves indicate how a packet is to be routed. But, all routing devices on an IP network must be using the same subnetting scheme.

Also note that a subnet mask for a given network segment is not part of the address and is not transmitted with every packet. It is simply a value which is known to all the routing devices adjacent to that segment.

Subnets of Class C networks

The following table is a listing of all possible values for the last octet (byte) in a Class C subnet mask.

Figure 2 Class C subnet masks

Mask	Binary	Subnets	Hosts/Subnet
128	10000000	0	0
192	11000000	2	62
224	11100000	6	30
240	11110000	14	14
248	11111000	30	6
252	11111100	62	2
254	11111110	126	0

Two important points about the address divisions created by a subnet mask:

- RFC 950 requires that the first and last subnet created by a mask are reserved. So, the number of usable subnets is always 2 less than the number of divisions created. This makes 128 an unusable netmask because it has no legal subnets!
- The first and last host address in each subnet are also reserved (see “Reserved Addresses” below). This means 254 is also an unusable subnet mask because there are no legal host addresses!

Reserved Addresses

In most IP machines, setting all the bits in the host portion of an IP address to 1 indicates a broadcast to all nodes on the network. In the Class B network described above, an address of 128.5.255.255 is a network broadcast address meaning the packet is destined for all nodes on the entire Class B network. 128.5.63.255 would be a broadcast address indicating that the packet is destined for all nodes on subnet 63.

But, one old version of TCP/IP instead considers an address in which the host bits are all set to 0 a broadcast address. For RAS 1500, you configure for this difference as part of basic setup.

On networks with a “high” broadcast address, setting all bits to 0 simply means “this host” or “this network” and is usually used only when a node does not know its own network or node address (and is probably requesting that information).

One other reserved address is 127.x.x.x. The contents of the last three bytes are not important. This is a loopback address used for troubleshooting. It allows you to verify that a device can send something to itself. A packet with this address does not leave the machine that sent it.

Supernetting

Because Class B Internet addresses are in short supply, larger networks are now usually granted a contiguous block of several Class C addresses. Unfortunately, this creates very large routing tables since multiple Class C routes have to be defined for each network containing more than 254 nodes. Larger routing tables mean more work for the routers and, therefore, poorer performance.

Supernetting is only supported by RIPv2.

With traditional IP, each class C network must have a routing table entry.

Supernetting, or CIDR (Classless InterDomain Routing), is a technique that allows each of these larger networks to be represented by a single routing table entry.

To do this, supernet addressing does something very different from traditional TCP/IP routing (which allows only one netmask per network). In supernet routing, each supernet can be assigned its own netmask.

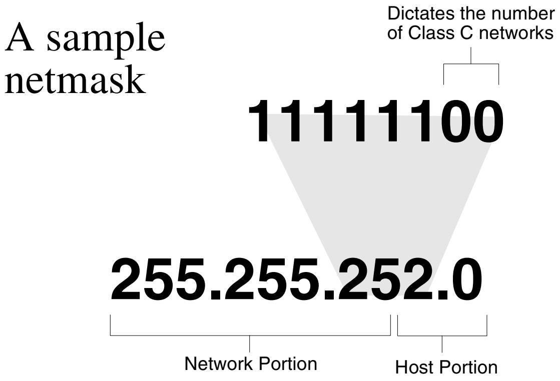
Since supernet addressing is a fairly complex mechanism, the easiest way to understand it is to step through the setup process.

Step 1 - Select a netmask for each supernet

Each supernet must have a netmask assigned to it. The netmask for an individual supernet can be, but does not have to be, the same as the netmask for any other supernet.

As in subnetting, a netmask creates a division between the network portion of an address and the host portion of an address. However, since the network you are defining is larger than a Class C network, the division you are creating is not in the fourth octet of the address. This example creates supernets composed of fewer than 254 Class C networks. So, their netmasks are actually splitting up the third octet in their IP addresses. See Figure 3.

Figure 3 Sample CIDR Netmask



Notice that the number of zero bits in the third octet actually dictates the number of Class C networks in the supernet. Each zero bit makes the supernet twice as large. So, a supernet composed of 8 Class C networks would actually have 3 zeroes (8 = 23).

