NETServer 8/16 Plus

CLI Reference Guide

US Robotics®

The Intelligent Choice in Information Access

2

Table of Contents

CLI Reference Guide

4

CLI Reference Guide

6

CLI Reference Guide

CLI Reference Guide   9

10

SHOW...**111**

CLI Reference Guide   11

12

TELNET COMMANDS..144

CLI EXIT COMMANDS...145

COMMAND FEATURES..145

14

Warranty and Service

U.S. Robotics Access Corp. Limited Warranty

Your U.S. Robotics® product is covered by a Limited Warranty. U.S. Robotics warrants that the product that you have purchased from U.S. Robotics or from a U.S. Robotics authorized reseller is free from defects in materials or workmanship during the Limited Warranty period, identified in the chart below, which is effective on the date of purchase.

During the Limited Warranty period, U.S. Robotics will repair or replace the product with the same or a similar model, which may be a remanufactured unit, at U.S. Robotics option, without charge for either parts or labor. Replacement parts assume the remaining warranty of the parts they replace. This Limited Warranty extends only to the original purchaser and is non-transferable.

The chart below identifies the terms of the factory repair/replacement warranty, as well as software/firmware updates and telephone support services included with the U.S. Robotics Limited Warranty.

	Free Telephone Support	Free Software/Firmware Updates	Hardware Support
NETServer Product Family	For 90 days, effective upon purchase	For 90 days, effective upon purchase	2 years Factory Repair/ Replacement

What Is NOT *Covered By the Limited Warranty*

Items not covered by the Limited Warranty include, but are not limited to, the following:

- Product installation support

- A product purchased from anyone other than U.S. Robotics or a U.S. Robotics authorized reseller

- Routine cleaning, or normal cosmetic and mechanical wear

- A product that is modified, tampered with, misused or subjected to abnormal working conditions, including, but not limited to, lightning and water damage

- Damage from repair or replacement of warranteed parts by anyone other than U.S. Robotics or a U.S. Robotics authorized service provider

THIS LIMITED WARRANTY DOES NOT GUARANTEE YOU UNINTERRUPTED SERVICE. REPAIR OR REPLACEMENT AS PROVIDED UNDER THIS LIMITED WARRANTY IS THE EXCLUSIVE REMEDY OF THE PURCHASER. THIS LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANT OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE OR PURPOSE. U.S. ROBOTICS SHALL IN NO EVENT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND OR CHARACTER, INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUE OR PROFITS, FAILURE TO REALIZE SAVINGS OR OTHER BENEFITS, LOSS OF DATA OR USE, DAMAGE TO EQUIPMENT AND CLAIMS AGAINST THE PURCHASER BY ANY THIRD PERSON, EVEN IF U.S. ROBOTICS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Jurisdiction Laws

This Limited Warranty gives you specific legal rights. You may have others, which vary from jurisdiction to jurisdiction. Some jurisdictions do not allow limitations on duration of an implied warranty, or the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.

© 1997 U.S. Robotics. All rights reserved. U.S. Robotics and the U.S. Robotics logo are registered trademarks of U.S. Robotics.

How To Access Your Warranty Services

Telephone Support

Warranty

For 90 days, effective upon product purchase, you have access to our technical support analysts. To get telephone support under the conditions of this Limited Warranty, call the USR no. on the next page.

16

Area	North America	Europe, Middle East, Africa	All Other Locales
Phone No.	1-800-231-8770 (toll free)	353-1-205-7700	1-847-797-6600
Weekdays	Monday - Friday	Monday - Friday	Monday - Friday
Time	7. a.m. - 8 p.m.	9 a.m. - 7 p.m.	7 a.m. - 8 p.m.
Time Zone	Central Standard Time	Central European Time	Central Standard Time

What Information Should I Have Ready Before Calling For Support?
> To enable U.S. Robotics to respond to your inquiry as efficiently and effectively as possible, please have available as much of the following general and product-specific information as possible before calling.

General Information
> √ Serial number & part number (both are contained within the barcode affixed to the unit)
> √ Product model name and number
> √ Detailed, specific questions

Product-Specific Information
> √ Applicable error messages
> √ Add-on boards or hardware
> √ Third-party hardware or software
> √ Operating system type and revision level

Telephone Support Options
> Customers who require telephone support beyond 90 days from the purchase date will be referred to a U.S. Robotics sales representative to establish a service contract, if desired.

Software/Firmware Updates

Warranty
> *For 90 days, effective upon product purchase*, you will have access to U.S. Robotics' Systems Software/Firmware Updates from the U.S. Robotics' Network Systems Division web site: ***http://totalservice.usr.com***

Software/Firmware Update Options
Customers who require Software∕Firmware updates beyond 90 days
from the purchase date will be referred to a U.S. Robotics sales
representative to establish a service contract, if desired.

Hardware Support

Warranty
During the applicable Limited Warranty period, if U.S. Robotics
determines your product requires servicing, you will be given a Service
Repair Order (SRO) number to help us track your Limited Warranty
request.

> **IMPORTANT**: Once you have received your SRO number, mail the
> product, postage prepaid and insured, to the shipping address on
> page 19. Please be sure your SRO number is clearly visible on the
> outside of the package and pack your unit securely.

Call the appropriate U.S. Robotics no. below for Hardware Support.

Area	North America	Europe, Middle East, Africa	All Other Locales
Phone No.	1-800-231-8770 (toll free)	353-1-205-7700	1-847-797-6600
Weekdays	Monday - Friday	Monday - Friday	Monday - Friday
Time	7. a.m. - 8 p.m.	9 a.m. - 7 p.m.	7 a.m. - 8 p.m.
Time Zone	Central Standard Time	Central European Time	Central Standard Time

Shipping Checklist - Did You Include:

- √   Your Name
- √   Your Company's Name
- √   Return Shipping Address
- √   A Contact Telephone Number
- √   Serial & Part Numbers (contained in barcode attached to the unit)
- √   Brief Problem Description

Shipping Address

North America and Locations *Outside* Europe, Middle East & Africa	Europe, Middle East, Africa
U.S. Robotics ATTN: SRO Receiving 1800 W. Central Rd. Mt. Prospect, IL 60056-2293 SRO#....................................	U.S. Robotics Services, Ltd ATTN: RMA Department 5 Richview Office Park Clonskeagh, Dublin 14 Ireland

Hardware Support Options

Customers who require out-of-warranty hardware support will be referred to a U.S. Robotics sales representative to establish a service contract, if desired.

Technical Support

For technical assistance, contact the U.S. Robotics Systems Product Support Department in one of the following ways. Whichever method you use to contact us, please have the product serial number(s) available.

Mail	8100 North McCormick Blvd. Skokie, Illinois 60076-2999
Toll-Free Line	(800) 550-7800 or (800) 231-8700
America Online	Keyword USROBOTICS
CompuServe	GO USROBOTICS
Anonymous FTP	ftp.usr.com* Username=Anonymous Password=your internet address.
World Wide Web	http://totalservice.usr.com

*The FTP is for downloading files only.

Rev: 4/97

CLI Reference Guide   19

20

Introduction

This section describes some basic concepts of the CLI. It explains the syntax used throughout this document and the structure of the command language as an aid to understanding how commands are structured.

Command Format

Many commands are *position independent*, *multi-tiered* and use *keywords*. Multi-tiered commands let you type the base command (e.g.: **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 described in the example below:

add appletalk network <network_name>
  address_range [appletalk_range]
  { interface [eth:1] **}**

> **add appletalk network** is the command
> **<network_name>** is the (required) value for the command
> **address_range** is a required parameter
> **[appletalk_range]** is the value for the address_range
> parameter which you must provide
> **interface** is only required if you want to override the default
> value, which is *eth:1*

Parameters
- **{ … }** parameters enclosed by *curly braces* are required, and are provided with *default* values. You do not need to specify these parameters unless you wish to override the default.
- **< … >** required values for a command or parameter which are position dependent and do not have keywords are enclosed by *arrows*.
- **[…]** 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]

CLI Reference Guide   21

- ♦ **,** (comma) you can select *one or more* of the displayed *bitmasks*:
      [FIRST,SECOND,THIRD,...]
- *Position independent* arguments are shown in a vertical array following the command.
- 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".
- If a keyword is not *unique*, it will "ding". Then, if you wish to list possible keywords, you may use positional help (see next item).

Entering Commands

Commands can be abbreviated if the portion of the command you type is unique. For example, you can type **se us jay pa bird**, short for: **set user jay password bird**, but you can't type **se us jay m bird**, because **m** can stand for **message** or **modem_group**. You can use command completion and positional help when entering command strings. These are explained in detail in the section titled *Command Features* on page 145.

Using Control Characters

- While working in the CLI, system messages may scroll across your screen. You can recall the last thing you typed, using [Ctrl] **l** (ctrl l). 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** (ctrl c) to abort any currently executing and stacked commands.
- Commands can be *retrieved* by typing [Ctrl] **p** [ctrl p] (for previous) and [Ctrl] **n** [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.

22

- Command line editing allows these options: [Ctrl] **b** (ctrl b) or [←] (left arrow) brings you go back one character; [Ctrl] **b** (ctrl b) or [←] (left arrow) brings you back one character; [Ctrl] **f** (ctrl f) or [→] (right arrow) takes you forward one character; [Esc] **b** (Esc-b) takes you back one word; [Esc] **f** (Esc-f) takes you forward one word; [Ctrl] **a** (ctrl a) takes you to the beginning of a command; [Ctrl] **e** (ctrl e) takes you to the end of a command and [Ctrl] **k** (ctrl k) kills the line.

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"** isn't unique because **m** can stand for **message** or **modem_group**.

- For brevity, some commands in this *User Manual* are abbreviated and annotated *(abbr.)*.
  Some parameters are omitted in examples because they default to standard values and do not require entry, or are unecessary for common configuration. See the *CLI Reference Guide* for more.

- *Command completion* finishes spelling a unique, abbreviated value for you just by pressing the [Esc] (Esc) key. It's handy when you're in a hurry or uncertain about a command. For example, if you type **add ip n** [Esc] (Esc), it will spell out the keyword **network** without losing your place in the command syntax.

Help

- Help is *general* o*r positional*. Type **help <any command keyword>** to get a cursory list of associated commands and its 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

- 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 ROM. These changes are lost by NETServer if power fails before saving them.

CLI Reference Guide   23

- Many *delete* commands require that you first *disable* the process or function. For example, commands to delete a network user, interface, route, TCP connection, community name, network service and others must first be disabled.

- Wherever an *IP address* value is required, you can enter a host *name* provided you have configured a 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 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. Network addresses are shown in this document using the syntax described in the table on the next page. For help setting bitmasks manually, see *Appendix B: Addressing Schemes* in the *NETServer Plus User Manual* for a bitmask table.

Address Type	Format	Range
appletalk_address	net.node	1-65280.1-253 (decimal)
appletalk_range	net-net	1-65280 - 1-65280 (decimal)
IP_address	a.b.c.d	0.0.0.0 to 255.255.255.255 (decimal)
ip_net_address	a.b.c.d/mask	255.255.255.255/A,B,C,H (or 8, 16, etc.)
ipx_net_address	xxxx	hexadecimal
mac_address	xx:xx:xx:xx:xx:xx	hexadecimal digit pairs
ipx_host_address	xxxx.xx:xx:xx:xx:xx:xx	ipx_net_address. mac_address

Interfaces

Interfaces are expressed as variants of the **mod:*x*** format where *x* is a modem number (port) from 1-16 depending on your NETServer model. You can specify more than one interface or a range in several ways. For example:

set switched interface mod:1,mod:2,mod:3

set switched interface "mod:1 mod:2 mod:3"

set switched interface mod:[1-3]

set switched interface mod:[1-3],mod:15,int:[9-11]

24

Names

You can specify names for networks, users and other system entities. Names can be up to 32 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. Note that names are *case-sensitive.* Some examples are:

Desired name:	Entered as:
Eric's PC	"Eric'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 command is employed when making WAN network (dial-in) connections and for dial-out users.

Default User

The *default user* is a powerful and efficient tool created at system setup which 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 callback*, write:

set user default type callback

The parameters that can be configured across the board are indicated by a (D) when you type **show user** <name>. 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. Some common entities are:

CLI Reference Guide   25

- **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 command displays table entries. For example, LIST MODEM_GROUPS displays all defined modem groups.

The SHOW command displays detailed information about a specific table entry or a set of scalars (non-table items). For example, SHOW MODEM_GROUP USR displays information on the USR 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 DNS server. The DNS server with the highest preference number will be used first. Login hosts also require a preference number.

26

CLI Commands

ADD

Use the ADD command to define:

- networks you will connect to
- hosts you need to access
- SNMP communities
- users who will dial out, dial in, access the network, or use the CLI

Note that some parameters have default values.

add appletalk network <network_name>
                    address_range [appletalk_range]
                    { interface [eth:1] **}**
                    {enabled [yes | no]**}**

Defines an AppleTalk network and the interface used to connect to it. Each
AppleTalk network address allows up to 253 nodes to be attached. You must
add at least one zone name to your AppleTalk network before you can enable
it. Unlike most added networks, AppleTalk nets are not enabled by default.

Parameters	Description
<network_name>	Designation of AppleTalk network, up to 32 characters.
address_range	Address range of the network being added. For example, 1-5 defines five networks, addresses 1 through 5. Options are 1 through 65280. Address 0-0 may be used, but only if the system isn't used as a seed router. See *set appletalk network* on page 76 for details on the seed router.
enabled	Sets networks as enabled or not.
interface	Name of the interface that the network will transmit to and receive data on. The only option is eth:1.

For example:

    add appletalk network Net1 address_range 1-5

add appletalk zone <zone_name, zone_name…>
　　　　　　　　network <network_name> [Max of 5 names]

Defines the AppleTalk zones that will be a part of the AppleTalk network. A
zone name describes a logical network segment on a physical network. The
first zone on the list is the "default zone".

