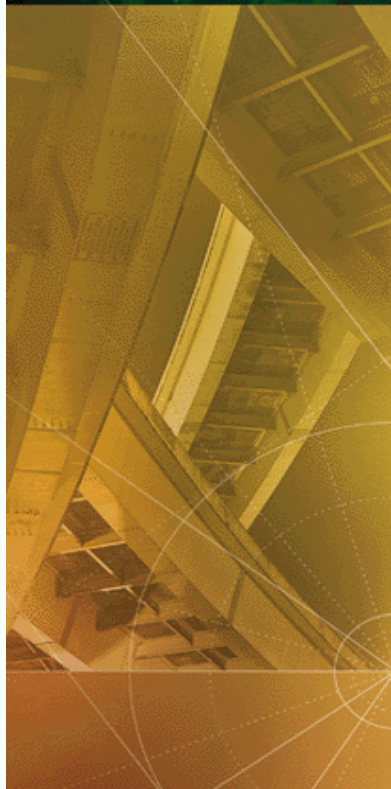
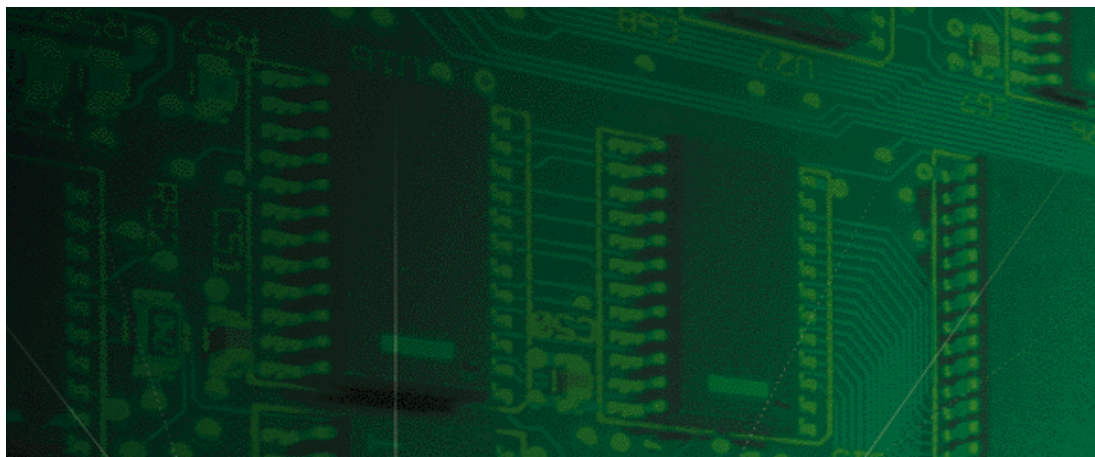




HiPer ARC Product Reference

Version 4.1



Part No. 1.024.1905-00

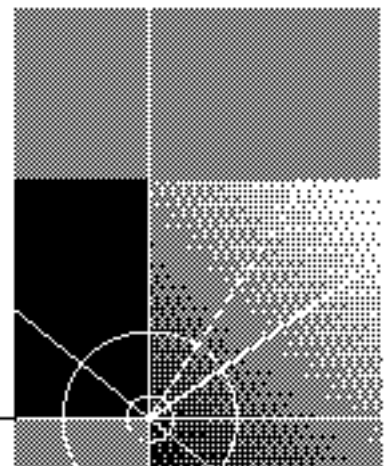


HiPer ARC Product Reference

Version 4.1

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

Part No. 1.024.1905-00
Published September 1998



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

Copyright © 1998, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

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

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

UNITED STATES GOVERNMENT LEGENDS:

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

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

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

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

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark of X/Open Company, Ltd. in the United States and other countries.

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

This guide was written and illustrated by Larry Cortese.

CONTENTS

ABOUT THIS GUIDE

Conventions	xvii
Related Documentation	xviii
Year 2000 Compliance	xix
Contacting 3Com Carrier Systems	xix

1 OVERVIEW

What's New with HiPer ARC v2	1
Full IPX Support	2
IPX Unnumbered Networks	2
Variable IPX RIP/SAP Timers	2
Multiple FLASH Configurations and Boot Images	2
TFTP Configuration/loading	2
Tap to Monitor Port Traffic	2
Layer 2 Tunneling Protocols (L2TP)	2
Point-to-Point Tunneling Protocol (PPTP)	3
Multilink PPP Interspan Protocol (MPIP) and Virtual Tunneling Protocol (VTP)	3
IP Multicast Forwarding	3
Reported IP Address	3
PPP EAP Client	3
TACACS+ support	4
RADIUS enhancements	4
Local DNS Host Rotation and Authentication	4
Call session statistics	4
Chat scripts	4
ATM support on the PCI ATM Network Interface Card	5
Embedded SNMP Version 1 agent	5
PPP startup messages	5
RADIUS monitor	5
Dynamic Slot Assignment	5
HiPer ARC Applications	6
IP Terminal Service	6
Network Dial In Access	7
Dial-Out Access	8
LAN-to-LAN Routing	9
Packet Filtering	9
Administrative Utilities	9
Total Control Hub Overview	10

System Components	10
Chassis Midplane	11
Midplane Data Buses	11
How HiPer ARC works with modems	12

2 HiPer ARC SETUP

System Administrator Requirements	15
TCP/IP Reference Material	15
Accessing the Configuration Interface	16
Establishing Communications with HiPer ARC	16
IBM-PC Compatible Computers	16
UNIX-Based Computers	16
Automated Quick Setup Programs	16
HiPer ARM Setup Wizard	16
Quick Setup (CLI)	16
Command Line Interface Conventions	17
Most commands are not case sensitive	17
Many commands are position independent, multi-tiered and have keywords	17
You can abbreviate commands	17
Double quotations distinguish text strings	17
Command syntax and CLI rules	17
Command completion	18
Command retrieval	18
Command reprint	18
Command Line Editing	18
Paused (--More--) output display	18
Using general and positional help	19
First disable, then delete objects	19
Saving changes	19
Running and stopping processes	19
Using network services	19
Using add and set commands	20
Using list and show commands	20
Rebooting	20
Hardware Setup	20
Security Configuration Advisory	20
Password Protecting adm	20
Adding a New Administrative User And Disabling adm	21
Using Quick Setup	21
Configuring with Quick Setup	21
Setting Up the System Manually	28
Power On	28
System Basic Setup	29
IP Configuration	30
IPX Configuration	32
Determining the IPX Network Number	32

For File Servers Running Novell Version 3.xx	32
For File Servers Running Novell Version 2.xx	32
Setting IPX Parameters	33
DNS Configuration - Optional	33
SNMP Configuration - Optional	34
Configuring a Manage User	35
Manually Configuring the WAN Interface	36
Configuring Static Routes	36
IP Routes	36
IPX Routes	36
Configuring Two HiPer ARCs on the Hub	37
Slot Configuration Test Cases	37
Example 1	37
Example 2	38
Example 3	38
Example 4	39
Example 5	39
Example 6	39
Viewing Chassis Parameters	40
PPP Compression Options	40
Viewing Compression Settings	40

3 CONFIGURATION OVERVIEW

Setting Up Applications	43
Configuration Command Overview	43
Configurable Table Overview	44
Interface Tables	44
User Table	44
Local and Login Hosts Tables	44
Initialization Script and Global Host Tables	45
Facility Level Table	45
Module Table	45
IP Network Table	45
IP Address Pool Table	45
IP Interface Block Table	45
Forwarding and IP Routing Tables	45
SNMP Configuration Tables	45
SYSLOG Table	46
Event Critical Messages Table	46
Filter and Associated Tables	46
File Table	46
Network Services and Available Servers Tables	46
Dial-Out Port Table	46
UDP Listeners Table	46
TCP Connections Table	46
DNS and Associated Tables	46
TFTP Access Table	46

Traceroute and Traceroute Hop Tables	46
Remote Ping and Ping Busy Out Tables	47
Address Translation Table	47
Chassis and Packet Bus Tables	47
CIP Port Parameter Table	47
User Manager Active Sessions Table	47
Chat Script Table	47
Modem Tables	47
PPP Tables	47

4 IP TERMINAL SERVER SETUP

Remote User Overview	49
Configuring the Remote Computer	49
Configuring Login Hosts	50
Host Name	50
Address	50
Preference	50
Rlogin, TELNET and ClearTCP Ports	50
Configuring Login Users	51
Password	51
Login Service	51
Type	51
Host Type	52
Login Host IP Address	52
Login Service	52
TCP Port	52
Terminal Type	52
IP Terminal Service Case Studies	53
Case Study A	53
Case Study B	55

5 NETWORK DIAL-IN ACCESS

Dial In Introduction	57
Dial-in Access Overview	57
IP Parameters	58
IPX Parameters	58
Remote Computer Setup	58
Configuring Address Pools	59
Configuring an IP Address Pool	60
Configuring an IPX Address Pool	60
User Configuration Overview	60
Defaults	60
Remote Addressing Options	61
Network User Types	61
Configuring an IP/IPX Network User	61
Password	61

Type	61
Network Service	61
Configuring PPP Parameters for Network Users	63
Compression Algorithm	64
Expansion Algorithm	64
Minimum Compression Size	64
Receive Asynchronous Character Control Map	64
Reset Compression Mode	64
Transmit Asynchronous Character Control Map	65
Channel Decrement	65
Channel Expansion	65
Maximum Channels	65
Configuring Additional Parameters	65
MTU	65
Receive PPP Authentication	65
Phone Number	66
Alternate Phone Number	66
Idle and Session Timeouts	66
Remote Access Case Study A	66
Assumptions	66
How to Configure this User	66
How it Works	67
Remote Access Case Study B	67
Assumptions	67
How to Configure this User	68
How it Works	68
Remote Access Case Study C	69
Assumptions	69
How to Configure this User	69
How it Works	69

6 NETWORK DIAL-OUT ACCESS

Introduction	71
Overview	71
IP/IPX Dial-Out	71
ClearTCP Dial-out	71
Network Communications Services Interface (NCSI)	72
NCSIPort	72
How It Works	72
TELNET Dial-Out	72
Network Dial-Out Configuration Overview	72
Network Dial-Out Configuration	73
Configure Modem Groups	73
Configure Dial-Out Service	73
Configure Dial-Out Users	74
Set Global Dial-Out Parameters	74
Configure Telnet Dial-out Service	75

Editing Network Services	78
NCSI Client Software Installation and Setup	78
Installing NPC Client for Windows 95	78
Configuring NCSIport for 95	80
Dialing Out Using a NCSI Port	82
An Overview of NPC's Windows 95 Based Options	87
Dial-out Case Studies	87
Case Study A	87
How it Works	88
Case Study B	89
How it Works	89

7 LAN-TO-LAN ROUTING

LAN-to-LAN Routing Overview	91
Connection Establishment	92
Dynamic Routing Settings	92
Dial-Out Scripts	92
Bandwidth Allocation	92
IP Routing	93
IPX Routing	93
Dynamic and Static Routes	93
How Packets are Routed	93
Establishing Connections to Remote Gateways	94
Configuring an Internal Network for Unnumbered Links	94
Spoofing	94
Authentication	94
PAP Authentication	95
CHAP Authentication	95
Configuring LAN-to-LAN Routing	95
LAN-to-LAN Routing Case Study	103
Assumptions	103
Configuring HiPer ARC main_office	104
Configuring LAN Networks	104
Adding User Parameters	104
Configuring Connection Parameters	105
Setting Authentication	105
Configuring Multilink PPP - Optional	105
Saving the Configuration	105
Testing the Connection - Optional	106
Configuring HiPer ARC branch_office	106
Configuring LAN Networks	106
Adding User Parameters	106
Configuring Connection Parameters	107
Setting Authentication	107
Configuring Multilink PPP - Optional	107
Saving the Configuration	107
Testing the Connection - Optional	108

Capsule Summary A	109
HiPer ARC main_office	109
HiPer ARC branch_office	109
Capsule Summary B	110
HiPer ARC main_office	110
HiPer ARC branch_office	110
Capsule Summary C	111
HiPer ARC main_office	111
HiPer ARC branch_office	111

8 TUNNELING WITH HIPER ARC

Introduction	113
Using L2TP	113
How it Works	114
Configuring an L2TP Tunnel on HiPer ARC	115
Configuring a Tunneled Dialin User	115
Configuring a Tunneled Dialout User	117
Configuring an L2TP Tunnel on a RADIUS Server	119
Using PPTP	120
Configuring a PPTP Tunnel on HiPer ARC	120
How it Works	120
Configuring a Tunneled Dialout User	121
Configuring a PPTP Tunnel on a RADIUS Server	123
Using MPIP	124
How it Works	124
Configuring a Multi-link PPP connection with MPIP	125

9 PACKET FILTERS

Filtering Overview	129
Filtering Capabilities	129
Information Sources	130
Filter Types	130
Data Filters	130
Advertisement Filters	130
Call Filters	130
Generic Filters	131
Creating Filters	131
Filter File Components	131
File Descriptor	131
Protocol Sections	131
Protocol Rules	132
Generic Filter Rules	132
Specifying the Filtering Action	133
Creating Filter Files	133
Configuring Filters	135
Setting Filter Access	135
Interface Filters	135