This would seem very limited since it restricts you to using groups that nicely fit into a power of 2 (1, 2, 4, 8, 16...). However, inconveniently-sized supernets can be accommodated because of a simple fact: a netmask with more 1 bits will override a netmask with fewer 1 bits.

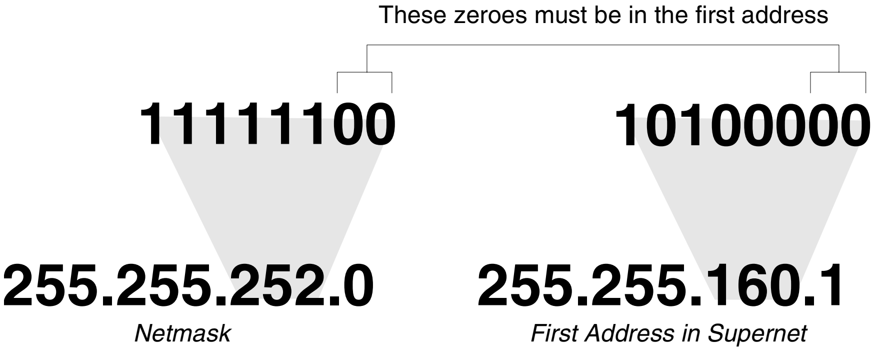
This allows a smaller supernet to share the address space of a larger supernet. If, for example, you had a supernet of size 6 and a supernet of size 2, you could assign the larger supernet an 8 network address space and assign the smaller supernet the portion of that address space that the larger supernet was not using.

Because the smaller supernet netmask has more 1 bits, packets whose address was part of its address space would be routed to the smaller supernet even though the address is *also* part of the address space dictated by the larger supernet netmask.

Step 2 - Select a range of addresses for each supernet

The range of addresses in a supernet must fit exactly into a space that can be described by its netmask. This means that the zero bits in the netmask must also appear in the first address of the supernet block. For this to be true, the third octet in the address must be an even multiple of the same power of 2 used to form the netmask. For example, if you had created a block of 8 networks, the third octet in the first address will be an even multiple of 8. See Figure 4.

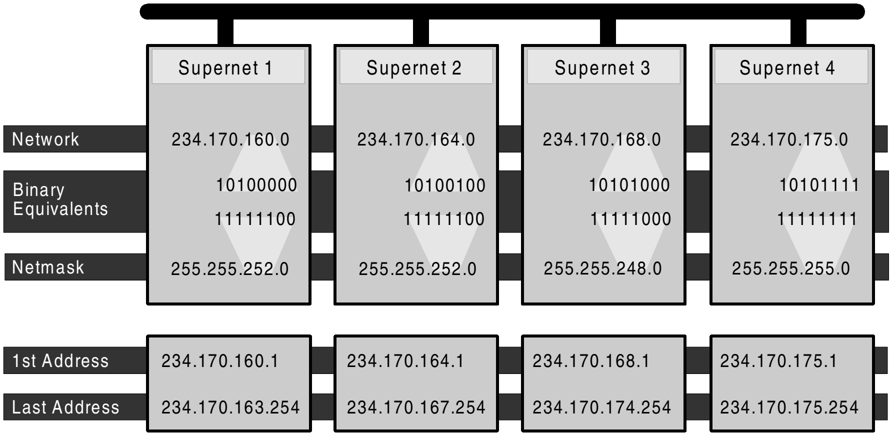
Figure 4 Selecting a Range of Addresses


These zeroes must be in the first address
11111100
10100000
255.255.252.0
Netmask
255.255.160.1
First Address in Supernet

Supernet Example

The four networks in Figure 5 are all connected to the same Internet service provider (ISP). The ISP has decided to use supernetting to reduce the size of his routing tables and improve throughput.