Parameters	Description
<zone name >	Designation of AppleTalk zone(s) to be added. No more than five names can be added at once. Limit: 32 characters.
network	Network designation you created earlier, where you are adding zones.

add dns host <host_name and domain_name> **address** <IP_address>

Adds the named host to the Local Host Table. When the system needs to
resolve an address for an IP host name, the Local Host Table is checked first,
before a request is sent to the remote DNS Name Server. *Note*: The *add
login_host* command may also add to this table. See that command's
description for details.

Parameters	Description
<host_name>	Designation of the local host.
address	IP Address of a named host in nnn.nnn.nnn.nnn format.

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. 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.

Parameters	Description
<IP_address>	IP Address of a server in nnn.nnn.nnn.nnn format.
preference	Specifies the order in which name servers are used.
name	Designation (optional) of the name server.

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 SNMP. A filter file is a text file stored in the FLASH file system that you load using TFTP. *Add filter* also verifies the syntax of the filter file. If syntax verification fails, you'll receive an error message, and the filter will still be added to the table, but is not usable. You must correct the filter file in a text editor, use TFTP to export the updated file to the system's FLASH file system, and use the *verify filter* command to check the filter's syntax.

Parameters	Description
<filter_name>	Designation of a filter file, up to twenty ASCII characters.

add framed_route user <name>
                      gateway [ip_address]
                      ip_route [ip_address]
                      metric [number]

Adds a framed (static) network to the user profile for dialup connections. This method of creating a static route does not run RIP to learn routes, so you must specify IP route and gateway addresses. See *add ip route* command.

Parameters	Description
<user name>	User name 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. Values are 1 through 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 serial* command to assign an initialization script to a switched interface, that string will be sent to the serial line driver whenever a connection terminates, to ready the modem for the next connection.

Parameters	Description
<script_name >	Designation of the init script, up to 7 ASCII characters.
command	Modem initialization string must be entered with double quotes, and be less than 56 characters. The string must end with the characters \\r\\n, which is interpreted by the system as carriage return, newline.

add ip defaultroute gateway <IP_address>
                          { metric [1] **}**

Defines a default gateway IP router, which acts as the default route for IP
packets destined for remote hosts.

Parameters	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. Values are 1 - 15.

add ip network <network_name>
                          address [ip_net_address]
                          frame [ETHERNET_II | SNAP]
                          { interface [eth:1] **}**
                          { enabled [yes] **}**

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

Parameters	Description
<network_name>	Name of IP network, consisting of up to 32 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 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 will generate it for you from the network address.
frame	Frame encapsulation to be used on this IP network. The options are: ETHERNET_II or SNAP.
interface	Name of the interface which this IP network will communicate over. The default is the first LAN interface (**eth:1**).
enabled	This optional parameter indicates whether the network is enabled (YES) or disabled (NO). Default: **YES**

add ip route <ip_net_address>
                    gateway [gateway_addr]
                    metric [hop_count]

Adds an IP static route entry to the IP Routing Table. IP packets destined for networks that match this network will be routed to this address. The command *list ip routes* displays your currently defined routes.

Parameters	Description
<net_address>	IP address of the remote 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 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 will generate it for you from the network address.
gateway	IP address of gateway used to reach this remote network.
metric	An integer representing how far away the route is, in "hops" through other routers. Values are 1 through 15.

add ipx network <network_name>
                address [ipx_address]
                { interface [eth:1] **}**
                { enabled [yes] **}**
                frame [ETHERNET_II | SNAP | DSAP | NOVELL_8023]

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

Parameters	Description
<network_name>	Name of IPX network. A unique ASCII string of up to 32 characters; white space must be surrounded by double quotes.
address	Address of the IPX network.
interface	Name of interface with which this IPX network will associate. The default is the first LAN interface (eth:1).
enabled	Optional parameter indicates whether network is enabled (YES) or disabled (NO). Default: **YES**
frame	Frame encapsulation to be used on this IPX network.

32

add ipx route <ipx_net_address>
　　　　　　　　　gateway [ipx_host_address]
　　　　　　　　　metric [metric_number]
　　　　　　　　　ticks [tick_number]

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

Parameters	Description
<ipx_net_address>	IPX network address requiring a route.
gateway	IPX address of the host which will act as a gateway. The format is nnnn.xx:xx:xx:xx:xx:xx (net_addr.mac_address).
metric	Number of "hops" through different routers needed to reach the remote IPX network.
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 number]
　　　　　　　　　gateway [network_number.mac_address]
　　　　　　　　　metric [metric]
　　　　　　　　　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 table on next page.

CLI Reference Guide　　　　　　　　　　　　　　　　　　　　33

Parameters	Description
service name	Designation of IPX service.
address	Internal network number for the IPX service on which this service resides.
gateway	Address of the router you defined as the gateway.
metric	An integer representing how far away the default router is, in "hops" through other routers. Values are 1 through 15.
node	The internal node number of the server on which the service resides. This is typically 00:00:00:00:00:01.
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's (or receiver's) IPX address and service type's port number.
type	Type of service: hex number referring to file server, print server, etc. Refer to the table below

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

34

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 a login host 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 will look up the address, using the DNS server that you define with *add DNS server*. Or, you can specify the IP address here. If you specify the IP address, it also will be added to the local DNS Table, which you can view using *list DNS hosts*. You can list the currently defined login hosts using *list login_hosts*.

Parameters	Description
<host_name>	Name or IP address that specifies an IP host.
address	This (optional) address will be added the DNS Local Host Table. If you do not specify an address here, the system will consult 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.
rlogin_port	This optional parameter specifies the port number that will be used when a user executes the rlogin CLI command, specifying this host.
telnet_port	This optional parameter specifies the port number that will be used when a user executes the TELNET CLI command, specifying this host.
clearTCP_port	This optional parameter specifies the port number that will be used when a user's application requests a ClearTCP session with this host

add modem_group <group_name>

Creates a modem group. To assign interfaces to this group, see following command.

CLI Reference Guide   35

add modem_group <group_name>
                     interfaces [interface_name,interface_name…]

Creates a modem group and assigns interfaces to the modem group. 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 modem group *All* is provided as a default modem group with all NETServer (8 or 16) modems included.

Parameters	Description
<group_name >	Name of the modem group, up to 32 characters. We recommend you limit the length of this name to eight characters. That will ensure the name will always display completely in certain list and show commands
interfaces	List of interfaces to be assigned to the modem group. The expected format is ssss,ssss,ssss... where the Interface Name must exist in the Interface Table. Interface names can be individual names, or ranges. A range must be in the format mod:[1-9].

add network service <service_name>
                     server_type [server_type]
                     socket [socket_number]
                     enabled [yes | no]
                     data ["string"]
                     close_active_connections [TRUE | FALSE]

This configures a network listener process that provides a certain type of service. To see the available server types, use the *list available servers* command. See table on next page.

Parameters	Description
<service_name>	Name of this type of service. Limit of 32 character ASCII string.
server_type	Designates the type of service being offered. Services currently available are: • **ClearTCPD** - enables access to a modem group • **DialOut** - for dial-out connections to IP or IPX hosts • **SNMPD** - SNMP agent • **TFTPD** - server for file transfers • **TELNETD** - TELNET server, either to the CLI or a modem group
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's (or receiver's) IP address and service type's port number.
enabled	Optional. Indicates whether the network is enabled (YES) or disabled (NO). When you add a network service, it is *disabled* by default. Within the command, be sure to add the enable value *after* any data value.
data	Ancillary Data. This field contains server-specific configuration data. See the table on the next page for configurable ancillary data parameters for TELNET.
close_active_ connections	Indicates whether or not to close any active connections when a service is disabled by the disable network_service command. The default is **FALSE**.

The table on the next page shows the configurable parameters for the TELNET services, which are specified with the data parameter.

Ancillary Data Parameters	Description

auth	On indicates that login/password authentication should be performed on incoming connections.
	  Format: **"auth=[on/off]"**
	  Default: on.

login_banner	ASCII string that will be sent to a client when the connection is made. It must be quoted.
	  Format: **"login_banner=[string]"**
	  Default: none.

login_prompt	ASCII string specifying the login prompt to be sent during authentication. It must be quoted.
	  Format: **"login_prompt=[string]"**
	  Default: "login:

service_type	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. This is applicable only to TELNET servers; you cannot ClearTCP into the system to manage.
	  Format: **"service_type=[manage, dialout]"**
	  Default: manage

modem_group	Used for modem sharing service, indicating the modem group the service will allocate a modem from. String must be quoted.
	  Format: **"modem_group="[string]"**
	  Default: none

drop_on_hangup	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.
	  Format: **"drop_on_hangup=[on/off]"**
	  Default: off

Add network service **examples:**

To configure a ClearTCP service to offer modem sharing on TCP port 2000, doing no authentication upon connect, using modem group Group1, type:

Note: all DATA values **must** be enclosed in *double quotations*.

add network service modem_sharing server_type cleartcpd socket 2000 data "auth=off,modem_group=\Group1\,service_type=dialout"

To configure a TELNET service to offer CLI access on port 4000, doing authentication upon connect and dropping the connection on hangup (abbr.):

add net ser CLI_access serv telnetd soc 4000 dat "drop_on_hangup=on"

add snmp community <community_name>
                    address [IP_address]
                    access [RO | RW]

Adds to the list of SNMP authorized users. 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*.

Parameters	Description
<community_name>	Group name that authorizes SNMP requests.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn
access	Determines what type of access to SNMP MIBs the added user will have. Options: Read Only (RO) and Read Write (RW).

CLI Reference Guide   39

add snmp trap_community <name>
                                     address <IP_address>

Adds to the list of community name/IP address pairs that are allowed to receive SNMP traps. You can see the list of authorized users with the *list snmp communities* command.

Parameters	Description
<name>	Group name defining who can receive SNMP traps.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn

add syslog <ip_name_or_addr> **loglevel** [loglevel]

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

Parameters	Description
<ip_name_or_address>	Host name or IP address of the Unix host that will receive syslog information.
loglevel	There are five levels of logging: • **CRITICAL** - a serious system error, which may effect system integrity • **UNUSUAL** - an abnormal event, which the system should be able to recover from • **COMMON** - a regularly occurring event that is not frequent • **VERBOSE** - a regular periodic event, e.g. a routing update message • **DEBUG** - for debugging only

40

add tftp client <ip_name_or_addr>

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

Parameters	Description
<ip_ name_or_addr>	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 [name]
>>**login_service** [RLOGIN | TELNET | CLEARTCP]
>>**network_service** [ARAP | PPP | SLIP]
>>**password** [password]
>>**enabled** [yes | no]
>>**type** [LOGIN,NETWORK,CALLBACK,DIAL_OUT, MANAGE]

Adds a user to the Local User Table. You may specify a type for the user, as well as login and network protocols, or use the defaults. The *list users* command displays these parameters for all users.

Parameters	Description
name	Name of user to be added, up to 32 ASCII characters.
password	User's password, up to 15 ASCII characters.
login_service	Protocol to be used for a login user. Options are: • **RLOGIN** • **TELNET** (*default*) • **ClearTCP**
enabled	Optional parameter indicates whether the network is enabled (YES) or disabled (NO) by this command.
network_service	Framed protocol to be used by network user. Options: • **ARAP** - the AppleTalk client software • **PPP** - Point to Point Protocol (*default*) • **SLIP** - Serial Line IP
type	Type of user - may be one or more types. • **LOGIN** uses the login_service specified. • **NETWORK** (*default*) uses network_service specified - a dial in user. • **CALLBACK** users are disconnected after authentication and called back. • **DIAL_OUT** - modem sharing or WAN users. • **MANAGE** users have administrative authority.

ARP

arp <ip_name_or_addr>

                  output [outputfile_name]

Prints the IP address (and Media Access Control Address [MAC] if on a locally connected network) of a network node to a file in FLASH or the CLI (default). If a node is not in the ARP cache, an ARP request will be sent out.

Parameters	Description
<ip_name_or_addr>	IP address or node name for the IP and MAC address you seek.

ASSIGN

assign interfaces <interface_name,interface_name,…>

                  modem_group <group_name>

Adds interfaces to an existing modem group or modem groups.

Parameters	Description
interface name	Interface names to be assigned to the modem group. The Interface Name must exist in the Interface Table. Interface names can be individual names, or ranges. A range must be in the format mod:[1-9].
modem_group	Name of modem group.

BYE

bye <interface_name>

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

COPY

copy file

Copies a file within the FLASH file system. This is a flat file system.

42

DELETE

Delete commands remove anything you previously *add*ed.

delete appletalk network <network_name>

Deletes the previously *add*ed AppleTalk network. 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,zone_name,… >
                              network <network_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 is not in use.

Parameters	Description
<zone_name >	Zone(s) you wish to delete.
network	Name of the network whose zone(s) you are deleting.

delete configuration

Deletes 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 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 will be processed through a DNS server, instead of locally. Use *list DNS servers* to see which servers are defined.

CLI Reference Guide   43

delete DNS server preference <preference_number>

Removes the name server associated with that preference number (preferred rank) from the table of accessible DNS servers.

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 what filter files are in FLASH memory.

delete file <file_name>

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

delete framed_route user <user name> **ip_route** <ip name or address>

Deletes the framed_route user created with *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

Deletes the ip default route created with the *add ip defaultroute* command.

delete ip network <network_name>

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

44

delete ip route <IP_address>

Deletes an IP address from the IP Routing Table, that you previously added with *add ip route*. Deleting this route will cause IP packets destined for this network to use the default route, which you can see using *list ip routes*. See *add defaultroute gateway* to find out how to add a default route.

delete ipx 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 the network's status. Be sure to use the *disable ipx network* command before deleting the network.

delete ipx route <ipx_net_address>

Deletes an IPX route on the interface you specified 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 a static IPX service from the IPX Services Table. This command will work only if a complete match on all parameters is found. Refer to *add ipx service* command for more information. See table on next page.

Parameters	Description
service name	Designation of IPX service.
type	Type of service: file/server, print, etc., expressed in hexidecimal format. See table for *add ipx service*.

delete login_host preference <preference_number>

Deletes the login host with the specified preference (priority) number. Use *list login_hosts* to see the *add*ed login hosts and associated preference number.

CLI Reference Guide   45

delete modem_group <group_name>

Deletes a modem group from the Modem Group Table. You can list current modem groups and their assigned interfaces using the *list modem_groups*, and *show modem_group* commands.