Input Filter	136
Output Filters	136
Call Filters	136
Input Filters vs. Output Filters	136
User Filters	136
Assigning a Filter to an Interface	137
Assigning a Filter to a User	137
Managing Filters	137
Displaying the Managed Filter List	138
Adding Filters to the Managed List	138
Removing a Filter from an Interface	138
Removing a Filter from a User Profile	138
Deleting a Packet Filter	139
Verifying Filter File Syntax	139
Showing Filter File Contents	139
Generating SYSLOG Messages for Filtered Packets	139
General Filter Setup	140
Filter Examples	141
IP Packet Filter Rule Examples	141
Source and Destination Address Filtering	141
Masks	142
TCP and UDP Parameter Filtering	142
Standard Port Numbers	143
IP and IPX-RIP Packet Filtering	143
IPX-SAP Filtering	144
ICMP Packet Filtering	144
IP/IPX-Call Filtering	145
Login-Access Filtering	145
HiPer ARC Global Filtering	146
Global Switch to Drop IP Fragments with Offset = 1	146
Global Switch to Drop Packets with a Partial TCP Header	146
Global Switch to Filter Out All IP Options	146
Global Switch to Filter Out IP Source Route Options	146
Keywords	147

10 ADMINISTRATIVE TOOLS

Reconfiguring Your System	149
Customizing CLI Parameters	149
Command Prompt	149
Command History	149
Idle Timeout	149
Login Required	150
Local Prompt	150
Setting the System	150
Running Script Files	150
Using Chat Scripts	152
Bootup Options	152

Using the Boot Configuration Menu	152
Software Downloads	155
TELNETd Access Port	155
Discarding and Renaming Files	156
Using the CLI Editor	156
Edit Command	156
Communicating with Remote and Local Sites	158
IGMP Forwarding	158
How it Works	158
Step by Step Instructions	159
Scenario A: Mbone Connection Via Ethernet Interface	164
How it Works	164
Scenario B: Mbone Connection Via WAN Interface	165
How it Works	165
Dial, Connect and Hangup Commands	165
Dial Command	166
Hangup Command	166
Reboot Command	166
Dialin User Message	166
Exiting the CLI	167
Bye, Exit, Leave, Quit Commands	167
Logout Command	167
Network Services	167
Adding Network Services	167
Enabling and Disabling Network Service	169
Deleting a Network Service	169
Using TFTP	169
Using Rlogin and TELNET	169
TELNET Status	170
TELNET Control Characters	170
Closing a Connection	171
Troubleshooting Commands	171
Viewing Facility Errors	171
Terminating an Active Process	171
Resolving Addresses	171
Resolving Host Names	171
Using Ping	172
The ping command	172
Listing Ping settings	173
Showing ping statistics	173
Setting ping row ceiling	173
Configuring a ping user	173
Using ping to monitor system connectivity	173
Using RADIUS to monitor system connectivity	174
Viewing HiPer ARC System Information	175
Viewing Interface Status, Settings	175
Monitor PPP activity	175
Tap all packets	175

Syslog option	175
Screen option	175
Taps on RADIUS/TACACS+ users	176
How Tap works	176
Displaying System Information	176
List Commands	176
List Critical Events	176
Show Commands	176
Show Memory	177
Show Dial-in Connection Settings, Counters	177
List Dialin Connections	177

11 COMMAND REFERENCE

Command Format	179
Parameters	179
Entering Commands	180
Using Control Characters	180
Abbreviation and Command Completion	180
Help	180
Additional Conventions	181
Network Address Formats	181
Interface Ranges	182
Names	182
Users	182
Default User	182
Command Language Structure	169183
CLI Commands	169183
Add Commands	169183
Arp Command	169200
Assign Command	169201
Bye Command	169201
Clear Command	169201
Copy Command	169201
Delete Commands	169201
Dial/dialout Commands	169206
Disable Commands	169206
Disconnect Command	169213
Do Command	169214
Edit Command	169214
Enable Commands	169214
Exit Command	169222
Hangup Commands	169223
Help Command	169223
Hide Command	169223
History Command	169223
Host Command	169224
Join Command	169224

Kill Command	169224
Leave Command	169224
List Commands	169225
Logout Command	169252
Monitor Commands	169253
Monitoring Stop/Start	169254
Idle Timer	169255
Decode and Hexadecimal Display	169255
Option A	169257
Option B	169258
Option C	169258
Option D	169258
Option E	169258
Option F	169259
Paused Commands	169260
PING	169260
Quit Command	169261
Reboot Command	169262
Reconfigure Command	169262
Rename Command	169262
Reset Commands	169262
Resolve Command	169263
RLOGIN Command	169263
Save Commands	169263
set Commands	169264
Set User Commands	169298
Show all Commands	169306
Show Commands	169306
TELNET Commands	169360
TFTP Command	169360
Traceroute Command	169361
Unassign Command	169362
Verify Command	169363
Dial-in User Commands	169363
TELNET Commands	169364
CLI Exit Commands	169365
Command Features	169365
Comments	169366

A NOTICES & TECHNICAL SPECIFICATIONS

Chapter Overview	367
Safety Compliances & Certifications—U.S.	367
FCC Part 15 Compliance Statement	367
For More Information	367
Hardware Specifications	368
Environmental Specifications	368
Power Specifications	368

Network Application Support (NAS) Backplane Pinouts	370
System Standards and Specifications	371
Data Compression Protocols	371
Software Specifications	371
Routing Support	371
Administration	371
Filtering & Security	371
PPP Specific Features	371
Industry Standards Support	372
Client Dial-up Support	372
Other Features	372
SLIP and PPP Client Software Support	372

B ADDRESSING SCHEMES

IP Addressing Basics	373
Subnetting	373
Subnets of Class C networks	374
Reserved Addresses	375
Supernetting (Advanced TCP/IP)	375
Step 1 - Select a netmask for each supernet	376
Step 2 - Select a range of addresses for each supernet	377
Supernet Example	378
Supernetting and HiPer ARC	378
IP Subnet Mask Address Table	379

C LEDs AND SWITCHES

LEDs	381
Run/Fail LED	381
LAN TX LED	382
LAN RX LED	382
WAN TX LED	382
WAN RX LED	382
Other LEDs	382
DIP Switches	382
DIP Switches 1 and 2	383
DIP Switch 5	383
DIP Switches, 3,4 and 5	383

D EVENT MESSAGES

Event Logging	385
SYSLOG Host Event Logging	385
Console Event Logging	385
Local FLASH File Event Logging	386
TELNET Session	386
Event Logging Levels	386
Event Logging Counters	386

Using SYSLOG	387
Configuring SYSLOG on the SYSLOG (UNIX) Server	387
Configuring SYSLOG Hosts on HiPer ARC	387
Setting the Event Log Level	388
Event Message Examples	388
IP Messages	388
Call Initiation Process Messages	390
User Manager Messages	391
Filter Manager Process Messages	391
UDP Messages	391
Configuration File Manager Messages	391
TELNET Messages	392
IP Dial-out Process Messages	392

E RADIUS AND TACACS+ SYSTEMS

HiPer ARC RADIUS Enhancements	395
RADIUS Authentication	395
RADIUS Accounting	396
Obtaining RADIUS	396
Performing Authentication	396
RADIUS Authentication Process	396
CHAP Authentication Using RADIUS	396
Configuring RADIUS from the CLI	397
Configuring RADIUS Authentication Settings	397
Enabling and Disabling Authentication	398
Configuring RADIUS Accounting Settings	398
Configuring RADIUS Accounting Settings	398
Enabling and Disabling RADIUS Accounting	400
RADIUS Accounting Examples	400
RADIUS Examples by User Type	401
Terminal user with incorrect password	401
Terminal user with correct password (TELNET, Rlogin, ClearTCP)	402
Administrative Terminal User	403
Terminal User with Port Tapping Enabled	404
Framed User with Port Tapping Enabled	406
L2TP Framed User/PPP-SLIP Framed User	408
Terminal Login-Callback User	409
Framed User with Multilink PPP Enabled	411
Dialback User	413
Chat Scripting with the RADIUS User	414
Syntax	415
SEND construct	415
Timeout	416
EXPECT construct	416
Conditional constructs	417
Action Statements	417
TELNET	417

PPP	418
Disconnecting the call	418
Miscellaneous constructs	418
Run time errors	418
Script Examples	418
Example A	418
Example B	419
Example C	419
RADIUS Security Server User Table Entries	420
Required Parameters	420
Optional Parameters	421
HiPer ARC-Specific Parameters	438
HiPer ARC-Supported Local Attributes Not Set Via RADIUS	460
Enhanced RADIUS Support	461
Enhanced Packet Formats	461
Attributes	463
Enhanced Command Codes	464
Dynamic Filter Change	467
Enhanced RADIUS Reference Information	471
RADIUS Attributes	471
RADIUS Attributes	471
RADIUS Accounting Attributes	476
TACACS+	477
Authentication	478
Authorization	478
Accounting	478
TACACS+ packet header	479
TACACS+ commands	479
TACACS+ Accounting Attributes	479
TACACS+ Authorization Attributes	480

INDEX

3COM CORPORATION LIMITED WARRANTY

ABOUT THIS GUIDE

This guide describes how to configure the software for the HiPer Access Router Card (ARC), a Network Access Server (NAS) module in the Total Control Hub. Step-by-step instructions detail all HiPer ARC applications as well as all Command Line Interface (CLI) commands, security and utilities.

This guide is intended for administrators with knowledge of networking, telephony and remote access applications. While initial configuration can be accomplished easily with the help of the HiPer Access Router Manager (HARM) or the Quick Setup program, more substantial configuration requires a broader understanding of networking principles.



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

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

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

Conventions

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

Table 1 Notice Icons

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

Table 2 Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Parameter/value	The words "parameter" or "value" mean that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example: To create a user, type the following: add user <user_name> In this example, you must supply a name for <user_name>.

Table 2 Text Conventions (continued)

Convention	Description
Commands	<p>The word “command” means that you must enter the command either exactly as shown or with associated parameters and then press Return or Enter. Commands appear in bold. Examples:</p> <p>To edit a user, enter the following command:</p> <pre>set user <user_name> password <password></pre> <p>To display all IP addresses, enter the following command:</p> <pre>list ip addresses</pre>
The words “ENTER” and “type”	<p>When you see the uppercase word “ENTER” in this guide, press the Return or Enter key. Do not press Return or Enter when an instruction simply says “type.”</p>
Words in <i>italics</i>	<p>Italics are used to:</p> <ul style="list-style-type: none"> ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify CLI command parameters and chapters in this manual. Examples: <p>See <i>Chapter 11: Command Reference</i>.</p> <p>Supply the <i>IP address</i> parameter ...</p>

Related Documentation

The following documents are included in the HiPer ARC documentation set. To order additional copies, contact your sales representative.

- *HiPer ARC 4.1 NAC Getting Started Guide*
This card offers instructions to install and set hardware parameters on the HiPer ARC 4.1 NAC.
- *HiPer ARC ATM NIC Getting Started Guide*
This card offers instructions to install and use the ATM NIC.
- *HiPer ARC Manager(HARM) - Windows Quick Reference Card*
This card offers quick and easy instructions to install and use HARM on a Windows system.
- *HiPer ARC Manager - UNIX Quick Reference Card*
This card offers quick and easy instructions to install and use HARM on a UNIX system.
- *HiPer ARC Manager - Windows Online Help*
This software is included in HiPer ARC firmware for use on a Windows system.
- *HiPer ARC Manager - UNIX Online Help*
This software is included in HiPer ARC firmware for use on a UNIX system.
- *HiPer ARC 4.1 Release Notes*
These notes provide information about the 4.1 system software release, including new features and bug fixes. They also provide information about any changes to HiPer ARC’s documentation.

- *Total Control Hub 3.5 System Overview*

This guide describes how Network Interface and Application cards interact on the Hub.

- *Total Control Hub 3.5 Installation Road Map*

This quick start card outlines the steps needed to get components of the Hub installed.

- *Total Control Hub 3.5 System Install Troubleshooting Guide*

This guide details information about how to troubleshoot Hub installation problems.

- *Total Control Cabinet Getting Started Guide*

This guide describes how to set up hardware components of the Total Control Hub.

Year 2000 Compliance

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

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

Contacting 3Com Carrier Systems

Use this chart as a reference when you need to contact 3Com Carrier Systems.

Contacting 3Com Carrier Systems

3Com Corp. - 5400 Bayfront Plaza - P.O. Box 58145 - Santa Clara, CA - 95052-8145

Internet	http://www.3Com.com
----------	---

Internet Customer Support	http://totalservice.usr.com
---------------------------	---

Sales	1-800-877-2677
-------	----------------

Technical Support (U.S. and Canada)	1-800-231-8770 7 a.m. to 8 p.m. CST Monday-Friday
--	---

Technical Support (Europe, Middle East, Africa)	353-1-205-7700 9 a.m. to 7 p.m. CET Monday-Friday
--	---

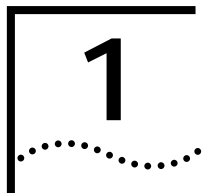
Technical Support (all other location)	1-847-797-6600 7 a.m. to 8 p.m. CST Monday-Friday
---	---

ISDN support	1-800-877-ISDN
--------------	----------------



The warranty that applies to this product is contained on the CD-ROM included with the product. Instructions to view and/or print the warranty can be found on the CD-ROM packaging.





OVERVIEW

This HiPer™ ARC Product Reference provides a basis for using the HiPer Access Router Card in 3Com's Total Control Enterprise Network Hub. HiPer ARC is a Network Applications Card (NAC) providing terminal server and remote access services, via analog and digital modem connections in a multi-protocol LAN/WAN networking environment.