Figure 5 Supernet example



	Supernet 1	Supernet 2	Supernet 3	Supernet 4
Network	234.170.160.0	234.170.164.0	234.170.168.0	234.170.175.0
Binary Equivalents	10100000 11111100	10100100 11111100	10101000 11111000	10101111 11111111
Netmask	255.255.252.0	255.255.252.0	255.255.248.0	255.255.255.0
1st Address	234.170.160.1	234.170.164.1	234.170.168.1	234.170.175.1
Last Address	234.170.163.254	234.170.167.254	234.170.174.254	234.170.175.254

- Supernets 1 and 2 each require four Class C networks, so they require a netmask with 2 zero bits ($4 = 2^2$) in the third octet. This yields a netmask of 255.255.252.0.
- Supernet 3 requires 7 Class C address spaces. Since 7 isn't a power of 2, we have to round it up to eight. This gives it a netmask of 255.255.248.0.
- Supernet 4 is a single Class C network, making it s netmask 255.255.255.0

Now, assign ranges of addresses. Assume that the ISP is responsible for the network 234.170.0.0 and that its first free addresses are at 234.170.158.0.

The third octet of Supernet 1 has to be an even multiple of 4, so the ISP grants an address range starting at 234.170.160.0 and hopes that the block between 158 and 160 can be filled in later.

Supernet 2 must also begin on an even multiple of 4. The first available address after Supernet 1 conveniently fits the bill. So, supernet 2 extends from 234.170.164.1 to 234.170.167.254.

Supernet 3 requires an even multiple of 8. It also can begin on the next available address.

Since supernet 4 can fit entirely in a single Class C address space, it can use the supernet 3 surplus space. It is therefore given the last Class C address space in the Supernet 3 territory, effectively reducing supernet 3 to only the 7 class C networks it needs.

Supernetting and RAS 1500

In order to define a supernet you must add the network address and its netmask. You have two options. The first option permits you to set the subnet numerically (8-30 bits). For example:

```
add ip network houston 192.75.202.99/23
```

Secondly, you can specify a class designation: A, B or C. You can also leave the subnet value blank and let RAS 1500 choose it for you. In this case, however, RAS 1500 will specify a class setting based on the IP address. For example:

```
add ip network houston 192.75.202.99/C
```

To avoid confusion when configuring an IP address and subnet mask, be aware that a dialup client subnet class designator is specified as /h (host). This occurs by default with pool addresses and specified addresses, as well as addresses learned from the client. The h designates a mask of all 1 bits (255.255.255.255).

This value can be used only when the station being identified is a host. Networked nodes still require class or numeric (32 bits) subnets. For example:

```
set network user houston remote_ip_address 234.170.168.1/h
```

IP Subnet Mask Address Table

Subnet masking is used to expand the number of networks due to the 32-bit limitation of the IP address field. When assigned an address by the NIC, the address can be further broken down to expand the single net number to many more by using host bits.

Sub-net Bits	Bit Positions	Decimal Mask	HEX Mask	Sub-Nets Available	Hosts Available
Class A	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh	255.0.0.0	FF-00-00-00	126	16777124
Class B	10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh	255.255.0.0	FF-FF-00-00	16384	65534
2	10nnnnnn.nnnnnnnn.sshhhhhh.hhhhhhhh	255.255.192.0	FF-FF-C0-00	2	16382
3	10nnnnnn.nnnnnnnn.ssshhhhh.hhhhhhhh	255.255.224.0	FF-FF-E0-00	6	8190
4	10nnnnnn.nnnnnnnn.sssshhhh.hhhhhhhh	255.255.240.0	FF-FF-F0-00	14	4094
5	10nnnnnn.nnnnnnnn.ssssshhh.hhhhhhhh	255.255.248.0	FF-FF-F8-00	30	2046
6	10nnnnnn.nnnnnnnn.sssssshh.hhhhhhhh	255.255.252.0	FF-FF-FC-00	62	1022
7	10nnnnnn.nnnnnnnn.sssssssh.hhhhhhhh	255.255.254.0	FF-FF-FE-00	126	510
8	10nnnnnn.nnnnnnnn.ssssssss.hhhhhhhh	255.255.255.0	FF-FF-FF-00	254	154
9	10nnnnnn.nnnnnnnn.ssssssss.shhhhhhh	255.255.255.128	FF-FF-FF-80	510	126
10	10nnnnnn.nnnnnnnn.ssssssss.sshhhhhh	255.255.255.192	FF-FF-FF-C0	1022	62
11	10nnnnnn.nnnnnnnn.ssssssss.ssshhhhh	255.255.255.224	FF-FF-FF-E0	2046	30
12	10nnnnnn.nnnnnnnn.ssssssss.sssshhhh	255.255.255.240	FF-FF-FF-F0	4094	14
13	10nnnnnn.nnnnnnnn.ssssssss.ssssshhh	255.255.255.248	FF-FF-FF-F8	8190	6
14	10nnnnnn.nnnnnnnn.ssssssss.sssssshh	255.255.255.252	FF-FF-FF-FC	16382	2
Class C	110nnnnn.nnnnnnn.ssssssss.hhhhhhhh	255.255.255.0	FF-FF-FF-00	2097152	254
2	110nnnnn.nnnnnnnn.nnnnnnnn.sshhhhhh	255.255.255.192	FF-FF-FF-C0	2	62
3	110nnnnn.nnnnnnnn.nnnnnnnn.ssshhhhh	255.255.255.224	FF-FF-FF-E0	6	30
4	110nnnnn.nnnnnnnn.nnnnnnnn.sssshhhh	255.255.255.240	FF-FF-FF-F0	14	14
5	110nnnnn.nnnnnnnn.nnnnnnnn.ssssshhh	255.255.255.248	FF-FF-FF-F8	30	6