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 *list available servers* and *list services*.

delete snmp community <name>

Deletes 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 snmp trap_community <name>

Deletes an SNMP trap community name from the list of names and IP addresses that are allowed to receive SNMP trap commands. You can use *list snmp communities* to see the current entries.

delete syslog <ip_name_or_address>

Deletes the specified IP host name or IP address from the list of addresses which are authorized to receive syslog information. Use *list syslog* to see the currently allowed addresses.

delete tftp client <ip_name_or_address>

Deletes the specified IP host name or IP address from the list of addresses which are authorized to TFTP. Use *list tftp clients* to see the currently allowed addresses.

46

delete user <name>

Deletes a user you previously added to the Local User Table. Use *list users* to see the currently defined user, and *show user* to see the attributes you assigned to that user using the *add user* or *set user* command.

DIAL

dial <user_name>

Generates an outgoing call to the location specified by the user name. You can use *list users* to list the defined users, along with the services they are defined to work with, and their current status. Maximum 32 characters allowed.

DISABLE

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 <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

Disables user authentication using the passwords stored in the Local User Table. You specified passwords when using the *add user* or *set user* commands, which are used to authenticate users trying to establish a connection. You can use *show authentication* to see if remote and/or local authentication is currently enabled.

Users can still be authenticated using remote authentication (RADIUS), if you have enabled it.

CLI Reference Guide 47

disable authentication remote

Disables user authentication using remote RADIUS servers. You must have *set authentication* to define the RADIUS server, and enabled it using *enable authentication remote*. You can use *show authentication* to see if remote and/or local authentication is currently enabled. Users can still be authenticated using local authentication, if you have enabled it.

disable interface <interface name>

Disconnects any calls from the specified interface and leaves the interface in a *disabled* state. A disabled interface remains in the Interface Table, but will not transmit or receive any data. You can enter multiple interfaces (ssss,ssss,ssss ...) or a range (mod:1 - 9). Use *list interfaces* to see the currently defined interfaces, and their status.

disable ip icmp_logging
Disables *display* of the Internet Control Message Protocol to the syslog server.

disable ip forwarding

Causes the system to stop forwarding any packets over IP networks. You may want to *disable ip forwarding* if you are using the system only as a terminal server. Users who TELNET to the system can still connect to remote hosts.

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.

48

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 *show ip routing* 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 *add ip route*. You can list the current IP routes using *list ip routes*.

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 *enable ipx rip network* 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 *enable ipx sap network* to restart SAP on this IPX network.

disable link_traps interface <interface_name>

Prevents SNMP from sending linkup and linkdown traps for the specified interface. You can see if the interface is currently enabled for traps by using the *show interface settings* command.

CLI Reference Guide   49

disable modem_group <name>

Disables the modem group you enabled with the *enable modem_group* command.

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, then all active connections are closed when the server is disabled.

disable security_option snmp user_access

Turns off SNMP access to the CLI. This prevents remote users from using SNMP and possibly damage the configuration. You can use *enable security_option snmp user_access* to re-enable full SNMP access.

disable security_option remote_user administration

Disables CLI access to 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 snmp authentication traps

Instructs SNMP to stop recording trap information for user (either local or remote) authentication.

disable telnet escape

Disables the TELNET escape character for all TELNET clients. When disabled, TELNET clients who hit the escape character during their session will not get a local TELNET command line.

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 user name. Disabling a user is useful when prohibiting a user's access temporarily. Note: disabling a user who is already connected doesn't disconnect that user.

DO

do <command_inputfile> **output** [outputfile]

Runs a script file, stored in FLASH memory, which contains a series of CLI commands.

ECHO

echo name <appletalk_address>
> **{ output** [output_filename] **}**
> **{ count** [count] **}**
> **{ interval** [interval] **}**
> **{ timeout** [timeout] **}**
> **{ type** [packet_type] **}**

Sends a packet to the specified address using the AppleTalk Echo Protocol. The remote station simply echoes the packet back.

Parameters	Description
<appletalk_address>	AppleTalk address to send the echo packet to.
output	File name to direct the output of this command to.
count	Number of echo packets to send.
interval	Length of time between sending the echo packets.
timeout	Period before giving up on receiving an echo reply.
type	Type of echo packet to send. The default type is short packet. They are: • ECHO_SHORT_PACKET: 16 bytes • ECHO_LONG_PACKET: 600 bytes

ENABLE

enable accounting

Enables remote accounting via RADIUS. Use *disable accounting* to disable accounting via RADIUS.

enable security_option remote_user administration

Enables remote TELNET users to access the CLI. This prevents remote users from modifying the configuration. You can use *enable security_option remote_user administration* to re-enable full TELNET access.

enable appletalk network <network_name>

Enables a previously defined AppleTalk network. You must have defined zones for this network, using the *add appletalk zone* command, before you can enable the network.

enable authentication local

Enables user authentication using the passwords specified in the User Table. When you issue the *add user command*, you must enter a password for local authentication to use. If there is no password, and remote authentication is not enabled, the user will not be able to establish a connection. You can use *show authentication* to see which authentication schemes are in use.

enable authentication remote

Enables remote (RADIUS) authentication. Local authentication takes precedence over remote authentication. You can use *show authentication* to see which authentication schemes are in use.

52

enable interface <interface_name>

Enables the specified interface. Enabling an interface enables it to transmit and receive data. You can enter multiple interfaces (ssss,ssss,ssss ...) or a range (mod:1 - 9). You can use *list interfaces* to see which interfaces are defined, and whether they are currently disabled.

enable ip icmp_logging

Enaables *display* of the Internet Control Message Protocol to the syslog server.

enable ip forwarding

Allows all IP networks to forward (route) packets. You should only need to use this command if you previously used *disable ip forwarding.*

enable ip icmp_logging

Enables the Internet Control Message Protocol . It provide feedback about routing, diagnostic or error messages encountered by IP. Use *show icmp counters, show icmp counters* commands for detailed information.

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.*

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*.

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*.

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* command.

enable ipx sap network <network_name>

Enables the Service Advertising Protocol (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* command.

enable link_traps interface <interface_name>

Informs SNMP to send linkup and linkdown traps for the specified interface. You can see if the interface is currently enabled for traps using the *show interface settings* command.

enable modem_group <name>

Enables the modem group you disabled with the *disable modem_group* command. The modem group *All* is provided as a default modem group with all NETServer (8 or 16) modems included. 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 snmp user_access

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

enable security_option remote_user administration

Allows CLI access by remote TELNET and dial-in users. CLI configuration can be done from the console port and by remote users. You can use *disable security_option remote_user administration* or *disable security_option snmp user_access* to restrict CLI access to the console port only.

enable snmp authentication traps

Informs SNMP to send traps for both local and remote authentication. You can use *show snmp* to see the current setting.

enable telnet escape

If the TELNET escape character was disabled by the *disable TELNET escape* command, this command re-enables it. When enabled, TELNET client users who press the TELNET escape key during their session will get a TELNET command line.

By default the escape character is [Ctrl] **]** (cntrl]). A TELNET user can change it using *set escape* in the TELNET program.

enable user <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

exit

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

HANGUP

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 enter multiple interfaces (ssss,ssss,ssss ...) or a range (mod:1 - 9).

hangup modem_group <name>

Makes the modem group unavailable for dial-in users. This command has the same effect as hanging up the phone.

56

hangup user

Makes the user unavailable for dial-in. This command has the same effect as hanging up the phone.

hangup user <user name> **all**

Makes all users unavailable for dial-in. This command has the same effect as hanging up the phone.

HELP

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 Esc (Esc) completes the keyword. If you have not yet entered enough of the keyword to be unique, pressing Esc causes the bell to ring.

Typing **?** after a command string displays the possible keywords and values for that command.

HIDE

hide events

Reverses the *show events* command where all events being directed to the console are also echoed to the TELNET session you are running.

HISTORY

history

Displays your previous CLI commands. You can recall commands from the history using Ctrl-**P** (ctrl-P) to recall commands up the list, and Ctrl-**N** (ctrl-N) to recall commands working down the list. The default depth is 10 commands. You can modify the history depth using the *set command history* command.

KILL

kill <"process name">

Kills an active process. Use *list processes* to see which processes are currently active. You can only *kill* a process that you started. An example would be a *ping* that you started that you now wish to kill.

LEAVE

leave

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

LIST

list aarp

Displays the AARP Address Mapping Table, which maps AppleTalk addresses to physical (MAC) addresses of AppleTalk nodes. The table lists:

- **Index** - interface index number
- **Net Address** - AppleTalk network address
- **Physical Address** - physical (MAC) address

58

list active interfaces

Displays the operational status, administration status, index and name of all active interfaces. The output is the same as the *list interfaces* command, except non-active interfaces are not displayed. Inactive interfaces are interfaces with no current connections.

list appletalk forwarding

Displays the entries in the AppleTalk Forwarding Table. The table lists:

- **Network Address Range** - AppleTalk network address range
- **NextHop** - address of next hop router; 0.0 implies entry is a local network
- **Protocol** - always 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 AppleTalk networks configured by the *add appletalk network* command. The table lists:

- **Name** - AppleTalk network name
- **Prot** - protocol - always APPLETALK
- **Int** - interface this network uses
- **State** - possible states are:
  - INITIALIZING
  - CONFIGURING
  - ENABLING
  - ENABLED
  - DISABLING
  - DISABLED
  - INVALID
  - TERMINATING
- **Type** - STATIC or DYNAMIC
- **Network Address** - address range of this entry

CLI Reference Guide   59

list appletalk routes

Displays the entries in the AppleTalk Routing Table. The table lists:

- **Address Range** - Range of addresses used on this route
- **Next Hop** - AppleTalk address of the next hop router. 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** - State 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 revealed.

list appletalk zones

Displays all the AppleTalk zones configured for the entire system.

- **Name** - zone name that you learned via routing (defined by *add appletalk zone* command*)*
- **Addr Range** - range of addresses used in this zone
- **State** - state of the zone
- **Port** - interface the zone runs over
- **From** - address of router from which the zone and network was learned

list available servers

Displays the available network servers. For example: 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.

60

list connections

Displays all connections established on switched interfaces. It lists:

- **IfName** - interface used by each user
- **User Name** - user of each connection
- **Type** - type of connection: dialout, dial_in, callback,manual, ondemand, shared_modem, etc.
- **DLL** - datalink layer protocol

list critical events

Displays last *ten* critical status events, and system time when each occurred. You can change which events are logged as critical, using *set facility*.

list dial_out

Displays the dial-out status of the current modem interfaces. It lists:

- **Index** - table list
- **General Name** - modem group
- **Specific Name** - interface
- **State** - condition of the interface regarding dialout use. Options are: *InUse*, *Avail*, and *UnAvail.*
- **Type** - if *InUse*, the type of network connection
- **Address** - address of the remote station: IP address for IP, MAC address for IPX.

list dns hosts

Displays the DNS Local Host and its IP address, which you configured using *add dns host* or *add login_host* commands (if you specified the IP address).

list dns servers

Displays DNS Name Servers, which you configured using the *add dns server* command. The name you defined for it, the preference, the IP address and current status (ACTIVE, INACTIVE) are listed for each DNS server.

list facilities

Displays the system facilities (processes) currently running, plus the default log level. The log level represents the severity of error that facility will output messages 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 filters

Displays all the filter names in the Filter Ttable, which you previously defined using the *add filter* command. You can remove filters using *delete filter*. The command lists the filter file name, the status of the filter, and the protocols the file applies to. For example:

```
Filter Name Status       Protocols
easyfilter.fil NORMAL     IPX IPX-SAP
```

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 only.

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 *AT&F1S0=1*. You can modify existing initialization scripts using the *set init_script* command.

62

list interfaces

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

- **Index** - number used to identify the interfaces position in the table
- **Name** - interface name: *eth:1*
- **Oper Status** - current, operating status of the interface; UP or DOWN
- **Admin Status** - administrative status you designated interface to be, up or down. For modem interfaces, Oper Status will be up only if the modem is connected.

list ip addresses

Displays the IP address for each interface. It lists:

- **Address** - IP address of the interface
- **Bcast Algo** - broadcast algorithm used
- **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

list ip arp

Displays the contents of the ARP cache. It lists:

- **IP Address** - network address for this entry
- **Phys Address** - MAC address that the IP address maps to
- **Type** - interface type: Ethernet or Token Ringor Dynamic
- **IfName** - interface name: *eth:1*

CLI Reference Guide   63

list ip interface_block

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

- **Address** - IP address of the NETServer interface
- **Neighbor** - IP address of the remote system
- **Status** - status of the connection: ENABLED or DISABLED
- **Interface** - *eth:1*

list ip networks

Displays all the IP networks you previously defined using the *add ip network* command, including any dynamic networks created with a modem established a PPP connection to the NETServer. It also lists:

- **Name** - network designation
- **Prot** - always the IP protocol
- **Int** - name of the interface this network runs on
- **State** - state of the network; ENABLED or DISABLED
- **Type** - STATIC or DYNAMIC network
- **Network Address** - address of the IP network

list ip routes

Displays all the statically defined IP routes that you previously defined using the *add ip route command,* including any routes learned via RIP. It lists:

- **Destination** - IP address that the route resolves to
- **Prot** - LOCAL, RIP or NetMgr
- **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

64

list ipx networks

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

- **Name** - designation you assigned this network
- **Prot** - protocol; always IPX
- **Int** - interface each IPX network runs on
- **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:

- **Network Addr** - network address of this route
- **Prot** - protocol used to find this route: LOCAL, RIP, STATIC, NLSP, OTHER
- **NextHopNIC** - network address of the next router (the next hop to the destination), or the MAC address for the local IPX nodes (on the LAN)
- **Gateway** - address of the gateway to this network
- **Metric -** # of hops through routers this network is distant from
- **Ticks** - estimated interval in eighteenth's of a second for packet delivery to the remote network.

list ipx services

Displays IPX services. It lists:

- **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: SAP, LOCAL, NLSP, STATIC or OTHER

CLI Reference Guide   65

- **Metric** - number of hops through routers to reach this service

list ipx static routes

Displays all IPX static routes previously defined using *add ipx route*.