The HiPer Access Router NAC is compatible with the PCI Dual 10/100 Base-T Ethernet and DS3 ATM NIC.

What's New with HiPer ARC v2

HiPer ARC v2 encompasses all the functionality of the previous release, and more. This section provides a brief overview of these new features. An in-depth description of each item can be found in subsequent chapters.

New features include:

- Full IPX support
- IPX unnumbered networks
- Variable IPX RIP/SAP timers
- Multiple FLASH configurations
- TFTP client support
- Tap to monitor port traffic
- Layer 2 Tunneling Protocols (L2TP) support
- Point-to-Point Tunneling Protocol (PPTP) support
- Multilink PPP Interspan Protocol (MPIP) and Virtual Tunneling Protocol (VTP)
- IP Multicasting (IGMPv2)
- IP Address spoofing (Reported IP Address)
- EAP client
- TACACS+ support
- RADIUS enhancements
- Local DNS host rotation and authentication
- Call session statistics
- Chat scripts
- ATM support on the PCI ATM Network Interface Card
- FLASH File System MIB
- PPP startup messages
- RADIUS monitor

- Automatic RADIUS filter (support RADIUS 3.x filters)
- Dynamic Slot Assignment

Each new feature is summarized on the following pages.



Refer to Chapter 11: Command Reference, for commands about each feature.

Full IPX Support

IPX is supported on LANs and for dialup pPPP users.

networks are enabled with largely the same support given IP networks.

IPX Unnumbered Networks

HiPer ARC supports any given dial in or dial out port to use a single network number. HiPer ARC provides a single global IPX network address. The node address for each IPX client can be accepted from the client or assigned by HiPer ARC if a client is unable to do so.

Variable IPX RIP/SAP Timers

Variable timers for IPX RIP and SAP are supported to reduce periodic updates and produce tariff savings. These are configurable on a per network basis.

Multiple FLASH Configurations and Boot Images

HiPer ARC can take a "snapshot" of an operating system configuration. This function "packages" the full system configuration as well as operation images in a file that can be stored in FLASH memory. At the direction of the administrator, the system can be requested to reboot using a "bulk configuration" file stored in FLASH.

The stored configuration can then be installed on top of an existing configuration and the system rebooted. The file remains in local storage.

TFTP Configuration/loading

HiPer ARC now supports TFTP client as well as TFTP server software to retrieve configuration files from another system. A table is maintained and used at boot time to retrieve the desired configuration files.

Tap to Monitor Port Traffic

This debugging tool records all traffic on a port or modem group and transmits it to the Console or a SYSLOG host. It's helpful to interpret raw data and display it in hexadecimal, ASCII or clear text format.

This tool records and displays raw data - similar to that provided by a protocol analyzer - before and after a call is connected and up to the point where a call is terminated on a user, interface or next session basis.

Layer 2 Tunneling Protocols (L2TP)

HiPer ARC can originate or host Layer 2 Tunneling Protocol (L2TP) sessions, which allow Virtual Private Networks (VPNs) to be established to other L2TP Network servers. HiPer ARC provides:

- L2TP Access Concentrator (LAC) support for incoming and outgoing calls
- PPP framing
- L2TP Network Server (LNS) support

Point-to-Point Tunneling Protocol (PPTP)

HiPer ARC can originate or host Point-to-Point Tunneling Protocol (PPTP) sessions, allowing Virtual Private Networks (VPNs) to be established with Windows NT Remote Access Servers (RAS) servers. HiPer ARC can support up to 8 NT RAS servers running PPTP sessions, which are saved as a global list in the FLASH file system. PPTP on HiPer ARC polls the list trying to establish tunnels with each server until a connection is made or the list exhausted.

Additionally, each local user and modem interface can connect up to 8 hosts in a port/user specified list, also saved as a list to FLASH.

HiPer ARC also offers PPTP support over incoming and outgoing ISDN/analog calls, including all protocols supported under ISDN that can carry PPP (v120, v110, 56k, sync, etc) connections. RADIUS also supports PPTP calls because it authenticates incoming calls based on DNIS/ANI data passed to the RAS server.

Multilink PPP Interspan Protocol (MPIP) and Virtual Tunneling Protocol (VTP)

HiPer ARC utilizes the Multilink PPP Interspan Protocol (MPIP) along with its proprietary tunneling protocol, VTP, to support incoming multilink PPP sessions where the links terminate on more than one HiPer ARC.

This is accomplished by MPIP re-combining MLPPP packet fragments at one endpoint router even though the links of a bundle are physically connected to different routers.

An MPIP control server residing on any HiPer ARC server located on the network keeps track of bundle owners and links, informing the client (the HiPer ARC to which the link is physically connected) who the bundle owner is. With that information in hand, the client establishes a secured VTP tunnel with the bundle owner HiPer ARC. The client uses this tunnel to transfer data on the MPIP link to the bundle owner HiPer ARC, and vice versa.

IP Multicast Forwarding

HiPer ARC provides full (host functional) IGMPv2 support including multicast registration request and proxy for clients. Specifically, it offers:

- Joining multicast groups over LAN and WANs
- Multicasting group memberships over the LAN
- Maintenance of group member lists for adjacent hosts
- Forwarding of multicast packets from the LAN to one or more HiPer ARC WAN clients, or vice versa

Reported IP Address

HiPer ARC supports unnumbered links by assigning a globally selected IP address as the local IP address for a WAN link. If this global IP address is set to zero then the LAN IP address is used.

Administrators can set the global IP address to the *same* value across multiple platforms on the same network. For example, HARC1, HARC2, and HARC3 are HiPerARCs configured with the same internal address - 1.1.1.1. If one or more PCs dial in, no matter which HiPer ARC they physically dial into, the remote address (1.1.1.1) appears the same.

PPP EAP Client

HiPer ARC supports the new PPP authentication protocol EAP (Extensible Authentication Protocol) for use with RADIUS.

TACACS+ support

HiPer ARC now supports the authentication, authorization, and accounting functionality of TACACS+.

- **Authentication** - determines who a dial-up user is and if that user should have access to the network, the access server or HiPer ARC.
- **Authorization** - determines what services a user has access to once a connection has been established. Authorization does not (but usually does) necessarily follow authentication. Authorization allows users to be mobile. Mobile and temporary users (portable users with modems in hotels and tele-commuters with modems or ISDN connections at home) can connect to the closest local connection and still have the same access privileges of their local networks.
- **Accounting** - collects information about what a user is doing and when for billing and security auditing purposes. Billing data includes connect time, user ID, location connected from, start time, and stop time. Billing information also identifies the protocol that the user is using and may contain commands being run if users are connected through NAS shell and TELNET.

RADIUS enhancements

The RADIUS Configurable PPP Compression Protocol is now supported, allowing a RADIUS Server to return the compression protocol type for each user in the Access-Accept message. Also, support for a DNS/RADIUS Server is available. It works by HiPer ARC querying a DNS server for a RADIUS server to use for a given user. This option is globally configurable.

NETServer 3.x RADIUS filter rule handling is now supported. If RADIUS returns an Authentication-Response, we support NETServer 3.x and HiPer ARC formats.

Local DNS Host Rotation and Authentication

HiPer ARC supports DNS host rotation and authentication in an external security server, using the responses from DNS or the authentication server. The feature includes three different components:

- The DNS Client supports DNS responses with multiple entries in the RR record (multiple IP addresses for a given name). At least the first 40 addresses are saved in the cache.
- When a login user is created, a host name can be assigned to the user as a destination. The name entered is not resolved at the time the name is entered, but rather the name is saved in the user profile. Once a user logs in, a DNS lookup occurs to get the list of addresses associated with the name. From these addresses a primary followed by eight alternate servers is built.
- A global switch allows randomization of IP addresses when returned as primary and alternate addresses. This allows each user to potentially connect to different hosts creating a type of load balancing.

Call session statistics

HiPer ARC provides a set of session statistics per port which are reset at the outset of every call to provide error statistics on a per-call basis.

Chat scripts

Chat-style scripts can be used to support dial in users, including setting up a TELNET session, reporting IP and gateway addresses, and runtime errors, setting time-outs, and disconnecting calls. HiPer ARC supports chat scripts locally as well as remotely for RADIUS users.

**ATM support on the PCI
ATM Network Interface
Card**

HiPer ARC supports the drivers, protocols, and network management for ATM on the PCI ATM NIC as well as a separate binary image for ATM and Ethernet. ATM support includes permanent virtual circuits (PVCs) over ATM using RFC 1483 encapsulation, IP over ATM using RFC 1577 for PVCs and SVCs, UNI 3.0 and 3.1, and ILMI.

More information can be found in the Total Control ATM NIC manual.

**Embedded SNMP
Version 1 agent**

HiPer ARC contains an embedded SNMP Version 1 Agent. All parameters and statistics are available as SNMP objects. Whenever possible, standard MIBs are supported such as MIB II, IPX MIB, Ethernet MIB, and many others.

Objects that are 3Com-specific are described in our proprietary MIB - *usr_hiper.mib*, a text file which is included in the HiPer ARC binary on the distribution CD-ROM. MIBs can also be obtained from 3Com's TotalService Website at <http://totalservice.usr.com>.

PPP startup messages

A message string can be displayed at a client's terminal when a PPP connection is established in HiPer ARC. Also, the HiPer ARC's local (server's) IP address and remote (client's) IP address can be shown.

RADIUS monitor

HiPer ARC supports monitoring of realtime RADIUS activity. This feature monitors: all RADIUS packets transmitted or received by HiPer ARC, all RADIUS authentication or accounting packets sent or received by HiPer ARC, a specific RADIUS user, the next session that starts up, or all RADIUS packets sent to or received from a specific server.

**Dynamic Slot
Assignment**

HiPer ARC supports dynamic slot assignment (DSA) in the Total Control Hub for static load balancing and hot-standby fault tolerance. DSA is an algorithm in the Network Management Card (NMC) which periodically polls chassis application cards for slots which support DSA. The NMC summarizes the information received and forwards that data to each HiPer ARC, and on the basis of that data, computes statically load-balanced slot assignments. New assignments are made every time a modem or application card is removed from, reboots, or is inserted into the Hub.

Also with idle mode rebalancing, modems are periodically rebalanced between application cards when no calls are up on the modem card.

HiPer ARC Applications

HiPer ARC is a multi-protocol, dial-up router and terminal server commonly described as a remote access server. The Hub performs four basic applications:

- IP Terminal Service
- Network Dial-in Access
- Dial-Out Access
- LAN-to-LAN Routing

Also, HiPer ARC provides many administrative tools for security including packet filtering, remote management, and a host of utilities for troubleshooting.

IP Terminal Service

HiPer ARC provides network access for dumb terminals or computers that emulate dumb terminals. So, remote terminals can log into an IP host on HiPer ARC's local network as if they were physically connected to it.

To do this, HiPer ARC receives TTY terminal output over a dial-up line. The ASCII data stream from these remote terminals is converted into a virtual terminal protocol (TELNET or Rlogin) and a session is established with a host to provide an IP terminal service connection on the Total Control Hub's local network. Since the connection is bi-directional, the terminal can also receive the host's responses.

HiPer ARC offers extensive access security, dialback, and substantial configurability for terminal service connections. See Figure 1 below.

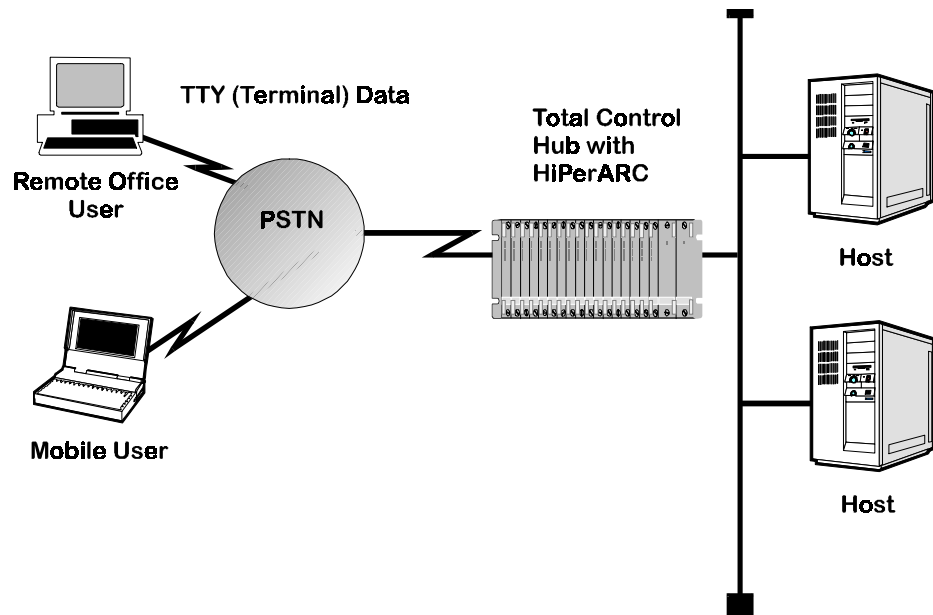


Figure 1-1 IP Terminal Service Topology

Network Dial In Access

HiPer ARC provides dial-in network access for remote users. Remote networked users can dial in and attach to the local network as if they were local nodes. These connections can be maintained continuously or established on an on-demand basis and disconnected when not needed.

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

- PPP (Point-to-Point Protocol)
- SLIP (Serial Line IP Protocol)

When received by HiPer ARC, the packets are forwarded from the remote user to the LAN and back again.