6	110nnnnn.nnnnnnnn.nnnnnnnn.sssssshh	255.255.255.252	FF-FF-FF-FC	62	2
Class D	1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx				
Future	11110xxx.xxxxxxxx.xxxxxxxx.xxxxxxxx				
All 1s	11111111.11111111.11111111.11111111				
All 0s	00000000.00000000.00000000.00000000				
0 = binary 0 1 = binary 1 n = network bits h = host bits s = subnet bits x = other					

D EVENT MESSAGES

This appendix contains the following information:

- Event Logging
- Event Logging Levels
- Event Logging Counters
- Using SYSLOG
- Event Message Examples

Event Logging

The RAS 1500 event logging system logs important information about RAS 1500 processes to a number of logging sinks. Logging sinks are destinations to which event information is sent (for example, a console or SYSLOG host) in the form of event messages. RAS 1500 is capable of logging event data to:

- SYSLOG host(s)
- the Console (local)
- a local FLASH file
- a TELNET session via the `show event` command

SYSLOG Host Event Logging

You can use the SYSLOG daemon to log RAS 1500 events to one or more remote hosts. Event messages are sent to a SYSLOG server via UDP using port # 514 - the standard UDP port for SYSLOG messages.

When ICMP logging is *enabled*, the following ICMP events are logged to SYSLOG:

- Sent Dest Unreachable
- Sent ICMP TimeExceeded
- Rcvd ICMP TimeExceeded

- Sent Parameter Problem
- Rcvd Parameter Problem
- Rcvd Source Quench ICMP
- Rcvd TimeStamp REQ ICMP
- Rcvd Address Mask REQ ICMP
- Rcvd Address Mask Reply ICMP
- Rcvd Router Solicitation ICMP
- Sent Router Advertisement ICMP
- Sent ICMP Redirect (Recv'd ICMP Redirect messages are not logged)

Console Event Logging

Event messages are automatically displayed on a local console. Of all ICMP messages generated, only *Received Destination Unreachable* messages are logged to the console.

Local FLASH File Event Logging

RAS 1500 event logging maintains a file - *log-file.local* - in the FLASH file system that contains a circular buffer of the last 20 event messages generated by RAS 1500. You can define a threshold for events written to this file. The default is *critical*, meaning only critical events are written to this file.

If RAS 1500 crashes and is rebooted, either manually or automatically, messages generated before the crash may not reach SYSLOG or Console logging facilities. But, the local FLASH file should contain the critical event messages generated just prior to the crash so that you can determine the cause of the error.

TELNET Session

All events normally directed to the Console only can also be echoed to the TELNET or dial-in session you’re running by issuing a `show events` command (the `hide events` command disables the function).