- **Network Addr** - 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 ticks, to reach the route's destination

list lan interfaces

Displays the installed interface - Ethernet (eth:1), along with 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:

- **Index** - number used to identify the interfaces position in the table
- **Name** - interface name: *eth:1*
- **Oper Status** - current, operating status of the interface; UP or DOWN
- **Admin Status** - administrative status you designated interface to be, up or down.

list login_hosts

Displays currently defined entries in the Login Host Table which you previously defined using *add login_host*. Values displayed are:

- **Preference** - preference (priority) number assigned to the host
- **Name** - name you assigned the login host
- **Port** - Rlogin, TELNET, and/or ClearTCP TCP port numbers assigned to that login host

66

list modem_groups

Displays modem groups that you previously defined using the *add modem_group* command, along with the number of interfaces in each group. For example:

```
MODEM GROUPS

GROUP        Number of
             Interfaces
All          8
```

list networks

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

- **Name** - designation of the network that you defined with *add network*
- **Prot** - protocol of the network: IP, IPX, AP, PPP, SLIP, FRM, DLCI
- **Int** - interface the network is running on
- **State** - Condition of network: ENA (enabled), ENA* (enabling), DIS (disabled), DIS* (disabling), INIT (initialized), INV (invalid), CONF
- **Type** - STAT (static), DYN (dynamic) or AUTO network
- **Network Address** - address of the network

list ppp

Displays PPP bundles and links. When multiple physical links are combined to run multilink PPP (RFC1717), the group of physical links is called a bundle. With ISDN, the multiple links are the two channels you defined using *add isdn signalling interface*. The second link (channel) will become active when the channel_expansion percentage has been exceeded. You can check the percentage using *list ppp*, and change it using *set network user ppp*.

- **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
- **Interface Name** - designation of interface belonging to this bundle

CLI Reference Guide   67

list processes

Displays all processes running on the system.

- **Index** - a reference number in the Process Table
- **Name** - designation of the process (e.g.: Domain Name System)
- **Type** - SYSTEM, APPLICATION, FORWARDER or DRIVER
- **Status** - ACTIVE, PENDING or INACTIVE

list switched interfaces

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

- **Index** - number used to identify the interfaces position in the table
- **Name** - interface name: *eth:1*
- **Oper Status** - current, operating status of the interface; UP or DOWN
- **Admin Status** - administrative status you designated interface to be, up or down. Oper Status will be up only if the modem is connected.

list services

Displays all network services you defined using *add network service*:

- **Name** - name of service
- **Server Type** - type of network server. For example: tftpd (TFTP daemon)
- **Socket** - TCP port number used 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** - the status you have requested for this service: ENABLED or DISABLED. See the *add network service* command for details.

68

list snmp communities or **list snmp trap_communities**

These commands display the defined SNMP communities, which you previously defined using the *add snmp community* command. *SNMP trap_communities* does not list access.

- **Community Name** - community designation for the IP address
- **IP address** - IP address of a member of the community
- **Access privelege (R/W)** - type of access a member has to MIBs

list syslogs

Displays IP addresses which get syslog entries from the system. See *add syslog* for more information, and *delete syslog* command to remove entries. This command shows:

- **Syslog** - IP address to which syslog entries will be sent
- **Log Level** - reporting level of entries to send
- **Msg Count** - current number of messages sent since system bootup

Compare with *list facilities* and *set facilities* commands, which control what gets output to the console port.

list TCP connections

Displays information about all TCP connections. Connection status is defined in RFC-793.

- **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** - status of the connection. E.g.: *Listen*

list tftp clients

Displays IP addresses of all users allowed to use the Trivial File Transfer Protocol (TFTP) to connect to the system. You must have used *add network service* to add TFTP support to the system and used *add tftp client* to authorize users to connect.

list udp listeners

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

list users

Lists all users, showing:

- **User Name** - user designation you specified using *add user*
- **Login Service** - TELNET, RLOGIN, or ClearTCP
- **Network Service** - type of network service: PPP, ARAP, SLIP
- **Status** - link status: ACTIVE, INACTIVE or DISABLED
- **Type** - type of user: see the *add user* command for options

LOGOUT

logout

Leave the CLI and close this connection. This ends the dial-in user's or TELNET session.

PAUSED COMMANDS

More (or CR)	Continue printing
Quit	Cancel rest of output

PING

ping <ip_name_or_addr>

        output [output_filename]
        count [count]
        interval [interval]
        timeout [timeout_value]

Sends an ICMP echo request to a remote IP host.

Parameters	Description
<ip_name_or_address>	IP address in dotted notation, or host name of remote system.
output	A file name to direct output to.
count	Number of ICMP echo requests to send.
interval	Seconds to wait between sending each request.
timeout	Seconds to wait for an echo response to return.

QUIT

quit

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

REBOOT

reboot

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

RENAME

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 see what files
currently exist.

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

RESET

reset modem <interface names list>

Resets the specified modem 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. For example:

reset modem mod:[2-5],mod:7

RESOLVE

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 has been specified using the *set DNS*
command, it will also be resolved, otherwise you must specify it as part of the
name. This command requires either a DNS local host entry (use *add DNS
host*) or a DNS server (use *add DNS server*) to resolve the host name. It is the
reverse of the *ARP* command.

RLOGIN

rlogin <ip_name_or_address>
> **login_name** [login_name]
> **TCP_port** [number]

Creates an *rlogin* client connection to the specified host.

Parameters	Description
<ip_name_or_address>	Either the IP address in nnn.nnn.nnn.nnn notation, or the host name of the remote system.
login_name	User name needed to login to the remote system.
TCP_port	TCP port number to create the connection to. By default, 513 is used.

SAVE

save all

Saves all changes made during your CLI session. We recommend saving your changes frequently, just as you would with any type of editor.

SET

set accounting
> **primary_server** [IP_address]
> **retransmissions** [count]
> **secondary_server** [IP_address]
> **timeout** [number_seconds]
> **start_time** [authentication | connection]
> **use_servers** [ONE | BOTH]

Configures the remote (RADIUS) accounting retransmission algorithm. Use *show accounting* to check these values. See table on next page.

Parameters	Description
primary_server	Initial server to send the accounting information to, unless use_servers is set to BOTH, in which case both servers will be sent to.
secondary_server	Second server to send the accounting information to, unless use_servers is set to BOTH, in which case both servers will be sent to.
retransmissions	Sum of retransmissions to 1 or both servers (if needed), depending on value of use_servers. Default: 100.
start_time	When accounting begins. You may choose either: • **Authentication** - session time in number of seconds after user name and password entered. • **Connection** - session time in number of seconds from modem pickup.
timeout	Interval between retransmissions. Default is 5 seconds.
use_servers	Retransmission algorithm used for accounting. • **ONE** - second server is a backup (default) • **BOTH** - both servers are sent to, until a response is heard from both servers.

set appletalk

> **{ allow_password_change** [TRUE | FALSE] **}**
> **{ arap** [ON | OFF] **}**
> **{ arap_node_network_range** [number-number] **}**
> **{ arap_zone** [string] **}**
> **{ force_manual_password_entry** [TRUE | FALSE] **}**
> **{ max_arap_nodes_reserved** [number] **}**
> **{ max_arap_sessions** [number] **}**
> **{ max_compressed_arap_sessions** [number] **}**
> **{ max_forwarding_table_size** [number] **}**
> **{ max_password_length** [number] **}**
> **{ max_routing_table_size** [number] **}**
> **{ min_arap_nodes_reserved** [number] **}**
> **{ min_password_length** [number] **}**
> **{ password_retries** [number] **}**

Sets AppleTalk parameters. See table on next page.

Parameters	Description
allow_password_change	Setting this parameter to TRUE allows ARAP users to change their passwords. Default: **TRUE**
arap	Setting this parameter to ON allows users to connect remotely over a phone line using ARAP client software. Default: **ON**
arap_node_network_range	Range of network numbers assigned to ARAP users. Default: **0 - 0**
arap_zone	ARAP zone names specifying which zone remote clients will appear in. Default: **NULL**
force_manual_password_entry	Setting this parameter to TRUE forces users to enter their passwords when connecting via ARAP. Default: **FALSE**
max_arap_nodes_reserved	Maximum number of ARAP node numbers reserved for use. ARAP nodes are reserved ahead so that remote users do not have to wait for a node to be negotiated for with other systems on the network. Default: **16**
max_arap_sessions	Maximum number of ARAP node numbers allowed at one time. Default: **16**
max_compressed_arap_sessions	Maximum number of ARAP node numbers using compression allowed at one time. Compressed sessions are faster, but use more system resources. Default: **16**
max_forwarding_table_size	Maximum number of Forwarding Table entries allowed. Default: **256**
max_password_length	Maximum length of a password allowed. Default: **16** characters
max_routing_table_size	Maximum number of Routing Table entries allowed. Default: **256**
min_arap_nodes_reserved	Minimum number of ARAP connections reserved for use. Default: **16**
min_password_length	Minimum length of a password allowed. Default: **4** characters
password_retries	Maximum number of remote dial-in attempts allowed. Default: **16**

set appletalk network <name>
        { aarp_gleaning [ENABLE | DISABLE] **}**
        { current_zone [name] **}**
        { ddp_checksums [TRUE | FALSE] **}**
        { default_zone [name] **}**
        { description [string] **}**
        { desired_node_address [appletalk_address] **}**
        { seed_router [TRUE | FALSE] **}**

Sets parameters for all AppleTalk networks.

Parameters	Description
<network_name>	Designation of the AppleTalk network.
aarp_gleaning	Enables the forwarder to learn hardware addresses from the AARP packets it receives. Default: **ENABLED**.
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: **FALSE**
default_zone	Designation of the default zone for systems on this network.
description	A designation of the network. Limit: 64 characters.
desired_node_address	AppleTalk address used first when probing for an AppleTalk address at the time the network is enabled. Default: **0.0**
seed_router	TRUE enables the router to propagate seed (network range, zones) data. Default: **TRUE**

set authentication

        primary_server [IP_address or name]
        primary_secret [string]
        retransmissions [count]
        secondary_server [IP_address or name]
        secondary_secret [string]
        timeout [number_seconds]

Configures the remote (RADIUS) authentication retransmission algorithm.

Parameters	Description
primary_secret	A designation to employ for security purposes. Limit of 16 ASCII characters.
primary_server	IP address or name of the initial server to exchange authentication data with.
secondary_secret	Additional designation to employ for security. Limit of 16 ASCII characters.
secondary_server	IP address or name of the second server to exchange authentication data with.
retransmissions	Maximum number of times to retransmit to one or both servers if transmissions fail. The default is 10.
timeout	Amount of time in seconds between retransmissions. Default: 3 seconds.

set clearTCP connect_message <"message string">

Sets the string that will be sent to ClearTCP clients, when the TCP connection is established. The message string must be enclosed in quotes. Limit of 64 ASCII characters.

set command

        history <numerical range>
        prompt <string>
        idle_timeout <numerical range>
        local_prompt <string>
        login_required [no | yes]

Configures command line parameters. See table on next page.

Parameters	Description
history <numerical range>	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**.
prompt <string>	Sets the global command prompt for the CLI. Use show command to see the currently defined prompt. Limit: **64** characters.
idle_timeout <range in minutes>	Sets console login connection to close after being idle for the specified interval. Range: **0-60 min**. Login Required must be set to yes.
local_prompt <string>	Sets a separate prompt for a command file process. Limit: **64** characters.
login_required [no | yes]	Sets whether a user trying to connect to the console port is given Login: and Password: prompts.

set connection

> **host_select** [ROUND_ROBIN | RANDOM]
> **message** ["prompt"]
> **service** ["prompt"]
> **user_name** ["prompt"]

Configures connection parameters for all dial-in users. Note that "message" will only be displayed if there are no other "message" parameters set for that interface. Use *show connection* to see what the current settings are.

Parameters	Description
host_select	Specifies how the system chooses which host to connect the user to. Next host is chosen sequentially (ROUND_ROBIN) or randomly.
message	String displayed when a dial-in user is connected. Limit: **64** characters.
service	String that prompts the user for login or network service. Limit: **64** characters.
user_name	String that serves as the user prompt. The global user name USR_NETS is specified if no name is entered. Limit of 64 characters.

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.

CLI Reference Guide   79

set dial_out

> **security** [YES | NO]
> **idle_timeout** <minutes>
> **recovery_timeout** <minutes>

Sets global parameters for all dialout connections over modems.

Parameters	Description
security	Determines whether to require user name and password when dialing out. If YES, login authorization is required. Default: **YES**.
idle_timeout	Interval allowed before an idle connection is closed. 0 is no timeout: default (NO) is 5 minutes. If dialout is on (YES), timeouts derive from user values. Range: **1 minute to 3 hours.**
recovery_timeout	When a connection is terminated, the time allowed before session is canceled. This allows a dialout user time to reconnect, if the phone cord is jarred from the jack or the PC rebooted, for example. 0 is no timeout, the default is 5 minutes. Range: **1 minute to 3 hours.**

set dns

> **domain_name** <string>
> **number_retries** <number>
> **timeout** <seconds>

Sets the global parameters for DNS; both the local DNS hosts (*list DNS host*) and the remote DNS servers (*list DNS servers*). See table on next page.

Parameters	Description
domain_name	Default domain designation to be used if no domain is specified (by *add dns server*) in the name to be resolved. For example: usr.com. Limit: **64** characters.
number_retries	Number of times the resolve name request will be sent to each Name Server if the server fails to respond to a request before the timeout period. Default is **1**, valid range is **1-5**.
timeout	Number of seconds to wait before deciding a request to a Name Server has timed out. Minimum interval and default is **5** seconds, maximum interval is **120** seconds .

set dns server preference <number>
                       name <host_name and domain_name>
                       address [ip address]

This command redefines the name of a Domain Name Server, that you previously defined using *add DNS server*. Use *list DNS servers* to see the currently defined DNS servers.