HiPer ARC offers access security, dialback, and substantial configurability for dial-in network connections. See Figure 2 below.

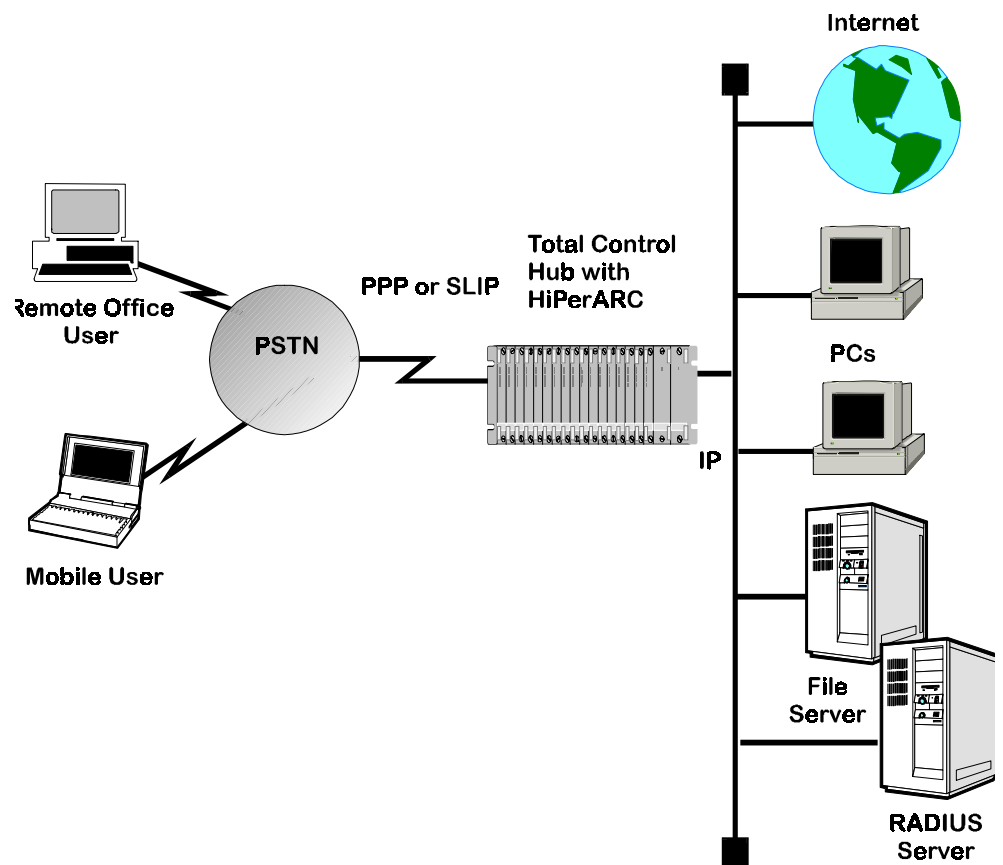


Figure 1-2 Network Dial In Topology

Dial-Out Access

Chassis ports (modems) can be accessed by PCs and workstations on a local IP network to provide dial-out service. HiPer ARC can also create pools of modems that can be used by local hosts on a first-come, first-serve basis.

To do this, HiPer ARC allows the host to establish a virtual terminal session with the modem. The host can then interact with the modem's command line and, from there, dial out.

On a UNIX host, a pseudo TTY driver can be installed that allows the host to interact with this virtual terminal connection as if it was actually a serial port. This makes the modem appear to be directly connected to the host.

Dial-out service allows network users to send faxes, connect to Bulletin Board Systems (BBS) or information services such as AOL, or access the Internet over a dial-up PPP connection. LAN users require a NCSI-compatible communications application to access Hub modems.

Consult *Chapter 6: Network Dial-Out Access*, for more information. See Figure 3 below.

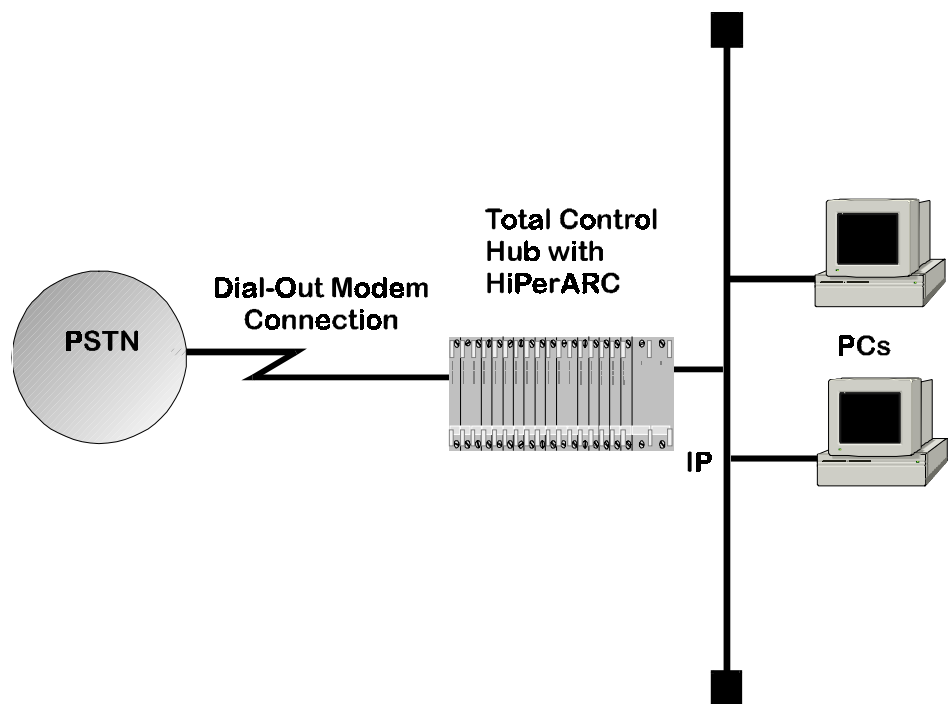


Figure 1-3 Dial-Out Topology

LAN-to-LAN Routing

HiPer ARC performs dial-up routing over a PPP connection between facilities (SLIP is not supported at this time). This occurs when one device dials up another and logs in as a user. See Figure 4 below.

Connections can be set up in a number of ways: manual, on-demand, timed, or continuous and connections configured to use various routing and protocol parameters. HiPer ARC is also capable of establishing additional connections to increase bandwidth automatically when traffic increases.

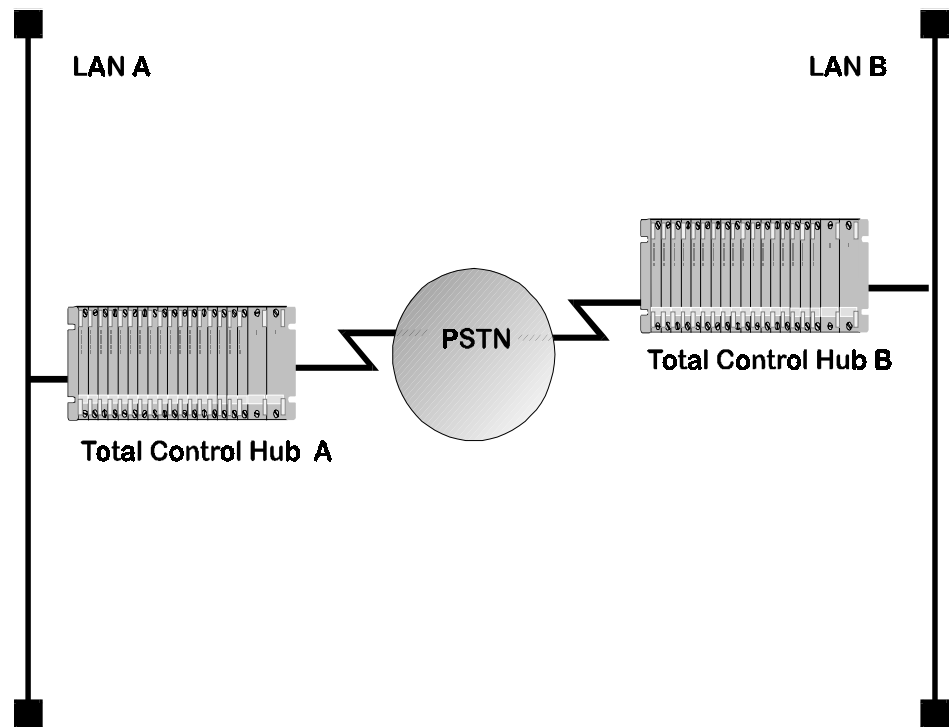


Figure 1-4 LAN-to-LAN Routing Topology

Packet Filtering

HiPer ARC supports IP packet filtering in both the inbound and the outbound directions of ports, users, and dial-out locations. Packet filter configuration is discussed in detail in *Chapter 9: Packet Filters*.

Administrative Utilities

HiPer ARC's command line includes an assortment of utilities for troubleshooting connections including:

- The ability to manually dial a location to test connectivity
- The ability to use TELNET, Rlogin or ClearTCP to establish a session with another host from HiPer ARC's command line.
- UNIX-like troubleshooting commands including *ping* and *traceroute* for debugging IP connections.

These commands are described in *Chapter 10: Administrative Tools* and *Chapter 11: Command Reference*.

Total Control Hub Overview

The Total Control Hub is designed to be a powerful data communications platform that can support a broad variety of applications. The applications that can be accommodated are governed by Network Application Cards (NACs) such as HiPer ARC and Network Interface Cards (NICs) that are installed in the chassis midplane.

NACs are intelligent data processors and routers, communicating over the midplane to provide a full-duplex connection with external networks. NICs provide the physical network interface.

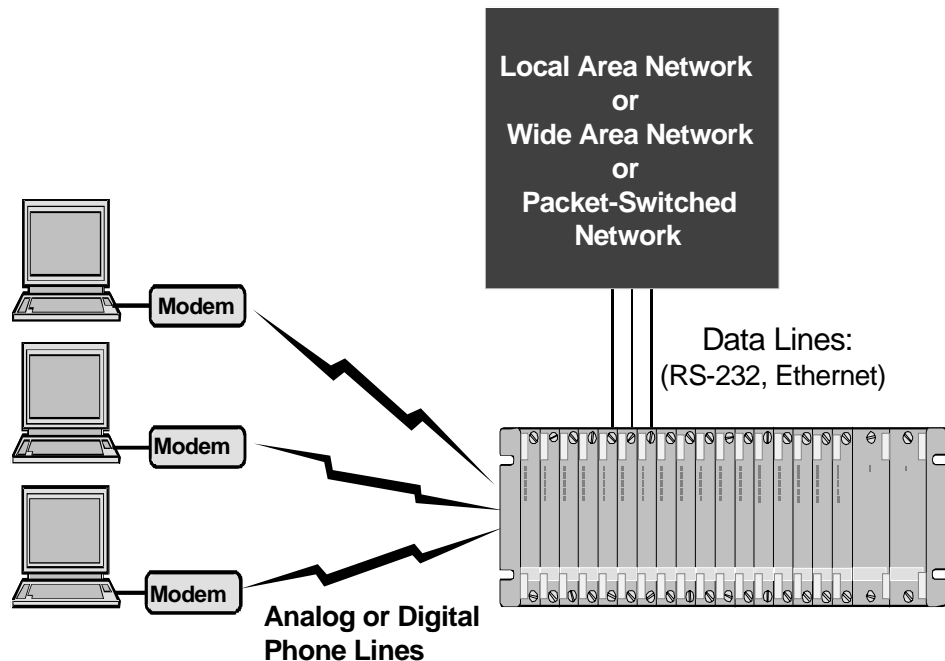


Figure 1-5 Total Control Hub Configuration

Figure 5 illustrates the capabilities of the Total Control Hub. This system provides modem management through the Total Control Manager/*SNMP* software and a Network Management Card (NMC). The NMC has a rear-mounted NIC, and must always occupy the right-most slot in the Total Control chassis (i.e., slot 17 in the Hub).

System Components

The basic configuration of a Hub consists of:

- One 19-inch chassis, or card cage, containing a high-speed, multi-layer midplane across the length of the chassis
- Up to 16 front-loaded Network Application Cards (NACs) including one or more HiPer ARCs, and their associated rear-loaded Network Interface Cards (NICs) including Quad or High Density Modem (HDM) cards
- One front-loaded NMC NAC, with its rear-loaded Network Interface Card (NMC NIC)
- One or two front-loaded Power Supply Units (PSUs); the second PSU available for redundancy
- Fan tray (required)

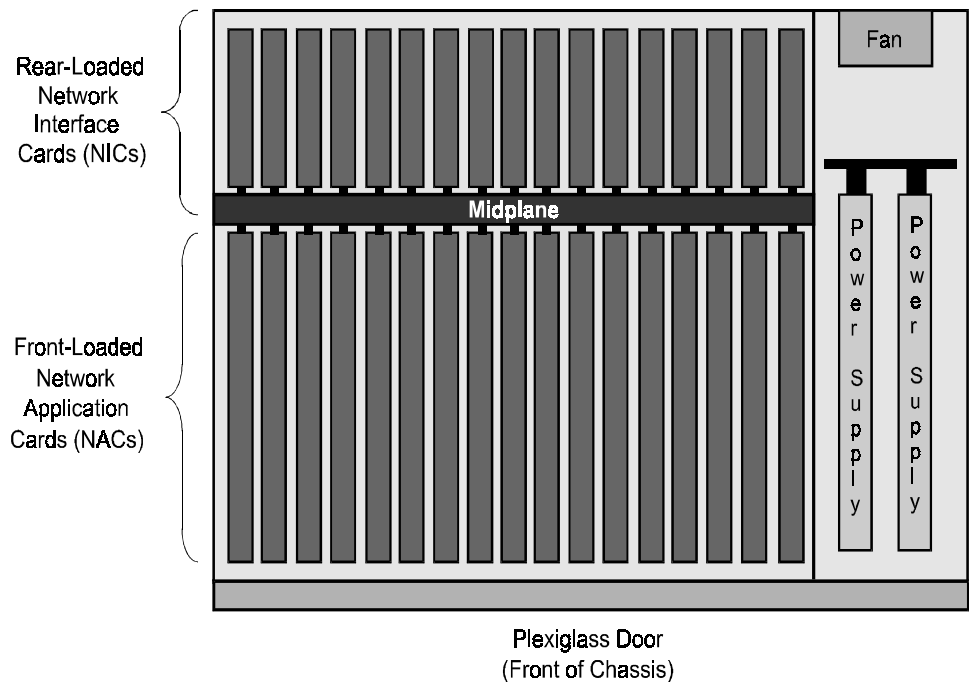


Figure 1-6 Total Control System (Top View)

Chassis Midplane

The heart of the Total Control chassis is its high-speed, multi-layer midplane, which spans the width and height of all card slots. The midplane provides seventeen connectors on the front for the NACs and the NMC, and an equal number of NIC connectors on the rear. The midplane provides multiple data buses that enable NACs to communicate with each other and the NMC.