Event Logging Levels

RAS 1500 processes are accomplished through a number of facilities, (for example, TELNET, SLIP, or IP routing). Various event messages are generated for each facility, and are sent to any logging sinks that you have defined. For each RAS 1500 facility, you can specify the level of event information sent.

Although the logging level of each event is fixed, you can configure the level of messages that are sent to a specific logging sink. Logging levels are:

- *Critical* — A serious system error that may affect the integrity of the system
- *Unusual* — An event that normally does not happen, but from which the system should recover
- *Common* — A normal event
- *Verbose* — A normal occurrence that happens frequently

You can configure whether event messages are sent to a logging sink according to the level of the message. For example, if you wanted to see only the *unusual* and *critical* events messages generated by the TELNET facility, you would set the event level threshold for TELNET to *unusual*.

Use the following command to list RAS 1500 facilities and their default log levels:

```
list facilities
```

Do not confuse `set facility` *and* `set syslog` *commands.* `Set facility` *determines which messages are generated on the console or to a telnetted PC - depending on the loglevel specified for each facility. The* `set syslog` *command, on the other hand, determines which messages are saved - depending on the global loglevel you've set for the particular SYSLOG host.*

Event Logging Counters

RAS 1500 keeps a running tab of packets successfully and erroneously generated by various processes. These *counter* commands can be used in addition to the SYSLOG to monitor system-wide performance of RAS 1500 facilities. The `show ICMP counters` command, for example, details many input and output counters for ICMP packets. See Chapter 4, "Router Command Reference," for more information.

Using SYSLOG

This section describes how to configure RAS 1500 to send event messages to the SYSLOG host you define. The first step (below) involves setting up your SYSLOG server to receive data from RAS 1500.

Configuring SYSLOG Hosts on RAS 1500

You can define separate SYSLOG hosts to which event messages are logged by the event logging level associated with the message. For example, you can configure a SYSLOG host to log event messages with a Critical logging level only, while another SYSLOG host logs Unusual or Critical event messages.

To configure a SYSLOG host, use the following CLI command:

```
add syslog <ip name or address> facility <facility_node>
loglevel <loglevel choice>
```

- *ip name/address* is the network designation of the syslog host to which you want event messages sent.
- *facility* is the syslog node priority to which syslog messages are sent. The choices are:
  - *log_auth*
  - *log_local0*
  - *log_local1*
  - *log_local2* ... and so forth to *log_local7*

For example, to define a SYSLOG host logging common, unusual, and critical events, type:

```
add syslog 191.54.42.115 facility log_auth loglevel common
ENTER
```

Setting the Event Log Level

You can set the log level for each RAS 1500 facility. By setting the event log level, you define the level at which you want messages associated with the facility to be displayed on the console port. Messages associated with a selected loglevel are displayed along with any more serious log levels.

For example, if you set the event log level for the IP facility to Critical, RAS 1500 will only send *critical* event messages to the console port.

To set the log level of a facility, use the following command:

```
set facility <facility_name> loglevel <loglevel choice>
```

For example, to set the loglevel of the IP facility to Unusual (only messages that are *unusual* and *critical* are sent to the Console port) type:

```
set facility IP loglevel unusual  ENTER
```

To display the list of facilities and their associated log levels, use the following command:

```
list facility  ENTER
```

Event Message Examples

RAS 1500 is capable of delivering hundreds of event messages, from common events to critical events. This section describes some representative event messages that are generated by RAS 1500 facilities. Each event message is categorized by the facility by which it is generated.

The message description includes information about the meaning of the message, and if necessary, any corrective action you can take.

IP Messages

"ip_fwd_add_ondemand: ondemand route %lx exists already"

Meaning: The administrator tried to add an ondemand user that has been configured with a remote IP address already being used by another user

Action: Select a different remote IP address for the user being configured

"ip_fwd_get_opt: no more IP address available for dynamic address assignment"

Meaning: There are no more available addresses in the IP address pool

Action: Increase the size of the IP address pool using the `set ip pool` command

"ip_addr_pool_init: attempting to initialize the ip address pool with an illegal value (X), current ip address pool starting address Y. \n"

Meaning: The administrator tried to specify a starting address for the IP address pool which is illegal. The address is either '0' or has a network prefix of '0'