Parameters	Description
preference	Priority of the name server in name searches.
name	Designation - must be unique - given the DNS server. This field is optional, but is useful for keeping track of name servers. Limit: **32** characters.
address	IP address of the DNS server.

set facility <facility_name> **loglevel** [level]

Sets the severity reporting level for a facility. The hosts that will receive the error log entries are defined using *add syslog loglevel*. Use *list facilities* to see what the current loglevel is for each facility. The levels are:

- **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 that is not frequent
- **VERBOSE** - a regular periodic event, e.g. a routing update message
- **DEBUG** - for debugging purposes only

set framed_route user <name>
                    gateway [ip_address]
                    ip_route [ip_address]
                    metric [number]

Specifies a framed (static) network to the user profile for dialup connections.
See add *framed_route user* and *add ip route* commands.

Parameters	Description
<user name>	User name 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. Values are 1 through 15.

set imodem interface <interface_name>
                AT_COMMAND [string]
                CALL_TYPE [AUTO | CLEAR | INTERNET |
                          MODEMFAX | V110 | V120]
                DIRECTORY_NUMBER [string]
                SPID [string]
                SWITCH [ATT | DMS100 | NI1 | NI2]
                TERMINAL_ENDPOINT_ID [string]

Specifies the following ISDN modem settings. Use the *show interface*
command to retrieve these settings. See table on next page.

82

Parameters	Description
<interface_name>	Designation you choose for a particular port (e.g.: mod:1).
at_command	Field in which you can designate your AT command choice.
directory_number <string>	Telephone number provided by your phone service.
call_type	Call type specifies your desiged channel connection service. Choices are: • **AUTO** - System adapts to the proper connection setting. The I-modem first tries to make a V120, then a V110, then a V.34 then an ordinary analog call if each succeeding negotiation fails. • **V120** - I-modem negotiates for V120 connections only. If the V120 connection isn't made, no connection is negotiated. • **V110** - I-modem negotiates for V110 connections only. If the V110 connection isn't made, no connection is negiated. • **MODEMFAX** - I-modem works in analog mode for modem or fax emulation only. If you know that you will make and receive analog calls only, this setting shortens the connect time. • **CLEAR** - I-modem sets up a synchronous clear channel, at 64 or 56 Kbps, with a remote device. Common applications are videoconferencing and remote access to mini- or mainframe computers. • **INTERNET** - This setting requires TCP/IP software be installed on your computer. This software must deliver asynchronous PPP through your PC's serial port. NetManage Chameleon and MacTCP are examples.) The I-modem first tries to make a clear-channel digital connection, converting asynchronous PPP data from your PC to synchronous PPP, which is typically required at your Internet Service Provider's end of the connection. If the I-modem can't make a digital, synchronous connection, it attempts an analog V.34 connection. From V.34 on, the call is negotiated as an ordinary analog call.

CLI Reference Guide   83

spid <string>	Service Profile ID provided by your phone supplier for each B channel. SPIDs tell the phone company of any special services you've ordered. Limit: **64** characters.
terminal_endpoint_id <string>	The TEI permanently specifies your link with the central office switch. The value range is **0-63**. This number is assigned by the telco. Default: **0**. If you aren't assigned a TEI, it is specified dynamically.
switch	Type of central office switch your ISDN line will terminate, and which protocol will control your calls: **ATT** - Running AT&T's 5ESS Custom protocol. **DMS100** - Running Northern Telecom's Custom protocol. **NI1** - Running National ISDN, version 1, protocol. **NI2** - Running National ISDN, version 2, protocol.

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*.

Parameters	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 be less than **56** characters. The string must end with the characters \\r\\n, which is interpreted by the system as carriage return, newline.

84

set interface <interface_name>

                    filter_access [ON | OFF]
                    input_filter <filter_name>
                    output_filter <filter_name>

Sets filter parameters for the specified protocol 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.

Parameters	Description
<interface_name>	Designation of interface you are setting parameters for. Limit: **32** characters.
filter_access	ON 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.
input_filter	Name of filter file you wish to be applied to the input stream coming in on the specified interface. Limit: **20** characters.
output_filter	Name of the filter file you wish to be applied to the output stream leaving the specified interface. Limit: **20** characters.

set ip network <name>

                    broadcast_algorithm [number]
                    reassembly_maximum_size [number]
                    rip_authentication_key [string]
                    rip_policies_update <rip_policies>
                    routing_protocol [NONE | RIPV1 | RIPV2]

Sets the broadcast algorithm, the maximum size used for reassembling fragmenting packets, the RIP authentication string, RIP policies, 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 that have already been defined using *add ip network*. You can list the currently defined IP networks using *list ip networks*. Note: as with all networks or network services, you must disable the IP network before setting these parameters, usingthe *disable ip network* command.

See RIP policies and table on the following pages.

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** - *enabled* 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. In general, it performs better when used with split horizon.
- **Flash Update** - *enabled* by default. It is also known as "triggered update", meaning routes that have their metrics modified will be advertised immediately, instead of waiting for the next scheduled broadcast.

The following flags 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 en*abled* 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.
- **Silent** - This flag tells RIPv2 not to send updates. It is *disabled* by default.

86

Parameters	Description
<network_name>	Designation of the IP network for which you want to set parameters.
broadcast_algorithm	Algorithm determines which address is used in broadcasts to represent the entire network. Choices are: • **1** - the IETF standard, nnn.nnn.nnn.255 (default) • **0** - the BSD standard, nnn.nnn.nnn.000
reassembly_maximum_size	Maximum size IP datagram that the system will try to reassemble, when the datagram has been fragmented to fit in the network packet size. Default: **3468**.
rip_authentication_key	Text 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**). 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)
routing_protocol	Sets routing protocol to be used on IP network. Choices are: no routing protocol, RIP version 1, or RIP version 2.

set ip routing

> **autonomous_system_number** [number]
> **table_maximum_size** [number]
> **metric_maximum_entries** [number]
> **rip_flags** [METRICS, SEND_REQUEST]
> **router_id** [IP_address]

Sets parameters for IP routing to the s pecified IP router address, which is the gateway to an Autonomous System.

Parameters	Description
autonomous_system_number	
table_maximum_size	Maximum number of IP routes system can hold in its table. Default: **1000**
metric_maximum_entries	Most next hop entries the System Table can maintain. Maximum: **512**
router_id	IP address
rip_flags	Flags indicate at which level a RIP instance is disabled or configured. Choices are: • **METRICS** - Specifies how to increment metrics using RFC1058. • **SEND_REQUEST** - Sends a RIP request for routing information when an interface first comes up.

88

set ip system

> **initial_pool_address** [IP_address]
> **pool_members** [number]

When dial-in network users have their IP addresses dynamically assigned, those IP addresses are allocated from a pool. Sets up that pool. The pool is created as a range, starting from an initial address. As PPP or SLIP users dial in, IP allocates an address from this pool and assigns them to the user.

Parameters	Description
<initial_pool_address>	First IP address in pool, written in nnn.nnn.nnn.nnn notation.
pool_members	Number of entries in pool. Pool addresses are allocated from initial_pool_address up to initial_pool_address + pool_members.

set ipx network <network_name>

> **delay_ticks** [number]
> **diagnostics** [DISABLE | ENABLE]
> **maximum_learning_retries** [number]
> **netbios** [ENABLE | DISABLE]
> **netbios_name_cache** [DISABLE | ENABLE]
> **netbios_cache_timer** [seconds]
> **netbios_max_hops** [number]
> **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_packet_size** [number]
> **sap_periodic** [ENABLE | DISABLE]
> **sap_nearest_replies** [ON | OFF]
> **sap_update_interval** [number]

Parameters	Description
<network_name>	Designation of the IPX network. Maximum size: **32** 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 or not to send diagnostic packets to this IPX network. Default: **ENABLED**
maximum_learning_retries	Number of times this network will resend packets to learn its directly connected neighbors. Default: **0**
netbios	Whether to support NetBIOS on dial-out IPX networks. Default: **ENABLED**
netbios_name_cache	Whether or not to cache a list of the other NetBIOS systems on this IPX network. Default: **DISABLED**
netbios_cache_timer	Interval a NetBIOS system is kept in the cache. Default: **60 seconds**
netbios_max_hops	Maximum number of hops this network will make to locate a NetBIOS system. Default: **8.** Range: **0 - 65535**.
packet_maximum_size	Maximum size packet that 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: **4**
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	Whether or not RIP sends periodic updates. Default: **ENABLED**
rip_update_interval	How often RIP should send periodic updates. Default: **60 seconds**
sap_age_multiplier	Number to multiply the sap_update_interval by, to obtain the value for aging out entries in the SAP database. Default**: 4**
sap_broadcast	Enables, disables SAP broadcasts. Default: **ENABLED**

90

sap_gap_timer	Time the system should wait between sending SAP packets. Default: **1**
sap_packet_size	Size of SAP packets. Default: **510 bytes**
sap_periodic	Whether or not SAP will send periodic updates. Default: **ENABLED**
sap_nearest_replies	Whether or not SAP will look its nearest neighbors. Default: **YES**
sap_update_interval	How often RIP should send periodic updates. Default: **60 seconds**

set ipx system

> **name** [network_name]
> **number** [internal network number]
> **priority** [priority level]
> **default_gateway** [ipx_host_add]
> **initial_pool_address** [ipx_addr]
> **pool_members** [number]

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

Parameters	Description
<network_name>	Designation for the dynamic IPX network.
number	Internal number for the dynamic IPX network.
priority	Priority for the dynamic IPX network.
default_gateway	Default router for the dynamic IPX network.
initial_pool_address	Initial IPX address used to dynamically assign IPX network.
pool_members	Number of addresses to reserve in the pool of IPX addresses used when dynamically assigning IPX networks.

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.

Parameters	Description
<preference_number>	Preferred rank of a login host. 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, then the default is **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, then the default is **23**.
clearTCP_port	TCP port number you wish to configure for ClearTCP access to the login host. There is no default TCP port number.

set modem_group <group_name>
                    access [DIAL_IN | DIAL_OUT | TWOWAY]
                    connection_type [DIRECT_CONN | NORMAL |
                                DIRECT_NET | NO_PROMPT |
                                PROMPT_USER_ONLY]
                    dial_prefix [string]
                    host_type [PROMPT | SELECT | SPECIFIED]
                    host_address [IP_address]
                    init_script [name]
                    login_service [TELNET | RLOGIN | CLEARTCP]
                    message ["login_message"]
                    password [string]
                    prompt ["prompt_message"]
                    protocol [ARAP | PPP | SLIP]
                    TCP_port [port_number]
                    type [NETWORK | LOGIN | LOGIN_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 that all the parameters that can be set using *set switched interface* can also be set using this command, but this command sets multiple interfaces with one command.

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.

See table on next page.

Parameters	Description
<group_name>	Designation of the modem group. Limit of 32 characters.
access	Sets access type for switched interface. Modem can allow dial-in only, dial-out only or both (TWO-WAY).
connection_type	Sets the connection type for switched interface. Options: • **Direct_net** uses the protocol parameter's setting to create a virtual node connection. Other connection types establish a virtual terminal connection, with the type determined by login_service parameter. Direct_net does not support the SLIP protocol. • **Direct_conn** - User name and password are supplied by parameters in this command. • **Normal** - prompt for user name *and* password. • **Prompt**_user_only - prompt for user_name only. • **No_prompt** - prompt for password only.
dial_prefix	Prefix added to all phone numbers dialing from this port. Limit of 64 characters.
host_type	Identifies how dial in connection is set up. Options: • **prompt** - prompted to enter host name or add. • **select** - a host is chosen from a login host list you specify, configured by *set connection* command. • **specified** - connected to IP add. configured here.
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.
init_script	Modem initialization string to use. Limit: **7** characters.
login_service	The login service to use, if the connection type is not direct_net. Options: • **TELNET** • **RLOGIN** • **ClearTCP**
message	String displayed to dial-in user when connection established. Limit: **64** characters.
password	Parameter used if the connection type is no_prompt or prompt_user_only.
prompt	String to present the dial-in user. Limit: **64** characters.
protocol	Protocol to connect with, if the connection type is direct_net. SLIP is not supported by direct_net connection type.
TCP_port	TCP_PORT number for the login host. Parameter used when connection type is *direct_conn* or *direct_net*.

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
user_name	Designation for the switched interface, used if connection type is no_prompt. Limit: **32** characters.

set network service <admin_name>
                             server_type [service_name**]**
                             socket [socket_number**]**
                             data ["string"**]**
                             close_active_connections [TRUE | FALSE**]**

Sets parameters for configured network services. You can list the configured network services using *list network services*. Service must be disabled for this command to work.

Parameters	Description
<admin_name>	Designation you assigned to network service with the add network service command. Limit: **32** characters.
server_type	Type of network service you wish to assign to this administration name. Currently available services are: • **TELNETD** - TELNET server • **ClearTCPD** - for ClearTCP applications • **DialOut** - for dialout calls • **HTML** - for gathering statistics • **SNMPD** - SNMP agent • **TFTPD** - server for file transfers
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's (or receiver's) IP address and service type's port number.
data	TELNET and ClearTCP Ancillary Data. This field contains server-specific configuration data. See table which lists the configurable ancillary data parameters in the *add network service* command on page 36.
close_active_ connections	Indicates whether or not to close any active connections when a service is shut by *disable network_service*.

set ppp receive_authentication [NONE | PAP | CHAP | EITHER]

Sets the type of authentication to be used when establishing PPP connections. See RFC 1334 for details about CHAP and PAP. Options are:

Parameters	Description
NONE	Don't check
PAP	Use Password Authentication Protocol
CHAP	Use Challenge Handshake Authorization Protocol
EITHER	CHAP tried first, then PAP. **Default**.

set snmp community <community_name>
                      address [IP_address]
                      access [RO | RW]

Modifies parameters for an SNMP community (authorized user or host to which notifications are sent). 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*.

Parameters	Description
<community_name>	Group designation authorizing SNMP requests.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn
access	Determines what type of access to SNMP MIBs the added user will have. Options are Read Only (RO) and Read Write (RW). **RO** is the default on public (0.0.0.0) networks and **RW** the default on private networks.

set snmp trap_community <community_name> **address** [IP_address]

Modifies parameters for an SNMP trap community (authorized user or host to which trap notifications are sent). 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*. See *set snmp_trap community* command above.