Midplane Data Buses

Management Bus

The Management bus consists of the NAC Management bus and the NIC Management bus.

The NAC Management bus provides dedicated, full duplex, 512 Kbps serial channels that run from the NMC slot to each of the NAC slots. This lets the NMC configure installed cards, query status, issue commands, perform tests, and download software to the NACs.

The NIC Management bus provides a common serial channel from the NMC to each NIC, and an individual dedicated serial channel from each NIC to the NMC. This bus operates at 9600 bps and lets the NMC manage the network interface directly.

Packet Bus

The Packet bus, which allows inter-card communications between all NACs in the chassis, spans all but the last slot.

The NMC, located in slot 17 in the Hub/16 does not have access to the Packet bus. The Packet bus is a 10 MHz, 32-bit wide parallel bus that is used between packet-oriented devices.

The High Performance Access Router card's primary use of the packet bus is exchanging data with the Quad or High Density Modems NACs. To do this, HiPer ARC forms a virtual serial connection to each modem over the packet bus.

TDM Bus

The TDM (Time Division Multiplexed) bus carries traffic between circuit-switched devices, such as a T1 Card and a digital modem. The TDM bus consists of multiple TDM highways passing synchronous serial data, providing 64 Kbps time slots.

How HiPer ARC works with modems

Although HiPer ARC talks to the chassis modems over the packet bus, it interacts with them as serial devices. Virtual serial ports (modems), are created using the packet bus. This allows a quad modem NAC to be configured and used by the unit as if they were four ordinary serial modems attached to a serial port.

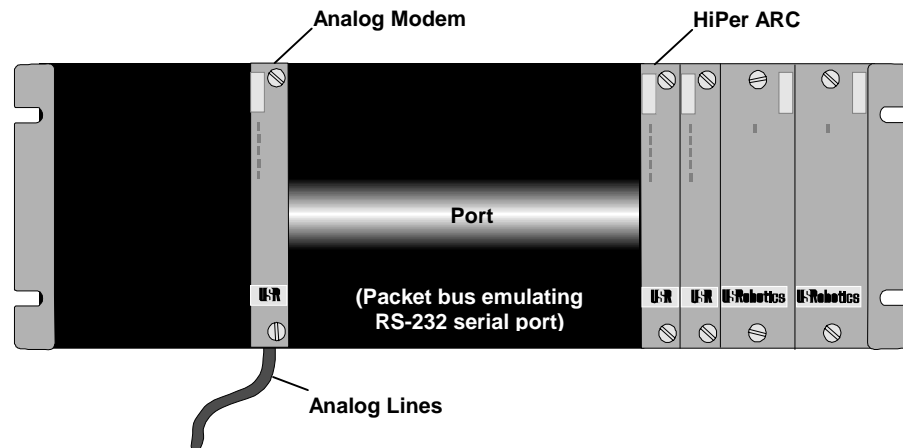


Figure 1-7 View of the chassis virtual ports routing through an Analog Quad Modem

When used with a T1 or E1 card, calls are routed through a Digital Quad Modem NAC rather than the analog Quad NAC shown in Figure 8.

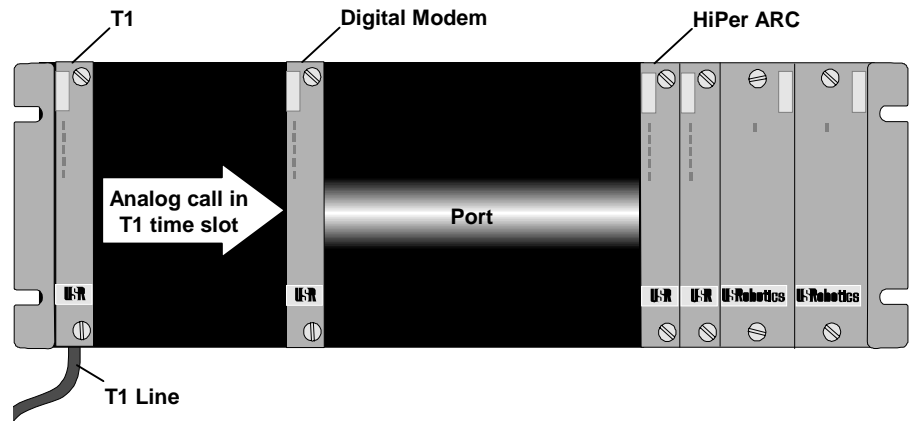
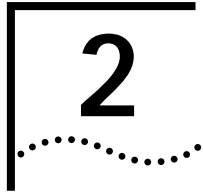


Figure 1-8 View of the chassis virtual port routing through a Digital Quad Modem

The configuration of these virtual ports determine what applications the attached modems can be used for. For example, virtual ports used for terminal service are configured as Login user ports.



HiPer ARC SETUP

This chapter describes what to do now that you are initially acquainted with HiPer ARC functionality. Read the following sections appropriate to your needs and skip the rest. The sections covered in this chapter are:

- System Administrator Requirements
- Accessing the Configuration Interface
- Command Line Interface Conventions
- Hardware Setup
- Security Configuration Advisory
- Configuring with Quick Setup
- Setting Up the System Manually
- Configuring a Manage User
- Manually Configuring the WAN Interface
- Configuring Static Routes
- Configuring Two HiPer ARCs on the Hub

System Administrator Requirements

This document assumes you're familiar with IP/IPX networks. TCP/IP information is available from a variety of sources, some of which are described below.

If you require the assistance of a qualified professional, consult your nearest authorized 3Com reseller for advice. For a service fee, 3Com also offers qualified engineering assistance on site. Contact *Product Support at (800) 231-8770 for more information.*

TCP/IP Reference Material

The network manager is typically responsible for devising an addressing strategy appropriate for the size and growth potential of the network. We recommend the following reference book for TCP/IP:

Comer, D.E., *Internetworking with TCP/IP Volume I: Principles, Protocols and Architecture*, Prentice-Hall, Englewood Cliffs, New Jersey, 1995.

You must obtain registered addresses from the Internet's Network Information Center (InterNIC) for IP machines and networks that will be attached to the Internet. InterNIC can be contacted at the following address and phone number.

Network Solutions
InterNIC Registration Services
505 Huntmar Park Drive
Herndon, VA 20170
1-703-742-4777

The InterNIC Website is: <http://ds.internic.net>

For networks with only a few IP machines, you may be able to contact your local Internet access provider and let them handle the details.

Accessing the Configuration Interface

This section explains how to attach to the configuration interface locally via the Console port. You may also do so remotely via the HiPer ARM (Access Router Manager), the Windows-based GUI provided in your package.

Establishing Communications with HiPer ARC

Depending on your type of computer, your terminal emulation communications settings should be set to:

- 115,000 baud
- 8 data bits
- no parity
- 1 stop bit
- direct connect

The Console port baud rate is configured on HiPer ARC via DIP switches. See *Appendix C: LEDs and Switches* for more detailed information. Also, be sure that a *null modem* is used to connect your PC with the HiPer ARC Console port and the cable has carrier capability.

IBM-PC Compatible Computers

Windows Terminal (included with Microsoft Windows) and Procomm Plus are popular communications packages which support VT100 terminal emulation for IBM-PC compatible computers. HyperTerminal, bundled with Windows 95, also supports terminal emulation.

UNIX-Based Computers

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

Automated Quick Setup Programs

As an alternative to manual configuration described in the manual, HiPer ARM offers two easy, automated configuration programs (see below) to quickly and efficiently get your unit up and running.

HiPer ARM Setup Wizard

A Setup Wizard is built into our Windows-based HARM, which can be accessed remotely (without hooking up the Console port) and does not require using the Command Line Interface (CLI). We recommend this program for its graphical user interface (GUI) and means of configuring your unit via SNMP.

Be aware that if you want to use HARM, you must *first* access the NMC or CLI and begin minimal configuration by adding an IP address and SNMP community for HiPer ARC before returning to HARM for additional system configuration. See the HARM/NMC documentation for easy setup.

Quick Setup (CLI)

HiPer ARC's automated *Quick Setup* program provides user-friendly configuration on the CLI. It performs simple setup of your entire system or selected functions. Simply answer the mostly yes or no queries and the program

does the rest. It is accessed automatically upon installing your hardware and turning on the Hub. If you prefer, you have the option to start configuration in Quick Setup and continue in HARM.



The Quick Setup program is designed for initial setup only. When setup is done, this one-time program will alter your configuration files, which Quick Setup cannot edit. So, if you make an error and need to restart, issue the **delete configuration** command to reboot and return to factory defaults.

Command Line Interface Conventions

The HiPer ARC CLI is an interactive, prompt line application that lets you view information and set system parameters. This section provides general information about CLI command conventions and usage.

Most commands are not case sensitive

You can type most commands and parameters in upper or lower case except for the *<name>* value which requires typing the correct case. The **kill** *<process name>* command is case sensitive though.

Many commands are position independent, multi-tiered and have keywords

Multi-tiered commands let you type the base command (e.g.: **set interface**) and implement associated parameters (*filter_access*, *input_filter*, 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.

You can abbreviate commands

Shorten most commands and command options by typing the first few letters that distinguish that command from any other. For example, while the full command is **list tcp connections**, type only type **li tc** to invoke it.



An error message displays if you type an ambiguous abbreviated command.

Double quotations distinguish text strings

Add white space or special characters to a string by wrapping it in double quotes.

Command syntax and CLI rules

This document uses the following CLI command syntax conventions:

- Keywords are in **bold** text. For example: **ping**
- Values following keywords are in *brackets*. For example: **[interval]**
- Values that are position dependent and do not have keywords are in *carets*. For example: **<ip_address>**. Some of these parameters are required and some are not. Required values are displayed in the CLI when querying a command (typing a question mark) or upon issuing a command where required values were omitted.

- *Position independent* arguments display vertically after the command, e.g.:

```
set dns
    domain_name <name>
    number_retries <1-5>
    timeout <5-125 seconds>
```

- A *vertical* character between parameters indicates a choice of options, e.g.:
<yes | no>
- A series of *commas* between a set of choices indicates multiple options, e.g.:
[login,network,callback,dial_out,manage,location]

Command completion

Finish spelling a unique, abbreviated command parameter by pressing the **TAB** key. It's helpful to speed up input or verify a command value.

For example, if you type **add ip n** and press **TAB**, command completion spells out the keyword **network** without losing your place in the command syntax. If the keyword is *not* unique, you will get an error message.

Command retrieval

Recall an earlier command by pressing **Ctrl p** or advance to the next command by pressing **Ctrl n**. Command retrieval consults the history of previous commands entered, defaulting to the last **10** commands. Change the depth of the buffer holding command history by issuing the **set command history** command. Issue the **history** command to view current depth and a list of your last issued CLI commands.

Command reprint

Redisplay what you typed before pressing the **ENTER** key by pressing **Ctrl I**.

Command Line Editing

Command line editing offers these options: **Ctrl b** or left arrow retreats one character; **Ctrl c** closes a CLI process; **Ctrl f** or right arrow advances one character; **ESC b** retreats one word; **Esc f** advances one word; **Ctrl a** advances to the beginning of a command; **Ctrl e** retreats to the end of a command, **Ctrl d** or **Ctrl k** deletes the selected character.

Paused (--More--) output display

When HiPer ARC outputs more information than your screen can accommodate, you can invoke a "more" pager for one more line or page of output or cancel the request. It works as follows. At the point on your screen where output breaks (-- More --), pressing:

- **ENTER** or **Ctrl m** - produces one more line of output
- **ESC** - produces one more page of output
- **q** or **Ctrl c** - cancels the output request

Two commands enable page breaks for commands which display long text output: **list**, **show**, et al. One command runs globally (for all HiPer ARC sessions) and the other locally (for the current session) They are:

```
enable command global_terminal_settings_page_breaks
enable command local_terminal_settings_page_breaks
```

- The following command varies the number of rows output to your screen:

```
set command global_terminal_settings_rows
```

Using general and positional help

HiPer ARC includes general and positional help to assist you in determining the proper command syntax.