Action: Specify a legal IP address as the start of the pool

"ip_addr_pool_init: bad address pool range (%lx), the value must be between 1 and 254. \n"

Meaning: The administrator tried to specify the size of the IP address pool using a value that is either too big (greater than 254) or too small

Action: Specify a pool size that is within this range using the `set ip pool <name> size` command

"ip_send_common: on demand route, X, input queue overflow. One packet dropped\n"

Meaning: When a call to an on-demand address is being established, IP datagrams for that address are queued. If the queue fills up before a call can be completely established, subsequent datagrams are dropped

Action: This message is informational. No action is required

"ip_fwd_get_opt: duplicate ip address %lx\n"

Meaning: A dial-in user tried to use an address already allocated for another dial-in user

Action: Re-configure the dial-in user to use a different remote IP address

"ipCfmSet_ipRoute: gateway of destination X, mask Y is not reachable. static route not added\n"

Meaning: The administrator tried to define a static route using a gateway that is not reachable via any of the existing IP routes

Action: Specify a different gateway that has an IP address that can be reached

"proxy_arp_insert: no common network address found for remote ip address X"

Meaning: A network user is connecting to the system using an IP address that is not on the same IP subnetwork as the network defined for the system's LAN interface. Therefore, no proxy ARPing will be performed for this user.

Action: Informational message. No action required

"IP routes created for ondemand users cannot be deleted this way. Disable the user to delete the route."

Meaning: The administrator tried to delete an IP route that was created for an on-demand user. These routes can only be deleted by disabling the user

Action: Delete the route using the `disable user` command

"The route destination (X) should not contain more bits than are specified in the route mask (Y)"

Meaning: The administrator tried to add an IP route where the network prefix of the destination contains more bits than are specified in the network mask

Action: If no netmask is specified, the natural mask of the address is assumed. To specify a host route, you must specify /H as the netmask. For example:

```
add ip route 204.249.182.199/H
```

"Failed to delete the route to X. Only routes marked as Static/NetMgt can be deleted."

Meaning: The administrator tried to delete an IP route that cannot be deleted

Action: Informational message. No action required

"Failed to create static or default route. The IP subnet for the specified gateway does not exist or is disabled."

Meaning: The administrator tried to add an IP route over an interface which is disabled or down

Action: Enable the interface before adding the route

"ip_fwd_add_ondemand: ondemand IP network address (X) conflicts with an IP network that already exists.\n"

Meaning: The administrator has defined an on-demand user whose remote IP address is already being used by an existing IP network

Action: Change the on-demand user's remote IP address to one that does not conflict with any existing networks.

Use the `list ip net` *command to view IP network addresses currently in use.*

Call Initiation Process Messages

"CIP: Unable to find an available default host for user %s, %x/n"

Meaning: The user tried to connect to a host from the login host table, but there is no available host

Action: The login host table is probably empty. Add a host to the table and let the user dial in again

"CIP: No available modem is found for modem group, %s/n"

Meaning: There is no available modem in the modem group

Action: If there is no modem available, the user should wait until one becomes available. If the modem group contains a subset of the available modems, you can add modem interfaces to this modem group

"CIP: The port is disabled for login services, %x/n"

Meaning: The user is a login user, but the interface is configured for network users

Action: Set the port_type to *login_network* or *login*

"CIP: The modem group %s already exists /n"

Meaning: The administrator tried to configure a modem group, but the modem group already exists

Action: Choose another modem group name

User Manager Messages

"AUTH: Unable to authenticate if both authentication IP's are set to 0"

Meaning: The user may not be defined locally, remote authentication is not enabled, or a remote authentication IP address is not configured

Action: Define the user locally or configure a RADIUS server IP address

"AUTH: Unable to account if both accounting ip's are set to 0"

Meaning: Remote accounting is enabled, but no RADIUS accounting server IP addresses have been configured

Action: Either disable remote accounting or configure a RADIUS accounting server IP address

"AUTH - Most likely client/server configuration mismatch"

Meaning: The RADIUS secret configured on RAS 1500 does not match the secret configured on the RADIUS server, or an invalid RADIUS server is trying to contact RAS 1500

Action: Ensure the secret is identical on RAS 1500 and RADIUS server

Filter Manager Process Messages

"FM: In filter file <name> had no rules for <protocol> protocol"

Meaning: A filter protocol section is defined, but there are no rules associated with it.