96

set switched interface <interface_name>
       access [DIAL_IN | DIAL_OUT | TWO_WAY]
       at_command [string]
       connection_type [DIRECT_CONN | NORMAL |
                DIRECT_NET | NO_PROMPT |
                PROMPT_USER_ONLY]
       dial_prefix [string]
       filter_access [ON | OFF]
       host_type [PROMPT | SELECT | SPECIFIED]
       host_address [IP name or address]
       init_script [name]
       input_filter [name]
       login_service [TELNET | RLOGIN | CLEARTCP]
       message ["login_message"]
       output_filter [name]
       password [string]
       prompt ["prompt_message"]
       protocol [ARAP | PPP | SLIP]
       TCP_port [port_number]
       type [NETWORK | LOGIN | LOGIN_NETWORK]
       user_name [user name]

Configures port parameters for the specified switched (modem) interface (mod:1, e.g.). To see which switched interfaces you have configured, use *list switched interfaces*. To see the settings for a particular interface, use *show interface settings*.

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.

See table on the next page.

CLI Reference Guide

Parameters	Description
<interface_name>	The switched interface to modify. Limit: **32** characters.
access	Sets access type for switched interface. The modem can allow dial-in only, dial-out only or both (TWO-WAY).
at_command	String representing any generic AT command. When implemented, output is displayed immediately on CLI.
connection_type	Sets connection type for switched interface. Options: • **Direct_net** uses the protocol parameter's setting to create a virtual node connection. Other connection types establish a virtual terminal connection, with the type determined by login_service parameter. Direct_net does not support the SLIP protocol. • **Direct_conn** - User name and password are supplied by parameters in this command. • **Normal** - prompt for both user name and pass. • **Prompt_user_only** - only prompt for user name. • **No_prompt** - only prompt for password
dial_prefix	Prefix added to all the phone numbers dialing from this port. Limit of 7 characters.
host_type	Identifies how connection is established. Dial-in user is: • **prompt** - prompted to enter a host name or add. • **select** - connected to a login host, selected from the list of login hosts, determined by the host_select field in the set connection command. • **specified** - connected to the configured IP add.
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.
init_script	Name of modem initialization script used. Maximum size: 7. 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 will be deleted.
login_service	Login service to use if the connection_type is <u>not</u> direct_net. Options: • **TELNET** • **RLOGIN** • **ClearTCP**
message	String to display to a dial-in user when connection is set. Limit: **32** characters.
prompt	String to present the dial-in user. Limit: **64** characters.

98

password	Used if connection_type is no_prompt or prompt_user_only.
protocol	Protocol (ARAP or PPP) to connect with, if connection type is direct_net. SLIP is not supported by direct_net connection type.
TCP_port	TCP port number for the login host. This parameter is used when the connection type is direct_conn or direct_net.
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
user_name	Designation configured for the switched interface. This parameter is used when connection type is no_prompt.

set syslog <IP_address> **loglevel** [level]

Sets the error reporting level for syslog entries that will be sent to the specified IP address. You must have previously defined this syslog IP address using *add syslog*. There are five levels of logging:

- **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 that is not frequent
- **VERBOSE** - a regular periodic event, e.g. a routing update message
- **DEBUG** - for debugging only

set system

        name ["name"]
        location ["location"]
        contact ["contact info"]
        transmit_authentication_name [keyword]

Specifies system information, displayed using *show system*. The transmit authentication keyword (limit of **32** characters) is used when the NETServer receives a challenge - 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 datalink layer, which you supply here. *Location*, *name* and *contact* names are limited to **64** characters. See table on next page.

Parameters	Description
contact	Name of NETServer administrator.
location	Site of the NETServer.
name	Designation of your NETServer.
transmit_authentication_name	Remote account name.

set time <time>

Sets the system time, and leaves the date unchanged. Use *show date* to see what the current settings are. The format is: hh:mm:ss. The seconds field is optional. The *set date <date> time* command also sets the time.

100

set user <user_name>

        alternate_phone_number [number]
        expiration [date]
        idle_timeout [seconds]
        input_filter [filter_name]
        message ["message"]
        modem_group [group_name]
        output_filter [filter_name]
        password [password]
        phone_number [number]
        session_timeout [seconds]
        type [LOGIN,NETWORK,CALLBACK,DIAL_OUT,
           MANAGE]

Modifies user parameters. See table on next page.

Parameters	Description
<user_name>	Name of user, previously defined using add user. Limit: **32** characters.
alternate_phone_number	Number to dial if the first number is busy. Limit: 64 characters.
expiration	Date after which this user becomes inactive. The format is: DD-MMM-[YY]YY. Month is the first 3 letters of the month. Year is either 2 or 4 digits - 96 or 1996.
idle_timeout	Interval to wait before timing out an inactive connection. Default: **0** seconds.
input_filter	Designation of the filter file in FLASH memory to be applied to the input datastream.
message	Message presented a dial-in user. Limit: **64** characters.
modem_group	Modem group used to make the connection.
output_filter	Name of the filter file in FLASH memory to be applied to the output datastream.
password	User's password, up to **15** ASCII characters. Value is required.
phone_number	Primary phone number to make the connection. Limit: 64 characters.
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. • **Login** users are TCP users who use the login_service specified. • **Network** users are framed protocol users, who use the network_service specified. • **Callback** users disconnected after authentication and called back. • **Dialout** users are either modem sharing users or WAN connection users. • **Manage** users with system administration authority.

set dial_out user <user_name>
                              local_IP_address [ip_net_address]
                              reply1_script [number]
                              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 (ISDN) and modem. Scripts strings are limited to **240** characters.

Parameters	Description
<user_name>	Name of user, previously defined using add user with dialout as the type. Limit: **32** 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** characters.

set dial_out user <user name> **site**
                              address_selection [ASSIGN | NEGOTIATE | SPECIFIED]
                              type [ONDEMAND | TIMED | CONTINUOUS | MANUAL]
                              default_route_option [ENABLE | DISABLE]
                              appletalk [ENABLE | DISABLE]
                              end_time [time]
                              ip [ENABLE | DISABLE]
                              remote_IP_address [IP name or net address]
                              ipx [ENABLE | DISABLE]
                              ipx_address [ipx_address]
                              range_appletalk_address [address_range]
                              send_password [string]
                              spoofing [ENABLE | DISABLE]
                              start_time [time]

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

Parameters	Description
<user name>	Name user, previously defined using add user with dialout as the type.
type	Describes what type of dial out connection this is: • **ONDEMAND** - makes connection when the system needs a session with remote network. • **TIMED** - makes connection at a set time • **CONTINUOUS** - always keeps connection up • **MANUAL** - starts connection manually with CLI
appletalk	Determines whether this user can connect to an AppleTalk network
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.
end_time	For TIMED user, specifies when to tear down connection.
ip	Determines if this connection supports IP or not.
address_selection	Determines how the IP address will be 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 • **SPECIFIED** - uses IP address set in remote_IP_address value
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 'A', 'B', 'C', or 'H', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If you don't specify a mask, the system will generate it for you from the network address.
ipx	Determines if this connection supports IPX or not.
ipx_address	For IPX connection, address of the remote network.
range_appletalk_ address	For an AppleTalk connection, the address range of the remote network.

104

send_password	Password sent to remote network. *Note*: passwords you defined with other commands are for dial-in users. Maximum length: **15** characters.
spoofing	Whether to use spoofing across the remote connection, to save overhead on the dial-out line's connection.
start_time	Time to start a TIMED connection.

set login user <user name>
> **host_type** [PROMPT | SELECT | SPECIFIED]
> **login_host_IP_address** [ip_ name_or_address]
> **login_service** [RLOGIN | TELNET | CLEARTCP]
> **TCP_port** [number]
> **terminal_type** [string]

Sets parameters for users whose type is LOGIN..

Parameters	Description
<user name>	User to set parameters for, earlier defined using add user with login as type. Limit: **32** characters.
host_type	Options are: • **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_service	Service used to login to the remote host.
TCP_port	TCP Port number the remote host expects this login to use.
terminal_type	Terminal type used for the remote connection, e.g. VT100.

set network user <name>

> **address_selection** [NEGOTIATE | ASSIGN | SPECIFIED]
> **appletalk** [ENABLE | DISABLE]
> **default_route_option** [ENABLE | DISABLE]
> **filter_zones** [ENABLE | DISABLE]
> **header_compression** [NONE | TCPIP]
> **ip** [ENABLE | DISABLE]
> **ip_routing** [LISTEN | SEND | BOTH | NONE]
> **ipx** [ENABLE | DISABLE]
> **ipx_address** [ipx_addr]
> **ipx_routing** [ALL | LISTEN | NONE | RESPOND | SEND]
> **ipx_wan** [ENABLE | DISABLE]
> **MTU** [number]
> **network_service** [ARAP | PPP | SLIP]
> **range_appletalk_address** [at_range]
> **remote_ip_address** [ip_addr]
> **rip** [RIPV1 | RIPV2]
> **rip_authentication** [string]
> **rip_policies_update** [rip policies]
> **send_password** [user password]
> **spoofing** [ENABLE | DISABLE]

Specifies parameters for users whose *type* is NETWORK. See table on next page.

106

Parameters	Description
<user name>	User, who must have network as the type.
address_selection	Determines how the IP address will be 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** - uses IP address set in remote_IP_address value
appletalk	Sets interface for user to allow AppleTalk across this link.
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.
filter_zones	Enables filtering for Appletalk zones.
header_compression	Sets TCPIP compression or no header compression.
ip	Sets interface to enable/disable prot. Default: enable.
ip_routing	Sets routing type (RIP packets) accepted on this connection. • **LISTEN** - detects packets destined for system's nets • **SEND** - routes packets destined for the remote network • **BOTH** - both listens and sends • **NONE** - ignores all routing packets. **Default**.
ipx	Sets interface for this user to enable/disable IPX prot.
ipx_address	For an IPX connection, address of remote network.
ipx_routing	Sets type of IPX RIP and SAP packets to accept on this connection. • **LISTEN** - detects RIP/SAP packets headed for system's networks • **SEND** - routes pckts. destined for remote net • **RESPOND** - if requested, answers with IPX RIP or SAP data. **Default**. • **ALL** - detects, sends, answers with RIP/SAP packets • **NONE** - ignores all routing packets

ipx_wan	Protocol used when two IPX nets wish to negotiate the IPX net number for the WAN connection. Both ends of the WAN connection must enable this protocol for it to work. Default is **DISABLED**.
MTU	Maximum Transfer Unit - largest data packet size allowed.
network_service	Type of network service. Default is PPP.
range_appletalk_ address	For AppleTalk connection, address range of the remote net. Format is sss-eee: sss is the start address, eee the end address. The start address can be 0 only if the end address also is 0. Start and end addresses ranges are 1-65280. Start address must be less than or equal to end address.
remote_IP_address	For a client IP connection, address assigned to client.
rip	Selects either RIPV1 or RIPV2.
rip_authentication	Authorizes RIP updates using a stored password. Maximum string length: 64 characters.
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. The default is indicated by (**D**). 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: **15** characters.
spoofing	Sets spoofing across the remote connection to save overhead on a dial-out line. Default is **DISABLED**.

set network user <user name> **ppp**
     channel_decrement [percent]
     channel_expansion [percent]
     compression_algorithm [ASCEND | AUTO |
            MICROSOFT | NONE | STAC]
     expansion_algorithm [CONSTANT | LINEAR]
     max_channels [number]
     min_size_compression [number]
     receive_acc_map [hex_number]
     reset_mode_compression [AUTO | EVERY_PACKET |
            EVERY_ERROR]
     transmit_acc_map [hex_number]

Sets parameters for users whose *type* is NETWORK, and who will be
connecting over an interface running multilink PPP. Multilink PPP groups
multiple links into a bundle to combine the communications capacity of both
links. This applies to ISDN, where there are two data channels, and your
provider allows combining both channels on demand.

See table on next page.

Parameters	Description
<user name>	Name user, previously defined using add user with network as the type.
channel_decrement	When the line usage of the second channel drops below this point, PPP will drop to the first channel only. Default: **20 %**
channel_expansion	When the line usage of the first channel exceeds this percentage, PPP will add the second channel into communications. Specifying 100% here disables the second channel for multilink PPP. Default: **60 %**
compression_algorithm	Specifies the proprietary compression algorithm PPP uses. Default: **AUTO**
expansion_algorithm	Specifies which type of expansion algorithm to decompress incoming PPP data. • **CONSTANT** - best for constant datastreams, such as file transfer • **LINEAR** - best for bursty traffic, such as interactive users. **DEFAULT**
max_channels	Sets how many channels you can use. The actual number of channels is determined by the channel_decrement and channel_expansion parameters. One channel disables multilink PPP. Default: **1**
min_size_compression	Data packet size that PPP decides is big enough to start compression. Data packets smaller than that will not be compressed. Default: **256**
receive_acc_map	Determines whether the system will use the asynchronous control character map to filter out incoming data. Default: **FFFFFFFF**
reset_mode_compression	Determines how often PPP examines packets to decide when to renegotiate the optimum compression algorithm. Default: **AUTO**
transmit_acc_map	Determines whether the system will use the asynchronous control character map to filter out outgoing data. Default: **FFFFFFFF**

110

SHOW

Show commands display details about system entities.

show accounting settings

Displays RADIUS accounting settings, which you can modify using the *set accounting command*.

ACCOUNTING SETTINGS:
- **Use_Servers** - options are ONE or BOTH
- **Primary Server is** - IP address of the primary RADIUS server
- **Secondary Server is** - IP address of the secondary RADIUS server
- **Retransmission Timeout** - number of seconds between retransmissions
- **Max Retransmissions** - maximum times to retransmit to both servers
- **Accounting Start Time** - the time accounting was started by the *enable accounting* command
- **Status is** - current status of RADIUS accounting

show accounting counters

Displays RADIUS accounting statistics.

ACCOUNTING COUNTERS
- **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

show appletalk counters

Displays counters the system maintains for AppleTalk connections.