For *general* help, type the following command:

```
help <any command>
```

A cursory list of associated commands and their proper syntax is provided.

Positional help is available when entering a command by typing a question mark (?) after the command. The CLI displays possible completions and returns the cursor to the point in the command before you entered the question mark.

First disable, then delete objects

Some *delete* commands require that you first *disable* the object or function. Deleting an IP network, for instance, first requires that it be *disabled*. But if you issue the **reconfigure ip network** command, HiPer ARC will automatically reconfigure network parameters of any established static IP LAN network. This command changes network parameters without you having to remove the router from service.

Saving changes

Save changes using the **save all** command. It is important to remember that most commands may be accepted when entered, but not necessarily *saved* across reboots until you use the **save all** command.

Running and stopping processes

HiPer ARC encompasses many standard processes. These processes are transparent to the user but administrators can run them issuing the **do** command, or end them using the **kill** <process name> command. This is useful for diagnostic or test purposes. Refer to *Chapter 10: Administrative Tools* for more information.

Using network services

The following network services are provided:

- *ClearTCPD* - a daemon enabling ClearTCP access to a modem group
- *SNMPD* - an SNMP agent utilizing the UDP protocol
- *TELNETD* - a TELNET daemon to access either the CLI or a modem group
- *TFTPD* - a TFTP daemon utilizing UDP on the server side of the network to access files
- *DialOut* - a supported PPP connection to an IP host

Using add and set commands

Issue **add** and **set** commands to set and change system parameters. These matched commands are functionally related, but also differ dramatically. Table entries such as user, interface, network, etc., require the **add** command to set initial parameters. Then use the **set** command to edit those parameters.

Using list and show commands

Issue **list** and **show** commands to view table entries or detailed table entries. The **list** command displays a list of table entries only, while the **show** command displays information about *a single line in a table* or a set of *scalars* (non-table items). The **show all** commands display all parameters for *all entries* in tables associated with particular commands.

Rebooting

In general, rebooting is rarely required but changing settings on the fly can sometimes cause inconsistent behavior in HiPer ARC. So, if you edit your configuration and want to ensure the changes are accepted, save your work using the **save all** command and issue the **reboot** command. A more flexible, feature-rich alternative employs the *Boot Configuration* menu to retrieve a configuration from FLASH memory or a network source as well as provides a host of other options.



Switching between RADIUS and TACACS+ requires a reboot.

Hardware Setup

Please consult the *HiPer ARC NAC Hardware Installation Guide* included in your package for hardware setup and configuration.

Security Configuration Advisory

HiPer ARC is configured with an administrative user named **adm** which has no password. This allows remote access via TELNET. To ensure security on your system, use the Command Line Interface to either:

- add a password to the **adm** user, or
- add a new administrative user and then disable **adm**



CAUTION: *If you intend to perform a NETServer to HiPer ARC upgrade, complete the upgrade first. The NETServer to HiPer ARC Upgrade program requires an **adm** user without a password.*

Password Protecting adm

To password protect **adm**:

- 1 Type the following text, making sure to fill in the desired password:

```
set user adm password <password_text>
```
- 2 Press **ENTER**.
- 3 Type:

```
save all
```
- 4 Press **ENTER**.

Adding a New Administrative User And Disabling adm

The alternative to password protection is to add a new user and then disable **adm**. However, be sure to add the new administrative user *first* and then disable **adm** only *after* you save the newly added user.

To add a new administrative user and disable **adm**:

- 1 Type the following text, making sure to fill in the desired user name and password:

```
add user <user_name> password <password_text> type login,manage
```

- 2 Press **ENTER**.

- 3 Type:

```
save all
```

- 4 Press **ENTER**.

- 5 Type:

```
delete user adm
```

- 6 Press **ENTER**.

- 7 Type:

```
save all
```

- 8 Press **ENTER**.

Using Quick Setup

If you're not performing a NETServer to HiPer ARC upgrade and you want to use the Quick Setup program, type the following.

```
_quicksetup
```

Then press **ENTER**.

For more information about Quick Setup, see *Chapter 2: HiPer ARC Setup*.

If you have any further questions, please contact the NETServer Trade Up Help Desk at **1 (800) 373-7367** or the email address **hiperarcupgrade@3com.com**.



WARNING: *in consideration of providing the password protection directions above, you are accepting the following disclaimer: 3com Corporation hereby disclaims and shall not be liable for damages of any kind, whether direct, indirect, special, consequential, or punitive, or for loss of revenue or profits, loss of business, loss of information or data, or other financial loss arising out of any event in which an unauthorized party accesses your system for any reason.*

Configuring with Quick Setup

If you've set up your hardware, you're ready to begin software configuration.

When using the CLI to configure your HiPer ARC, we recommend the *Quick Setup* program to get your unit up and running fast. This CLI program incorporates a Wizard to help you step by step through the process. A script of the Quick Setup follows - use it to jot down information you'll need to know.



If you do not want to use Quick Setup, skip to Setting Up the System Manually.

Power on the Total Control Hub.

In a few moments, after your screen has registered system initialization, it will load the bootrom and display the following message:

BOOT PROM Version 1.15 (Built on August 23rd, 1998 at 12:24:24)

For the following few seconds, new code can be downloaded but that is unnecessary at this point in first-time configuration. After HiPer ARC loads the kernel and enables several processes, this Boot Configuration menu appears:

```

HiPer Access Router Boot Configuration
1.      Boot mode                      :FLASH
2.      IP Configuration Source        :STATIC
3.      Boot IP Interface              :eth:1
4.      Boot IP Address                :149.112.217.148
5.      Boot IP Default Gateway        :149.112.217.254
6.      Boot IP Network Mask          :255.255.255.0
7.      TFTP Image on Startup          :NEVER
8.      TFTP Boot Server IP Address    :149.112.213.1
9.      TFTP Boot Image File Name      :ne040001.dmf
10.     Crash upload                   :DISABLED
11.     Crash Dump Upload Filename     :
12.     Manufacturing Diagnostics      :NONE
13.     Delete Router Configuration    :NO
14.     Delete Boot Configuration      :NO
15.     Command Line Parameters
E       Exit                          :
       Enter Choice                    [E]

```

These items let you configure parameters for system booting upon normal power up, after a system crash or to simply test the system - all unnecessary options at this point in first-time configuration.



For more information on the Boot Configuration Menu, see Chapter 10: Administrative Tools.

To proceed, you can type **Esc** and press **ENTER** or simply wait until the menu times out and the HiPer ARC prompt appears with the following screen - the actual Quick Setup script.



Underlined spaces have been added to the script to allow its use as a worksheet. Text in parentheses and italicized indicates a text annotation. If you are reading this section before actually configuring HiPer ARC, we recommend jotting down configuration information here before actually running the program to facilitate setup. Bracketed text [xxx] indicates the default value.

HiPer> Welcome to Quick Setup

The HiPer Quick Setup will let you set up simple configuration for your whole system or different portions of the system.

Do you want to continue with HiPer Quick Setup?____

There are two ways to proceed: You can set up only the basic configuration, which will allow you to continue with the Windows-based Access Router Manager. Or you can configure a simple configuration for IP and IPX.

Do you want to configure only enough to use the GUI based system [yes]? ____

*(If you pressed **yes** to the previous question, the script will continue with Quick Setup Identification information. If you pressed **no**, the script will continue with the next question below).*

Please answer the following questions with "yes" or "no" to indicate which portions of the system you want to configure.

When Quick Setup displays a question it will display a default answer in square brackets, like "[yes]". If you simply press enter, this is the answer that will be used for you.

Network management [yes]? ____

IP [yes]? ____

IPX [yes]? ____

Quick Setup Identification information

>>> Enter the name of your system []: _____

>>> Who is the system contact person []?_____

>>> Where is this system located []?_____

Quick Setup Management information

You can set up your system to require a user to log in via the console or leave it so that the console is always in command line mode.

>>> Do you want a log in required at the console [no]? ____



*(IMPORTANT: If you desire login at the console, after Quick Setup is completed, maintain system security by configuring an **idle timeout** for Console login. If you do not set this value, the console will remain connected until the first HiPer ARC reboot. The commands to issue following Quick Setup are:*

set command idle_timeout [1-60 minutes] ENTER

save all ENTER

If you do not require a console login, continue below.)

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no**, the script will continue with: "Do you want to be able to manage the system via SNMP...").*

You will need a user configured in order to log in at the console.

>>> What user name will be allowed to manage this system [administrator]? _____

>>> What password will be used for this user [administrator]? _____

>>> Do you want to be able to manage the system via SNMP [yes]? ____

*(If you pressed **yes** to the previous question, the script will continue below. If you pressed **no**, the script will continue with: "Do you want to allow command line management via TELNET ...").*

An SNMP community names a group of systems that can manage your system via SNMP. It is a rudimentary form of security.

>>> What SNMP community will manage this system [public]? _____

Along with a community name, you need to give the IP address of the system using that community. "0.0.0.0" means any system.

>>> What is the address of the management station [0.0.0.0]?_____

You also need to specify if this community can only read information, or read and write information.

>>>Can this community change management information [yes]?__

This completes the section on SNMP management configuration.

>>> Do you want to allow command line management via TELNET [yes]? __

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no** to the previous question, the script will continue with: "Do you want to set up the syslog daemon ...")*

>>> Do you want to set up the syslog daemon [no]? ____

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no**, the script will continue with: "Would you like to set up radius accounting ...").*

>>> What is the ip address of the syslog []? _____

What level of information do you want logged to the syslog?

It must be one of the following: "common", "unusual", "critical".

>>> What level of logging do you want [critical]? _____

>>> Would you like to set up radius accounting [yes]? ____

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no**, the script will continue with: "Would you like to set up radius authentication ...").*

>>> Enter the IP address of the primary radius accounting server []?_____

>>> Would you like to set up radius authentication [yes]?__

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no**, the script will continue with: "Would you like to use NMC chassis awareness ...").*

>>> Enter the IP address of the primary radius authentication server [n.n.n.n]?
__

>>> What is the shared secret with this server []? _____

>>> Would you like to use NMC chassis awareness [yes]? ____

Quick Setup IP information

IP configuration for LAN interface eth:1

The HiPer uses a network name to identify the network for future management commands.

>>> Enter the network name of your IP network [ip]: _____

>>> Enter the IP address []:_____

The IP mask can be specified as a class ("A", "B", or "C"), the number of one bits in the mask, or as an address in the format 255.x.x.x

>>> What should the mask be set to [C]? ____

You need to specify the framing for the IP network. It should be either "ethernet_ii" or "snap".

>>> What is the framing for the IP network [ethernet_ii]? ____

>>> Do you want to set up a default gateway [yes]? ____

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no**, the script will continue with: "Do you want to configure DNS for..." or "It is possible to restrict...").*

The default gateway gives the address of a router that the HiPer will forward packets to when it has no other route to their destination. It cannot be the same address as the IP address for the HiPer.

>>> Enter the IP address of the default gateway [] ? _____

The metric or "hop count" tells the HiPer how far the default router is from the HiPer.

>>> What metric should be applied to the default gateway [1]? ____

>>> Do you want to configure DNS for this HiPer [yes]?

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no**, the script will continue with: "Do you*

want to set up an address pool ..." or "You can either assign each user his or her own address ...").

>>> What is the address of the main DNS server for this HiPer []?_____

>>> What is the default DNS domain name for this HiPer [] ? _____

You can either assign each user his or her own address or you can set aside a pool of addresses for dynamic allocation.

>>>Do you want to set up an address pool [yes]? __

*(If you pressed **yes** to the previous question, the script will continue with the next question below. If you pressed **no**, the script will continue with: " It is possible to restrict access to the TFTP server ...").*

The address pool is a continuous range of addresses.

>>>Enter the name of your IP address pool [ippool]: _____

>>>What is the initial address in the pool []? _____

>>>How many addresses should be in the pool [16]? _____

It is possible to restrict access to the TFTP server to a specific system or a list of systems. Quick Setup will allow you to enter one system that is allowed or allow all systems access.

>>>Do you want to allow all systems to access the TFTP server [no]?_____

*(If you pressed **no** to the previous question, the script will continue with the next question below. If you pressed **yes**, the script will continue with: "IP setup is completed. Would you like to review.. "*

>>> From what IP address will you allow access to your TFTP network server []?_____

IP setup is completed.

Quick Setup IPX information

The network name is used by the HiPer to identify your IPX network.

>>> Enter the name of your network []: _____

The network number is a non-zero hexadecimal number of up to 8 digits.

>>> Enter the ipx network number []: _____

You need to specify the framing for the IPX network.

It should be one of the following: "ethernet_ii", "snap", "dsap", "novell_8023."

>>> What is the framing for the IPX network [ethernet_ii]? _____

You can either assign each user his or her own address or you can set aside a pool of addresses for dynamic allocation.

>>>Do you want to set up an address pool [yes]? __

*(If you pressed **yes** to the previous question, the script will continue below. If you pressed **no**, the script will continue with: "Would you like to review ...")*

The address pool is a continuous range of addresses.