Action: A protocol section must either contain at least one rule, or be commented out for the syntax to be valid

"FM: In filter file <name>, previously defined section <protocol section name>"

Meaning: There are two protocol sections that use the same name, for example, you defined two IP protocol sections in the filter file

Action: Delete one of the duplicate protocol sections

"FM: In filter file <name>, ambiguous first line"

Meaning: The filter file does not contain the required file descriptor on the first line

Action: Place file descriptor (#filter) on first line of file

UDP Messages

"UDP - could not get source IP address"

Meaning: RAS 1500 tried to send a UDP message (for example, an SNMP trap or syslog message) with no IP networks enabled

Action: Create an IP network

Configuration File Manager Messages

"Could not get my own Mailbox Handle."

Meaning: The Configuration File Manager process could not resolve its own mailbox

Action: Reboot the system

"Could not resolve @mailbox://MIBRegistrar."

Meaning: The Configuration File Manager could not resolve the MIB Registrar mailbox

Action: Reboot the system

"The configuration file <filename> is corrupt. Status <error status>."

Meaning: The Configuration file has been corrupted. It will be renamed to <filename>.bad

Action: Keep a copy of the <filename>.bad file. If the file was uploaded to using TFTP, upload the file again making sure the TFTP transfer mode is set to octet

"Could not create a list for CFM Control Structures. Status: <error status>."

Meaning: The Configuration File Manager could not allocate the resources necessary for normal operation

Action: Reboot the system

TELNET Messages

"CIP_GET_SHARED_DEV_REQ failed: no modems available"

Meaning: A user is attempting to TELNET to RAS 1500 to perform modem sharing, but there are no free modems available for the group defined

Action: Use the list service command to see which modem group is configured. Determine why all modems in the modem group are being used

"User X attempted CLI access without dial-out privileges. \n"

Meaning: A user is attempting to TELNET to RAS 1500 to perform modem sharing using a valid username and password, but the user profile does not have dial-out enabled

Action: Use the `set user <name> type dial_out` command to enable dial-out privileges for the user

IP Dial-out Process Messages

"INIT: Could not allocate a private data area. Status: <error status>."

Meaning: The dial-out process could not allocate enough memory for its data. The dial-out process will not be started

Action: Free some memory, for example, delete some users. Once some memory has been freed, save the configuration and reboot the system

"Could not register socket <socket> with the IP forwarder. Status: <error status>(<error value>)."

Meaning: The dial-out process failed to register its socket with the IP forwarder. The IP dial-out service will not be started

Action: Ensure the IP forwarder process is running by using the `list processes` command. Ensure that there is an IP network defined. Reboot the system and re-enable the dial-out service

"Could not unregister socket <socket> with the IP forwarder. Status: <error status>(<error value>)."

Meaning: The dial-out process failed to unregister its socket with the IP forwarder. This message is displayed only when disabling the dial-out network service

Action: When the IP dial-out service reaches this state, it cannot be enabled again without rebooting. Reboot the system

"Could not register the IP Dial-out service with SAP. Status: <error status>(<error value>)."

Meaning: The dial-out process failed to register the IP dial-out service with the SAP process. The IP dial-out service will not be started

Action: If the dial-out service is enabled, disable the dial-out service and re-enable the dial-out service. If message is displayed again, reboot the system

"Could not set the IP ACS timer. Status: <error status>(<error value>). The IP Dial-out service will be automatically disabled."

Meaning: The dial-out process could not start its service timer. This timer is required for normal operation. The dial-out network service will not be enabled

Action: A system error occurred. If re-enabling the dial-out network service fails, reboot the system

"There are no interfaces assigned to the Dial-out process' modem groups."

Meaning: The dial-out process detected that there were no interfaces contained in the modem group it was assigned to use

Action: Verify that at least one interface has been assigned to the dial-out service modem group. If no interface is assigned, add at least one interface to the dial-out service modem group and re-enable the dial-out service

INDEX