- **Table Lookups** - # of times a node performed an address lookup in its Address Mapping Table.
- **Table Hits** - # of times the hardware address corresponding to an AppleTalk address was found in the Address Mapping Table.
- **Queries Received** - # of requests to determine the hardware address of a given protocol address.
- **Replies Received** - # of response packets received by a node.
- **Extended Replies Received** - from AARP (AppleTalk's client software)
- **Zone Conflict Errors** - # from AARP
- **Obsolete Packets Received** - # from AARP

  NBP Counters
- **Look Up Requests Received** - # of NBP lookup requests taken by node.
- **Look Up Replies Received** - # of NBP replies taken by node.
- **Broadcast Requests Received** - # of NBP broadcast requests taken by the node.
- **Forward Requests Received** - # of NPB forwarding requests taken by the node.
- **Lookup Replies Sent Out**- # of NBP replies sent by the node.
- **Registration Failures** - # of times a name registration failed on the given node.
- **Input Errors** - # of bad NBP packets received by the node.

  ECHO COUNTERS
- **Requests** - # of echo protocol requests received by the node.
- **Replies** - # of echo protocol replies received by the node.
- **Requests Sent Out** - # of echo protocol requests sent out by the node.

  RTMP Counters
- **Requests Sent** - # of RTMP requests sent by the node.
- **Version Mismatches** - # of RTMP packets received with a version mismatch.
- **Errors Received** - # of bad RTMP packets received by the node.

112

show appletalk settings

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

- **ARAP** - Setting this parameter to ON allows users to connect remotely over a phone line using ARAP client software.
- **Max ARAP Sessions** - Maximum number of ARAP connections allowed at one time.
- **Max Compressed ARAP Sessions** - Maximum number of ARAP connections using compression allowed at one time. Compressed sessions are faster, but use more CPU because the compression is done in software instead of in the modem.
- **ARAP Zone** - Zone the ARAP user will appear in.
- **ARAP Node Net Range** - Range of network numbers for ARAP users.
- **Max ARAP Nodes Reserved** - Maximum number of ARAP connections reserved for use. ARAP node numbers are reserved ahead so that a remote user does not have to wait for a node to be negotiated with the network.
- **Min ARAP Nodes Reserved** - Minimum number of ARAP connections reserved for use. ARAP nodes are reserved ahead so that a remote user does not have to wait for a node to be negotiated for.
- **Allow ARAP Password Change** - Set to TRUE if the ARAP user can change the password.
- **Max Password Length** - Maximum length of password for ARAP client.
- **Min Password Length** - Minimum length of password for ARAP client.
- **Number of ARAP Password Retries** - Number of times an ARAP user can retry typing in the password.
- **Force Manual ARAP Password Entry** - Setting this parameter to TRUE forces the user to enter a password when connecting via ARAP.
- **Max Routing Table Size** - Limit of Routing Table entries allowed. This number can increase with more memory in the system
- **Max Forwarding Table Size** - Limit of Forwarding Table entries allowed. This number can increase with more memory in the system.

CLI Reference Guide   113

show appletalk network <name> counters

Displays the counters for the specified Appletalk network.

- **Input Packets** - sum of packets received by this network
- **Output Packets** - sum of packets transmitted by this network
- **AARP Inbound Probes** - probes received to get an address
- **AARP Outbound Probes** - probes sent out with an address
- **AARP Inbound Requests** - requests received to translate an address
- **AARP Outbound Requests** - requests transmitted to translate an address
- **AARP Inbound Responses** - responses received for probes and requests
- **AARP Outbound Responses** - responses sent due to probes and requests
- **DDP Inbound Receives** - sum of AppleTalk packets received
- **DDP Inbound Local Datagrams** - datagrams received by DDP
- **DDP No Protocol Handlers** - sum of requests asking for unknown socket
- **DDP Too Short Errors** - sum of packets too short
- **DDP Too Long Errors** - sum of packets too long
- **Checksum Errors** - sum of packets failing checksum
- **DDP Forwarding Requests** - sum of packets forwarded
- **Echo Requests** - sum of echo packets received
- **Echo Replies** - sum of echo packets replied to

ZIP COUNTERS
- **GetNetInfo Packets Received** - number of times a MAC asked what network it was on
- **GetNetInfo Reply Packets Sent Out** - sum of replies to above
- **Invalid Zone -** ZIP packets counted with invalid zone names
- **Invalid Address -** ZIP packets counted with invalid addresses

114

show appletalk network <name> **settings**

Displays the settings for the specified network.

- **Interface** - interface this Appletalk network runs on
- **Address Range** - address of this network
- **Frame Type** - encapsulation type
- **Description** - additional information about network
- **Status** - ROUTING
- **Node Address** - network node number the router obtained on this network
- **Desired Node Address** - configured network node number
- **Current Zone** - zone the router is registered in
- **Default Zone** - default zone name for the network
- **Seed Router** - network router with network number built into its port descriptor
- **Network Learned From** - address of the node that the network information was learned from.
- **Zone Garnered From -** default zone from which AT zone list info is gathered
- **Send DDP Checksums -** DISABLED (default) or ENABLED
- **AARP Gleaning -** ENABLED (default) or DISABLED

  ZONES
- **Name** - the name of each zone
- **Status** - VALID or INVALID

show authentication counters

Displays the RADIUS and local User Authentication counters.

  AUTHENTICATION COUNTERS
- **Local Successful Authentications** - # of times user/password pair matched
- **Local Failed Authentications** - # of times user/password pair didn't match
- **Remote Successful Authentications** - # of times RADIUS OK'd user
- **Remote Failed Authentications** - # of times RADIUS rejected user

CLI Reference Guide   115

show authentication settings

Displays the RADIUS and local User Authentication Settings, which you can modify using the *set authentication* command.

AUTHENTICATION SETTINGS
- **Local Authentication is** - ENABLED or DISABLED
- **RADIUS Authentication is** - ENABLED or DISABLED
- **Primary Server is** - IP address of the primary RADIUS server
- **Primary Server Port is -** Port # of the primary RADIUS server
- **Secondary Server is** - IP address of the secondary RADIUS server
- **Secondary Server Port is -** Port # of the secondary RADIUS server
- **Retransmission Timeout** - interval between retransmissions
- **Max Retranmissions** - number of retransmissions before failure reported

show clearTCP or **show clearTCP settings**

Displays the clearTCP *connected* message. It can be modified using the *set clearTCP connected_message* command.

show command or **command settings**

Displays the settings for Command History Depth, Current and Local Prompt, Login Required and Idle Timeout. See *set command [parameter]* to modify. Prompts can hold a maximum of **64** characters. For example:

COMMAND SETTINGS:	
History Depth:	10
Global Prompt:	NETServer>
Local Prompt:	NETServer>
Console Login Required:	NO
Console Idle Timeout:	5
Current Idle Timeout:	0

116

show configuration or **show configuration settings**

Displays a variety of system information including system, network, protocol, interface, forwarding, routing, bridging, DNS, host and datalink parameters.

show connection counters

Displays the counters kept for dial-in connections.

- **Number of Calls** - number of incoming calls

show connection settings

Displays the settings for dial-in connections, which can be modified using the *set connection* command.

SETTINGS FOR CONNECTIONS
- **Host Selection Method** - ROUND-ROBIN or RANDOM
- **Global User Name** - USR_NETS is the global user name, 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

show critical_event or **show critical_event settings**

Displays where the log files for critical event messages are stored in the FLASH file system.

- **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 is @file:/./old-log-file.local

show date

Displays the system *date, time,* and *uptime*. For example:

CLI Reference Guide   117

System Date:	09-FEB-2107 15:06:10
System UpTime:	2d 08:37:54

show ddp or **show ddp counters**

Displays the Counters for Appletalk DDP Forwarding and Listener

APPLETALK DDP FORWARDING COUNTERS
- **Forwarding Requests** - forwarding requests received
- **Bad Routes** - packets transmitted that couldn't find a route
- **DDP Broadcast Errors** - broadcast packets dropped because this wasn't its destination
- **DDP Hop Count Errors** - packets dropped because hop count exceeded

APPLETALK DDP COUNTERS
- **Outbound Requests** - packets transmitted by DDP
- **DDP Outbound Shorts** -short packets transmitted by DDP
- **DDP Outbound Longs** - long packets transmitted by DDP
- **DDP Inbound Receives** - total AppleTalk packets received
- **DDP Inbound Local Datagrams** - forwarded packets for which this network was the destination
- **DDP No Protocol Handlers** - received requests for an unknown socket
- **DDP Too Short Errors** - short packets in error
- **DDP Too Long Errors** - long packets in error
- **Short DDP Errors** - short packets that couldn't be forwarded
- **Checksum Errors** - packets with checksum errors

show dial_out or **show dial_out settings**

Displays the current settings for the dialout server. You can modify the settings using the *set dial_out* command. For exampls:

118

DIAL_OUT SETTINGS	
Security - Login Required:	YES
Idle Timeout (User:	5
Recovery Timeout (Workstation):	5

show dns counters

Displays various counters for DNS.

- **Total Queries Received** - sum of DNS queries received
- **Total Response Sent** - sum of DNS responses sent
- **Responses from Local Client** - DNS responses from local DNS Host Table
- **Responses from Server** - 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** - server said invalid request format
- **Problems with Name Server** - internal server error
- **NonExistant 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

show dns settings

Displays settings for all DNS servers, which you can modify using *set DNS*.

- **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 will be 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

show events

Displays all events being directed to the console to also be echoed to the TELNET session you are running. Any number of users can employ this function. The *hide events* command ends this directive.

show file

Displays the contents of an ASCII file.

show filter <filter_name>

Displays the filter rules for all protocols specified in this file. The file name specified MUST be a filter file.

120

show filter <filter_name >

                         protocol [BR-ETH,BR-ETH-CALL,IP | IP-CALL,
                                    IP-RIP,IPX,IPX-CALL, IPX-RIP, IPX-SAP,
                                    ATALK,ATALK-CALL, ATALK-RTMP,
                                    ATALK-ZIP, LOGIN-ACCESS]

Displays the filter rules, based on the protocol options specified. The filter name MUST be a filter file, as listed using *list filters*.

- **BR-ETH** - Ethernet Bridge data filter rules
- **BR-ETH** - CALL - Ethernet Bridge call 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
- **ATALK** - AppleTalk data filter rules
- **ATALK-CALL** - AppleTalk call filter rules
- **ATALK-RTMP** - AppleTalk RTMP advertisement filter rules
- **ATALK-ZIP** - AppleTalk ZIP advertisement filter rules
- **LOGIN-ACCESS** - Login access filter rules

show icmp counters

Shows Input and Output Counters for ICMP. Two types of ICMP messages - error and query messages - are sent to syslog hosts.

ICMP COUNTERS
      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
- **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
- **Parameter Problems** - sum of ICMP messages generated by a router when it encounters an error
- **Source Quench** - sum of ICMP messages informing a host it should slow data transmission to ease congestion
- **Redirects** - sum of ICMP messages concerning a router advertising a host of a better next hop
- **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
- **Timestamp Replies** - sum of ICMP timestamp reply messages
- **Address Masks** - sum of ICMP Address Mask Reply messages
- **Address Mask Replies** - sum of ICMP request messages concerning a host's ability to gather network information
- **Advertise** -
- **Solicit** -

      OUTPUT COUNTERS

- **Messages** - total of ICMP messages transmitted
- **Errors** - ICMP packets transmitted with errors

122

- **Destination Unreachable** - sum of these messages sent
- **Time Exceeded** - sum of these messages sent
- **Parameter Problems** - sum of these messages sent
- **Source Quench** - sum of these messages sent
- **Redirects** - sum of these messages sent
- **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
- **Advertise** -

show icmp settings

Displays incoming login-access information including logged ICMP packets.

show imodem interface <name> **settings**

Displays the Current Modem Configuration screen (ATI12 command)
followed by the Switch Settings Screen (ATI4 command):

```
U.S. Robotics Total Control MP I-modem with ISDN/V.34 ISDN Switch
Settings...
   Switch Protocol *W   2                        US National ISDN-1
   Multipoint      *M   1                        Multi-point
   Dialing Mode
   SPID            *S1  84755511110111       <-SPID1
                   *S2  84755511120111        SPID2
   Directory No.   *P1  5551111              <-DN1
                   *P2  5551112               DN2
   TEI             *T1  00                     Automatic TEI
                   *T2  00                     Automatic TEI
   Physical Interface:  Active
   Data Link Layer  :  Active
OK
```

CLI Reference Guide   123

```
USRobotics Courier V.Everything Settings...

 B0  C1  E1  F1  Q0  V1  X7
 BAUD=115200 PARITY=N  WORDLEN=8
 DIAL=PULSE  ON HOOK  TIMER

 &A3  &B1  &C1  &D2  &G0  &H1  &I0  &K1  &L0  &M4  &N0
 &P0  &R2  &S0  &T4  &X0  &Y1

 S00=000  S01=000  S02=043  S03=013  S04=010  S05=008  S06=002  S07=090
 S08=002  S09=006  S10=007  S11=070  S12=255  S13=000  S14=000  S15=000
 S16=000  S17=000  S18=000  S19=000  S20=000  S21=010  S22=017  S23=019
 S24=150  S25=000  S26=001  S27=000  S28=008  S29=020  S30=000  S31=000
 S32=009  S33=000  S34=032  S35=000  S36=000  S37=000  S38=000  S39=000
 S40=000  S41=000  S42=126  S43=200  S44=015  S45=000  S46=000  S47=000
 S48=000  S49=000  S50=000  S51=000  S52=000  S53=000  S54=064  S55=000
 S56=000  S57=000  S58=000

 LAST DIALED #: T5558883333
```

124

show interface <interface_name> **counters**

Displays counters for the specified interface.