>>>What is the initial address in the pool []? _____

>>>How many addresses should be in the pool []? _____

Would you like to review your current settings before executing [yes]? __

*(If you pressed **yes** to the previous question, the script will continue below. If you pressed **no**, the script will continue with: "Do you want to change any answers?")*

Identification Information:

System Name:_____

System Contact:_____

System Location:_____

Management Information:

Console Login:_____

User name:_____

Password:_____

SNMP Management:

SNMP Community:_____

SNMP IP Address:_____

SNMP Read & Write:_____

TELNET Management:

Syslog Daemon:

Syslog IP Address:_____

Syslog Level:_____

Radius Accounting:

IP Address:_____

Radius Authentication:

IP Address:_____

Radius Secret:_____

NMC chassis awareness:_____

IP Information:

IP configuration for interface eth:1

IP Network Name:_____

IP Network Address: _____

IP Mask: _____

IP Frame Type: _____

IP Def Gateway Addr: _____

IP Def Gateway Metric: _____

DNS Server Information:

DNS Server Address: _____

DNS Server Domain Name: _____

IP address pool: _____

IP pool address: _____

IP pool size: _____

IP WAN Information:

TFTP Client Information:

TFTP Access: _____

IPX Information:

IP configuration for interface eth:1

IPX Network Name: _____

IPX Network Number: _____

IPX Frame Type: _____

IPX address pool: _____

IPX pool address: _____

IPX pool size: _____

Do you want to change any answers [no] ____

*((If you pressed **no** to the previous question, the script will continue below. If you elected to change an answer by pressing **yes**, Quick Setup will prompt you section by section for new entries and ask you once again to review current sessions before executing.))*

Do you want to actually execute these commands [yes]? ____

Setting Up the System Manually

This section describes how to manually set up your HiPer ARC with minimum configuration. If you want to use our Windows-based GUI, refer to the on-line *HiPer ARM* documentation for instructions.

Power On

To begin manual configuration:

- 1 Power on the unit. After a few moments, when your screen has registered system initialization, loaded the kernel and enabled a number of processes, the *Boot Configuration* menu appears (see description on page 2-22). For the following few seconds, new code can be downloaded but that is unnecessary at this point in first-time configuration. After HiPer ARC loads the kernel and

enables several processes, this Boot Configuration menu appears:). Type the following:

15 ENTER

- 2 The **Hiper>>** prompt appears. When prompted by the Quick Setup Program to continue, type: **no**

System Basic Setup

- 1 Name your HiPer ARC and specify additional system information. The name you enter serves as the HiPer ARC's DNS name and SNMP system name. It will also be the name that the HiPer ARC advertises in SAP broadcasts.

The name must be *unique* - no other device on your network can share it. You should also indicate the following information:

- *location* - where the HiPer ARC actually resides
- *contact* - the person to contact about HiPer ARC issues

Use the following command:

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

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

```
set system name "total control" location "boston" contact "Keyser Sosay @ 508 123-4567
666x" ENTER
```

Or type:

```
set system name "total control" ENTER
set system location "boston" ENTER
set system contact "Keyser Sosay @ 508 123-4567 666x" ENTER
```

- 2 Verify the previous configuration by typing::
- 3 *Optional.* Set the system Greenwich Mean Time (GMT) *date* and *time* using this command:

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

For example:

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

- 4 Verify the previous configuration by typing::

```
show date
show time
```

- 5 Save your work by typing

```
save all ENTER
```

IP Configuration

This section describes how to manually configure the HiPer LAN interface (eth:1/eth:2) for IP networks.

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

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

The first four octets describe the IP station address, followed by the subnet mask (contiguous) designator. You can specify the subnet by class, numerical designation or in the IP address format. If you specify a Class C mask, for example, this command will generate a 255.255.255.0 subnet value for you. If you specify the number of 1 bits in the mask, the acceptable range is 8-30 (32 if a host). For help counting the bits, see *Appendix C: Addressing Schemes* for a handy bitmask table.

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

Enter IP network information. Type:

```
add ip network <network name>
      interface [eth:1 or eth:2]
      address <station address/mask>
      frame [ethernet_ii | snap]
```

For example:

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

A numerical mask example:

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

- 2 Verify the previous configuration by typing:

```
show ip network backbone
```



Check the connection by using the **ping** <ip address> command. See Chapter 10: Command Reference for more information.

- 3 Configure an IP address pool of contiguous network addresses for allocation to dialin hosts. This command limits RIP traffic by aggregating users within a single advertised address. Set an *initial_pool_address*, overall *size* of the pool, and *public* or *private* pool membership. Use this command:

```
add ip pool
      initial_pool_address <ip_address/subnet mask>
      route <aggregate | no_aggregate>
      size <1-4096>
      state <public | private>
```

For example:

```
add ip pool homelan initial_ip_address192.75.202.99/c route aggregate size 150 state private ENTER
```

- 4 Verify the previous configuration by typing:

```
list ip pools
```

- 5 Set a *default gateway*. Default gateways must be on the same subnet as a configured interface.

You also need to supply a metric (hop count) for each type of default gateway. Possible values range from 1 (default) to 15. Note that since the actual metric of a default gateway is only 1 hop, the value entered here is used to control the perceived cost of the gateway to other routers on your network.

For example, a high metric will limit the number of hops that the route is broadcast and may cause other routers to see it as a less preferable route.

To add the default gateway, use the following command:

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

For example:

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

- 6 Verify the previous configuration by typing:

```
list ip defaultroute
```

- 7 Save your work by typing

```
save all ENTER
```

IPX Configuration

To configure HiPer ARC's LAN interface on an IPX network, you must:

- Determine the IPX network number
- Set HiPer ARC IPX parameters



Important: Even if your network uses only IPX, you must still set up an IP address for HiPer ARC if you want to use our NMC or HARM application later.

Determining the IPX Network Number

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

For File Servers Running Novell Version 3.xx

- 1 Go to a console of a file server on the same network segment as HiPer ARC.
- 2 From the Novell Console program press **Ctrl Esc**, then **Esc**, until the : (colon) prompt appears. Select **System Console** and press **ENTER**.
- 3 Type the following:

config **ENTER**

A display similar to the one shown below appears:

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

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

- 4 Jot down the LAN protocol IPX network number for the frame type you require.

For File Servers Running Novell Version 2.xx

- 1 Go to the console of a file server on the same network segment as HiPer ARC.
- 2 Press **Ctrl Esc** until the : (colon) prompt appears and type the following:

config **ENTER**

A display similar to the one shown below appears:

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

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

- 3 Jot down the network address for the frame type you require.

Setting IPX Parameters

To configure HiPer ARC's LAN interface for an IPX network:

- 1 Specify *IPX network* information including the network *name*, *address*, *interface* and *frame* type of the network segment connected to HiPer ARC's LAN port. Note that the same physical network segment will have a different network number for each frame type used. Be sure to enter the network number associated with the chosen frame type. Use the following command:

```
add ipx network <network name>
                address [ipx address]
                interface [eth:1 | eth:2]
                frame [ethernet_ii | snap | dsap | novell_8023]
```

For example (abbr.):

```
add ipx net segment2 add 00000576 int eth:1 fra ethernet_ii ENTER
```



Omit preceding zeros: HiPer ARC accepts "576" as the correct network number.

- 2 Verify the previous configuration by typing:

```
show ipx network segment2
```

- 3 Set the IPX default gateway with the format *xxxxxxx.xx:xx:xx:xx:xx:xx* where *xxxxxxx* is the IPX network address and *xx:xx:xx:xx:xx:xx* is a MAC address.

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

For example:

```
set ipx system default_gateway 011:11:11:01:11:00:11 ENTER
```

- 4 Verify the previous configuration by typing:

```
list ipx routes
```

- 5 Save your work by typing:

```
save all ENTER
```

DNS Configuration - Optional

This section sets a Domain Name Server (DNS). If you do not wish to use DNS, skip to SNMP Configuration.

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

Also, name up to 10 DNS servers using the command below and specify the order (*preference*) you prefer they be chosen (highest priority: 1).



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

Use the following command:

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

For example:

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



*The DNS server is only consulted to resolve host names not found in the Hosts Table. If you are using a name service, the Hosts Table may be left empty. Use the **resolve name** or **host** command to learn DNS host names or numbers.*

- 2 Verify the previous configuration by typing:

```
list dns servers
```

- 3 Specify the *default domain* - the Ethernet segment where your system resides and where you are defaulted should you forget to name the DNS server. Adding this entry to the Hosts Table avoids having to always specify the domain. Type:

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

For example:

```
set dns domain_name usr.com ENTER
```

- 4 Verify the previous configuration by typing:

```
show dns
```

- 5 Save your work by typing:

```
save all ENTER
```

SNMP Configuration - Optional

The following section configures SNMP service. If you do not wish to set up SNMP, skip to *Save Your Work*.

If you plan to use an SNMP application to configure and manage the HiPer ARC, you must specify *SNMP community* values. SNMP community names segregate administrative management groups and should match the community settings of your generic SNMP software. You must set the following:

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



For a public community with read-only privileges, assign the address to any station (0.0.0.0). Read/write and administrator privileges are also available.

- 1 Add the SNMP community values. Type:

```
add snmp community <name>
address <IP address>
access [ro | rw | adm]
```

For example (abbr.):

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



Abbreviate command keywords provided they are unique to the command.

- 2 Verify the previous configuration by typing:

```
list snmp communities
```

- 3 Save your work by typing:

```
save all ENTER
```

Configuring a Manage User

This section describes how to create an administrative user with *manage* privileges to configure HiPer ARC at the CLI via a direct login to the system through the Console port or eventually via a TELNET session. You can add a remote login user, or, if you prefer to dial in, add a manage user locally through the Console port now, but you can not do so via TELNET at this point in set up.



Important: Only manage users can access the CLI.

- 1 Create a manage user. You have these options:

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

```
add user <user_name>
network_service [ppp | slip]
password [password]
type [login,network,callback,dial_out,manage]
```



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

Network example with a password:

```
add user predator type manage,network password arnold ENTER
```

Login example without a password:

```
add user predator type manage,login password arnold ENTER
```

- 2 Verify the previous configuration by typing:

```
show user predator
```

- 3 Save your work.

```
save all ENTER
```


Manually Configuring the WAN Interface

Protocols are set up over the WAN by creating and editing a *user profile*. A user profile specifies the call type, protocols, addresses, and bandwidth management parameters that determine how you connect and communicate to that user (remote site) over the WAN. User profiles are detailed in chapters 4 - 8.

When you save user profiles you've just created, you're finished configuring the HiPer ARC side of the link. Configuration of the router on the remote side of the link will vary with your product, but set up will include the local IP address. See your product manual for more information.

Configuring Static Routes

HiPer ARC provides the ability to dynamically learn remote IP routes via the IP RIP protocol. HiPer ARC also offers the option of configuring a static route when you know the destination you want to connect with. The **add ip route** or **add ipx route** commands set the destination's *IP/IPX address*, the gateway used to access the remote destination, and a metric value or distance in hops to reach the destination from HiPer ARC.

IP Routes

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

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

The IP address of the remote destination is written in the format *nnn.nnn.nnn.nnn*, entered with or without a mask specifier. The mask specifier can be designated either 'A', 'B', 'C', or 'H' (host), or with a numeric value from 8 to 30 (32 if a host) that describes the number of one bits in the mask. You can also specify the netmask in the *xxx.xxx.xxx.xxx* format. If you do not specify a mask, the system will generate it (based on the network address) for all routes (ip_net_addresses) except host routes, for which you must specify a mask. For help counting the bits, see *Appendix C: Addressing Schemes* for a bitmask table.

For example:

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

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



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

IPX Routes

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

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

The *IPX network address* of the remote destination is written in the hexadecimal format *xxxxxxx* where addresses *ffffff* or *ffffffe* are invalid.

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

For example:

```
add ipx route ffff111 gateway ffff101.ff:ff:ff:00:00:ff metric 1 ticks 1 ENTER
```

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



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

Configuring Two HiPer ARCs on the Hub

Administrators concerned with enhancing the performance of their Total Control Hub may want to install two or more HiPer ARCs in their chassis. Using more than one HiPer ARC lowers latency rates by applying plenty of CPU processing power to calls received and relegates fewer calls per card. It also guarantees redundancy should one HiPer ARC card fail, and, if the Hub is employed as a router, ensures that performance will not degrade significantly as LAN traffic increases.

In order to properly configure more than one HiPer ARC on the Hub, *statically* configure your installed modem cards by setting their card type ownership or *dynamically* configure the cards using Dynamic Slot Assignment (DSA). A third method employs DSA rebalancing which periodically reassigns slot ownership by the Network Management Card (NMC).

With one HiPer ARC installed, modem and other NACs in the Hub normally are set dynamically by the device discovery ability (Chassis Awareness) of the NMC which automatically determines the card type. If your Hub has the NMC installed, we recommend you configure only the owner parameter for each HiPer ARC and allow the NMC to configure the system as necessary.

Slot Configuration Test Cases

To configure more than one HiPer ARC, use this command on each HiPer ARC:

```
set chassis slot <1-16>
  card_type <empty | hdm_24 | hdm_30 | quad_i_modem | quad_modem>
  owner <no | yes>
  ports <1-30>
```

If your Hub does not have an NMC installed, and you want to statically configure slots, you must specify all values configured by the **set chassis slot** command. If your Hub has the NMC installed, you need only specify slot and owner parameters for static configuration - the NMC will do the rest.

Example 1

In the example below, if an NMC is installed, set the owner value for the modem cards on each HiPer ARC:

HiPer A:

```
set chassis slot 1,3,5,7,9,11,13,15 owner yes ENTER
set chassis slot 2,4,6,8,10,12,14,16 owner no ENTER
```

HiPer B:

```
set chassis slot 1,3,5,7,9,11,13,15 owner no ENTER
set chassis slot 2,4,6,8,10,12,14,16 owner yes ENTER
```

Issue the following command to verify your previous configuration:

```
list chassis
```

The first two commands above allow the NMC to configure owned Hub slots and prevents configuration of non-owned Hub slots. In other words, HiPer ARC A owns the odd slots and HiPer ARC B owns the even slots. Be careful not to configure conflicting owned/non-owned slot values.