INPUT COUNTERS
- **Octets** - bytes received
- **Ucast** - Unicast packets received
- **MultiCast** - Multicast packets received
- **BroadCast** - broadcast packets received
- **Discards** - Number of inbound packets which 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** - unknown protocol in packet

OUTPUT COUNTERS
- **Octets** - bytes transmitted
- **Ucast** - unicast packets transmitted
- **MultiCast** - multicast packets transmitted
- **BroadCast** - broadcast packets transmitted
- **Discards** - Number of outbound packets which 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)

CLI Reference Guide   125

show interface <interface_name> **settings**

> Displays settings for the specified interface. An example of the settings is shown below.

```
INTERFACE mod:1 SETTINGS
Description:                        Netserver Modem Driver
Type:                              RS232
Speed:                             28800
High Speed:                        0
Administrative Status:             Up
Operational Status:                Up
Link Up/Down Traps:                ENABLED
Promiscuous Mode:                  FALSE
Connector Present:                 TRUE
Filter Access:                     OFF
Last Change:                       0d 00:00:02
Input Filter:
Output Filter:
Host Type:                         SELECT
Connection Type:                   NORMAL
Port Type:                         LOGIN_NETWORK
User Name:                         larry
Access:                            DIAL_IN
Start Time:                        24-DEC-2131 11:15:56
Dial Prefix:
Init Script:                       USR_int
TCP Port:                          0
Protocol:                          PPP
Prompt:                            login:
Message:                           Welcome to USRobotics
Host Address:                      000.000.000.000
Login Service:                     TELNET
```

126

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 settings

Displays system wide IP information.

- **IP Dynamic Address Pool Begin** - start of IP address range
- **IP Dynamic Address Pool Size** - size of IP address range
- **IP System Host Address** - IP address of the system
- **IP Forwarding** - ENABLE or DISABLE forwarding of IP packets

CLI Reference Guide   127

show ip network <network_name> **settings**

Displays parameter settings for the specified IP network. See the *set ip network* command on page 85 for additional details.

- **Interface** - interface this IP network runs on
- **Network Address** - network address of this IP network
- **Frame Type** - frame type used by the interface
- **Mask** - subnet mask used by this IP network
- **Station** - station address of this IP network
- **Broadcast Algorithm** - broadcast algorithm used for this network
- **Max Reassembly Size** - maximum packet size allowed to be reassembled from fragments
- **IP Routing Protocol** - routing protocol used
- **IP RIP Routing Policies** - routing policies used by RIP
- **IP RIP Authentication Key** - text string used for RIPv2 authentication
- **Status** - ENABLED, ACTIVE, INACTIVE, DISABLED

show ip routing settings

Displays parameter settings for the specified IP network. Statistics are gathered from parameters configured by the *set ip routing* command.

- **IP Router Administrative Status -** whether status is enabled or not
- **IP Static Remote Routes -** whether static routes are enabled or not
- **LAN Host Address** - IP address of Ethernet host
- **IP Autonomous System Number** - system number assigned
- **IP Max Table Size** - maximum number of IP Routing Table entries
- **IP Max Metric Entries** - maximum metric entries allowed
- **IP RIP** - whether RIP is enabled on not
- **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

128

show ipx counters

Displays counters for all IPX network activity.

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** -
- **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

CLI Reference Guide   129

show ipx network <network_name> **counters**

Displays statistics for the specified IPX network.

- **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 <network_name> **settings**

Displays parameter settings for the specified IPX network. You can modify most of these values using the *set ipx network* command.

- **Interface** - interface this IPX network uses
- **Network Address** - network address of this IPX network
- **Frame Type** - frame type used by the interface (ETHERNET II or SNAP)
- **Maximum Packet Size** - maximum allowable packet size for this IPX network. Default is 1500.
- **Status** - operational state of the network
- **Network Delay (ticks)** - time in number of ticks it takes to reach this IPX network
- **Network Learning Retries** - number of times this network will resend packets to discover its directly connected neighbors
- **Diagnostics** - sending of diagnostic packets ENABLED or DISABLED
- **NetBIOS** - support ENABLED or DISABLED
- **NetBIOS Name Caching** - support ENABLED or DISABLED
- **NetBIOS Cache Timer (sec)** - interval a NetBIOS system will be kept in the cache
- **NetBIOS Maximum Hops** - most hops this network will make to locate a NetBIOS system
- **RIP State** - status ENABLED or DISABLED
- **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)** - number of seconds to wait before aging out RIP entries
- **RIP Age Multiplier** - number to multiply the rip_update_interval by, to obtain the value for aging out the entries in the RIP database

130

- **RIP Max Packet Size** - largest allowable size of a RIP packet
- **RIP Broadcast** - support ENABLED or DISABLED
- **RIP Periodic** - support ENABLED or DISABLED
- **SAP State** - support ENABLED or DISABLED
- **SAP Pace** - fastest pace, in packets per second, at which SAP packets may be sent on this circuit (*not settable via the CLI*)
- **SAP Update (sec)** - # of seconds waited before SAP entries aged out
- **SAP Age Multiplier** - number to multiply the *sap_update_interval* by, to obtain the value for the aging out the entries in the SAP database
- **SAP Packet Size** - greatest allowable size of a SAP packet
- **SAP Broadcast** - support ENABLED or DISABLED
- **SAP Periodic** - support ENABLED or DISABLED
- **SAP Nearest Server Reply** - SAP seeks nearest neighbors, YES or NO

show ipx rip counters

Displays information about RIP for IPX.

- **Incorrect RIP Packets** - number of RIP packets that do not make sense

show ipx rip settings

Displays information about RIP for IPX.

- **State** - ON or OFF
- **Incorrect RIP Packets** - number of RIP packets that do not make sense

show ipx sap counters

Displays information about SAP for IPX.

- **Incorrect SAP Packets** - number of SAP packets that do not make sense

CLI Reference Guide   131

show ipx sap settings

Displays information about SAP for IPX.

- **State** - ON or OFF
- **Incorrect SAP Packets** - number of SAP packets that do not make sense

show ipx settings

Displays settings for dynamic IPX networks. You can modify these values using the *set ipx system* command.

- **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
- **Dynamic Address Pool Size** - number of addresses to reserve for dynamic IPX address assignments

show memory

Displays System DRAM Memory usage.

- **Total System Memory Resources** - total amount of memory in system
- **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

show modem group <name>

Displays the list of interfaces that belong to the specified modem group.

132

show network <name> **settings**

Displays the configured settings for the specified network. The display varies depending on the type of network specified.

show network <name> **counters**

Displays the statistical counters for the specified network. The display varies depending on the type of network specified.

show ppp on interface <name> **settings**

Displays PPP settings on the specified WAN interface when interface is active.

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
- **Local Endpoint Length** - maximum length of the local Endpoint Discriminator Address, default is 6
- **Local Endpoint ID** - value of the local Endpoint Discriminator Address
- **Remote Endpoint Class** - value of the remote Endpoint Discriminator Class, which indicates the type of address being used as the identifier
- **Remote Endpoint Length** - maximum length of the remote Endpoint Discriminator Address
- **Remote Endpoint ID** - value of remote Endpoint Discriminator Address

SETTINGS for PPP BUNDLE 1 COMPRESSION
- **Operational Status** - *Opened* or *Not Opened*
- **Compression Protocol** - authentication protocol used by the local PPP entity when it authenticated the local PPP entity to the remote PPP entity: PAP, CHAP or NONE

CLI Reference Guide   133

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 is 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 will use Protocol Compression when transmitting packets to the remote PPP entity, ENABLED is the default
- **Remote To Local Protocol Compression** - Indicates whether the remote PPP entity will use Protocol Compression when transmitting packets to the local PPP entity, ENABLED is the default
- **Local To Remote ACC Compression** - Indicates whether the local PPP entity will use Address and Control Compression when transmitting packets to the remote PPP entity, ENABLED is the default
- **Remote To Local ACC Compression** - Indicates whether the remote PPP entity will use Address and Control Compression when transmitting packets to the local PPP entity, ENABLED is the default

SETTINGS for PPP LINK AUTHENTICATION

- **Operational Status** - *not opened* or *opened*
- **Local To Remote Compression Protocol** - authentication protocol used by the local PPP entity when it authenticated the itself to the remote PPP entity, PAP is the default
- **Remote To Local Compression Protocol** - authentication protocol used by the remote PPP entity when it authenticated the itself to the local PPP entity , PAP is the default

134

show ppp on interface <name> **counters**

Displays statistics for PPP running on the specified interface when interface is active.

   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
- **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

CLI Reference Guide   135

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
system transmit authentication name using *set system* command.

- **DIAL-IN Users Authenticate PAP or CHAP** - Choices are:
  CHAP, PAP, EITHER or NONE. *EITHER* is the default
- **System Transmit Authentication Name** - remote account keyword used
  by PPP at the datalink layer for WAN connections

show security_option or **show security_option settings**

Displays status for SNMP User Access and Administration by Remote Users.
You can modify the 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.

- **SNMP User Access** - ENABLED (default) or DISABLED
- **Administration by Remote User** - ON (default) or OFF

136

show snmp counters

Displays many SNMP statistics.

INPUT COUNTERS
- **Packets** - number of SNMP packets received
- **Bad Versions** - SNMP messages for an unsupported SNMP version
- **Bad Community Names** - SNMP messages which used an unknown SNMP community name
- **Bad Community Uses** - SNMP messages which 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 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

CLI Reference Guide   137

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 snmp settings

Displays SNMP settings, which you can modify using *enable* or *disable snmp authentication traps* commands.

- **Authentication Traps** - ENABLED (default) or DISABLED

show system or **show system settings**

Displays system information.

- **System Descriptor** - for example:
  USRobotics Total Control NETSERVER V1.0.0, Built on Oct 31 1996 at 11:33:05.
- **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

138

- **System Location** - site where system is located. Modify using *set system* command
- **System Services -** for example, Internet EndToEnd Applications
- **System Transmit Authentication Name** - keyword for PPP on the WAN, modified using *set system* command
- **System Version** - loaded version of the system software

show tcp counters

Displays system-wide TCP statistics.

    TCP COUNTERS
- **Active Opens** - number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state
- **Passive Opens** - number of times TCP connections have made a direct transition to the SYN-RCVD state from the 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 TCP settings

Displays system-wide TCP settings. Note: These settings cannot be edited.

TCP SETTINGS
- **Retransmission Algorithm** - for example, Van Jacobson
- **Minimum Timeout** - minimum retransmission timeout interval
- **Maximum Timeout** - maximum retransmission timeout interval
- **Maximum Connections** - sum of TCP connections allowed. Default: **1024**.

show telnet or **show telnet settings**

Displays the status of the TELNET *escape* feature (ENABLED or DISABLED). It is set using *disable* and *enable TELNET escape* commands.

show udp or **show udp counters**

Displays statistics for UDP datagrams.

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> or **show user** <name> **settings**

Displays the parameters defined for the specified user. The type of information displayed depends on the type of user you specify. You can use *list users* to see which users are defined, and what *type(s)* user each is.

140

TELNET

TELNET commands are available to users who dial in, and whose *type* is
network (type parameter in *add user*), whose *host_type* is **prompt** (host_type
parameter in *set login user*), and whose *login_service* is **TELNET**
(login_service parameter in *set login user*).

telnet <ip_name_or_addr>

Establishes a TELNET client session with the specified IP host name or
address. In order for the system to resolve the host name, you must either add
the host name and address to the DNS Local Host Table, or define a DNS
server.

telnet <ip_name_or_addr> **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. The
default TCP port number is **23**.

UNASSIGN

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 *show modem_group*.

CLI Reference Guide   141

verify filter <filter_name>

> Verifies the syntax of a filter file, which has been previously *add*ed 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, then you use this command to verify the files 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)*.

connect <ip_name_or_addr>

> Connects a dial-in user to the specified IP host.

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. See the **CLI Exit Commands** to learn how to exit the CLI, and return to the **Dial-in User Commands**.

rlogin <ip_name_or_addr>

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 <ip_name_or_addr> **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_addr>

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_addr> **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.

TELNET Commands

The following commands are available to users whose **host_type** is *prompt*, and whose **login_service** is *TELNET*. Login users who have TELNET client connections can access these commands by hitting [Ctrl] **]** (ctrl]).

close

Closes the active TELNET connection.

help

Lists the available commands

send <string>

Sends a TELNET control character. The available commands are:

Parameters	Description
AYT	Are you there
IP	Interrupt process
BRK	Break
AO	abort output
EC	erase character
EL	erase line
GA	go ahead
NOP	no - operation
EOR	end of record
SYNC	synch

set escape <string>

Allows changing the TELNET escape character from [Ctrl] **]** (ctrl]) 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** (ctrl x), use '**set escape ^ x**'.

status

Displays the IP address of the remote host 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

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

Logout

Leave the CLI and close this connection. This ends the dial-in user's or TELNET session.

Command Features

The command language has several built in features that make it easier to use. When abbreviating commands, it sometimes hard to remember the commands and their syntax. Using command completion and positional help aids in jogging your memory of the commands and their parameters, while you are typing in a command string.

Command Line Edit

Command line edit allows non-destructive cursor movements on a command already typed.

Ctrl **b** (ctrl b) or ← (left arrow)	go back one character
Ctrl **f** (ctrl f) or → (right arrow)	go forward one character
Esc **b** (Esc-b)	go back one word
Esc **f** (Esc-f)	go forward one word
Ctrl **a** (ctrl a)	go to beginning of command
Ctrl **e** (ctrl e)	go to end of command
Ctrl **d** (ctrl-d)	delete character
Ctrl **k** (ctrl k)	delete line

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.

Ctrl **p** (ctrl p) or ↑ (up arrow)   recall previous command in history list

Ctrl **n** (ctrl n) or ↓ (down arow)   recall next command in history list

Positional Help

Positional help displays the list of possible parameters when you type **?** after any command or parameter. It then 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, and add it to your command, without having to retype 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** **(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 will be displayed (completed), and you can continue entering the command. If the command or parameter is ambiguous, the bell will ding, and the display will not change.

146

Output Pause

The output will pause when there is more than 24 lines of output. Type 'more' (or press CR) to continue, or 'quit' to stop.

Command Kill

To discontinue the current command action, and flush any commands which have been typed ahead, use ⌨Ctrl⌨ **c** (ctrl c).

Comments

;   Nothing following the semicolon will be processed. This is useful when you are writing CLI script files. The *do* command runs a CLI script.

Index

CLI Reference Guide

P

R

S