IMPORTANT: Non-owned slots (owner no) are considered off-line by both HiPer ARCs and their modems non-functional by NMC. any modems.

Example 2

In the next example, configure two HiPer ARCs with all ports statically set, without an NMC installed. Be sure to turn off chassis awareness. Type:

HiPer A:

```
set chassis slot 1-8 card_type hdm_30 owner yes ports 30 ENTER
set chassis slot 9-16 card_type hdm_30 owner no ports 30 ENTER
disable nmc chassis_awareness
```

HiPer B:

```
set chassis slot 9-16 card_type hdm_30 owner yes ports 30 ENTER
set chassis slot 1-8 card_type hdm_30 owner no ports 30 ENTER
disable nmc chassis_awareness
```

Issue the following command to verify your previous configuration:

```
list chassis
```

The first two commands above assign ownership of all 30 modems in each of the first 8 HDM cards to one HiPer ARC and all 30 modems on each of the next 8 HDM cards to the second HiPer ARC in the Hub. To support load balancing, we recommend you statically configure half of your modem ports per HiPer ARC installed. If you have a mix of different card types in the Hub, you should assign ownership so that the total number of ports are owned equally by HiPer ARCs.

Example 3

In the example below, set the same configuration as above but with the NMC installed. Chassis awareness is *enabled* by default. Also, be sure that enough IP/IPX addresses are configured in the address pool (**add ip/ipx pool** command) to handle traffic for the entire chassis. Type:

HiPer A:

```
set chassis slot 1-8 owner yes ENTER
set chassis slot 9-16 owner no ENTER
enable nmc dynamic_slot_assignment
```

HiPer B:

```
set chassis slot 9-16 owner yes ENTER
set chassis slot 1-8 owner no ENTER
enable nmc dynamic_slot_assignment
```

The commands above illustrate how the NMC can recognize the card type and port numbers without you having to specify them.

Example 4

In the example below, to configure one HiPer ARC with half the slots configured statically and the other HiPer ARC with half the slots configured dynamically, type:

```
HiPer A:          set chassis slot 1-8 card_type hdm_24 owner yes ports 30 ENTER

HiPer B:          set chassis slot 9-16 owner yes ENTER
```

Example 5

Another scenario involves installing one HiPer ARC to handle all modems statically and having the other HiPer ARC, a manual “warm spare,” on hand in case the first HiPer ARC fails. This option avoids a single point of failure and extensive down time for a heavily used Hub. Load rebalancing should *not* be used when configuring a hot standby. Type:

```
HiPer A:          set chassis slot 1-14 card_type hdm_24 ports 24 owner yes ENTER

HiPer B:          set chassis slot 1-14 card_type hdm_24 ports 24 owner no ENTER
```

If the HiPer ARC which currently owns the modem cards fails, type:

```
HiPer A:          set chassis slot 1-14 card_type hdm_24 ports 24 owner yes ENTER

or

HiPer B:          set chassis slot 1-14 owner yes ENTER
```

Example 6

The following scenario sets the same configuration as above but turns on DSA and turns off Idle Rebalancing. Type:

```
HiPer A:          set chassis slot 1-14 card_type hdm_24 ports 24 owner yes ENTER
                   disable nmc dsa_idle_rebalancing

HiPer B:          set chassis slot 1-14 card_type hdm_24 ports 24 owner no ENTER
                   enable nmc dynamic_slot_assignment
                   disable nmc dsa_idle_rebalancing
```

If the HiPer ARC which currently owns the modem cards fails, type:

```
HiPer A:          set chassis slot 1-14 card_type hdm_24 ports 24 owner yes ENTER

or

HiPer B:          set chassis slot 1-14 owner yes ENTER
```

Viewing Chassis Parameters

Use the following command to verify your dynamic and static slot settings, as well as card types and port numbers on the Hub. Type:

```
list chassis ENTER
```

The command lists:

Slot	Owner	Description	Ports	Type
1	NO	--EMPTY--	0	STATIC
2	NO	--EMPTY--	0	STATIC
3	YES	Quad Anal-Digi V.34 Modem	4	DYNAMIC
4	NO	--EMPTY--	0	STATIC
5	NO	--EMPTY--	0	STATIC
6	NO	--EMPTY--	0	STATIC
7	NO	--EMPTY--	0	STATIC
8	NO	--EMPTY--	0	STATIC
9	NO	--EMPTY--	0	STATIC
10	NO	--EMPTY--	0	STATIC
11	NO	--EMPTY--	0	STATIC
12	NO	--EMPTY--	0	STATIC
13	NO	--EMPTY--	0	STATIC
14	NO	--EMPTY--	0	STATIC
15	NO	--EMPTY--	0	STATIC
16	YES	HiPer Access Router NAC	0	DYNAMIC

PPP Compression Options

PPP compression on HiPer ARC presents throughput concerns in the case of a Hub supporting mostly ISDN traffic. PPP compression could seriously affect latency if enabled in this circumstance. In response, administrators should turn off ppp compression for digital packets - HiPer ARC compresses digital and uncompressed analog packets by default - and add a second HiPer ARC for enhanced performance. Use the following command to turn off all PPP compression for all call types:

```
set ppp ccp_modemtype_accept none ENTER
```

Or, to enable PPP compression only for analog calls with modem compression:

```
set ppp ccp_modemtype_accept compressed_analog ENTER
```

Viewing Compression Settings

Use the command below to verify the type of packet compression you want HiPer ARC to perform. Type:

```
show ppp settings ENTER
```

For example:

```

PPP AUTHENTICATION
DIAL_IN Users Authenticate PAP or CHAP:  EITHER
PPP Authentication Preference:           DEFAULT
System Transmit Authentication Name:     HiPer

PPP offloading                           ENABLED

```

CCP will be attempted for call type(s):	DIGITAL UNCOMPRESSED_ANALOG
Primary NBNS Server address:	0.0.0.0
Secondary NBNS Server address:	0.0.0.0
DNS configuration Usage:	SYSTEM
Primary PPP DNS Server address:	0.0.0.0
Secondary PPP DNS Server address:	0.0.0.0
PPP session start message:	PPP session from %server_ip to % client_ip beginning....

3

CONFIGURATION OVERVIEW

HiPer ARC and related components are Simple Network Management Protocol (SNMP) manageable by HiPer ARM or HiPer ARC via a TELNET connection. The parameters you set through these interfaces are stored in a number of tables that reside in the card's FLASH memory.

This chapter includes the following sections:

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

Setting Up Applications

The CLI allows you to perform four basic applications. Refer to the appropriate chapter for more information:

- IP terminal service (see Chapter 4)
- Network dial-in access (see Chapter 5)
- Dial-out access (see Chapter 6)
- LAN-to-LAN routing (see Chapter 7)

Configuration Command Overview

Configuration data is stored in several tables (User and Interface tables, e.g.). You can change most parameters in these tables using the generic **set** command:

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

For example:

```
set user maximillian message "Mexico is Mine" ENTER
```

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

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

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

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


You can view current configuration information with either the **show**, **list** or **show all** commands. List commands display table entries, show commands display information about a specific table or non-table entry. For example:

```
show network backbone ENTER
```

```
show user John ENTER
```

```
list networks ENTER
```

```
list services ENTER
```

```
list users ENTER
```

For a complete list of commands and options see *Chapter 10: Command Reference*. Also, you can access the on-line **help** command by typing:

```
help <command> ENTER
```

Configurable Table Overview

This section briefly describes some important internal databases, or tables, which contain configuration information accessed by **list** <keyword> commands. Not *all* HiPer ARC tables are detailed.

Interface Tables

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

User Table

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

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



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

Local and Login Hosts Tables

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

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

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

Initialization Script and Global Host Tables

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

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

Facility Level Table

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

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

Module Table

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

IP Network Table

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

IP Address Pool Table

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

IP Interface Block Table

This table contains IP addresses associated with each system interface. Interfaces with point-to-point connections show the neighbor field with the address of the remote system.

Forwarding and IP Routing Tables

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

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

SNMP Configuration Tables

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

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

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

The *SNMP Community and Trap Community Pool* tables save names and addresses of communities as associated pools.

SYSLOG Table

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

Event Critical Messages Table

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

Filter and Associated Tables

Filter file names of filters you create are stored in the *Filter Table* but the filters themselves are stored as ASCII text in FLASH memory. The *Access Filter Table* determines whether user filters take precedence over interface filters.

File Table

This table contains system files and other files you may have loaded in HiPer ARC including filter files.

Network Services and Available Servers Tables

The *Network Services* and *Available Servers* tables hold information related to HiPer ARC-supported network services such as TELNET, SNMP, ClearTCP, DialOut and TFTP. These default services can be edited or new services created with the **add** and **set network services** commands.

Dial-Out Port Table

This table lists virtual ports available for NCSI dial-out service.

UDP Listeners Table

This table details User Datagram Protocol (UDP) ports being used by HiPer ARC. These ports correspond to processes which are receiving UDP data (for example SNMP, User Management, TFTP service).

TCP Connections Table

The *TCP Connections Table* contains information regarding all system and user-created TCP links.

DNS and Associated Tables

The Domain Network Service tables in HiPer ARC contain resource records about address resolution. The tables include the: *DNS Host Table*, *DNS Server Table*, *DNS Cache* and *Negative Cache* tables, and *Resolve Cache* and *Negative Cache* tables.

TFTP Access Table

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

Traceroute and Traceroute Hop Tables

The *Traceroute* and *Traceroute Hop* tables contain routes that data packets take from their source to a specified destination on the network and the interval to reach each hop and return. Traceroute utilizes the ICMP protocol to monitor network messages and the UDP protocol to transmit packets.

Remote Ping and Ping Busy Out Tables	These tables contain a host of information regarding ICMP entries for local and remote ping requests. Entries are added to the <i>Remote Ping Table</i> using the ping command while the list ping service_loss_systems command displays resource records of connected systems stored in the <i>Ping Busy Out Table</i> .
Address Translation Table	This table contains the network address to physical address equivalences resolved by ARP.
Chassis and Packet Bus Tables	These tables contain hardware and software information about NIC and NAC cards stored in Hub slots.
CIP Port Parameter Table	This <i>Call Information Process (CIP) Table</i> contains information regarding current connections on HiPer ARC derived from the list connections command.
User Manager Active Sessions Table	This table contains protocol and other information regarding current network or login sessions.
Chat Script Table	The <i>Chat Script Table</i> contains chat script files created to handle dialin users using the add chat_script command.
Modem Tables	More than a dozen modem tables contain entries for <i>Data Compression</i> , <i>Call Control</i> , <i>Error Correction</i> , <i>Call Statistics</i> , and <i>Signal Conversion</i> , among others. These tables are associated with the add modem_group command.
PPP Tables	Several PPP tables contain entries regarding PPP connections on HiPer ARC. These include: <ul style="list-style-type: none">■ PPP Link Table■ PPP Authentication Table■ PPP Bundle Table■ PPP IP Table■ PPP Compression Table■ AAA Table

Remote User Overview

Remote users dial in to establish a terminal session with a host on a local network using a login service such as TELNET, Rlogin or ClearTCP. See Figure 1.

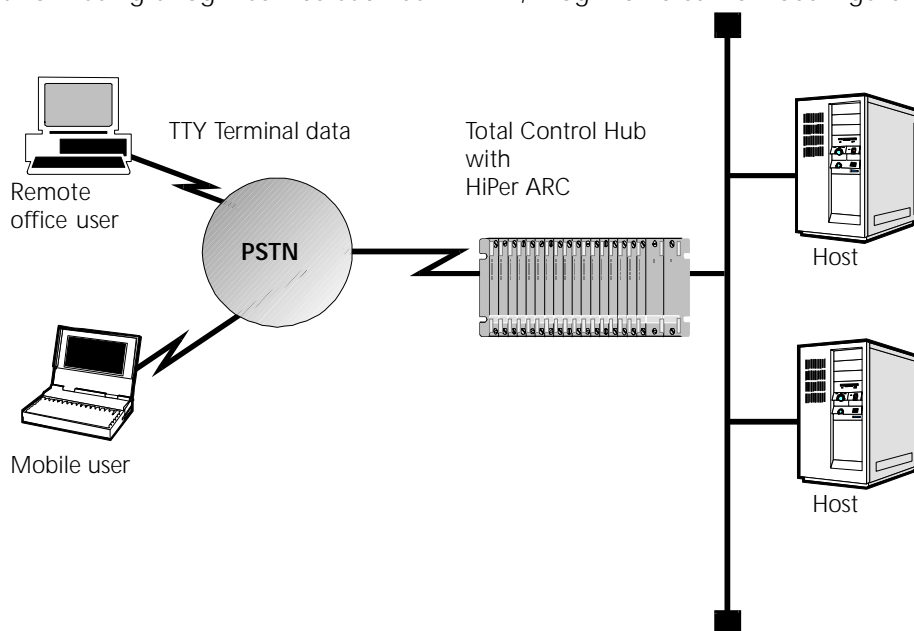


Figure 4-1 IP Terminal Server Topology

Configuring the Remote Computer

Remote terminal users are known as login users. The system administrator should provide the remote login user with the following information:

- A user name
- A telephone number
- Login host address or name



HiPer ARC does not require passwords to be supplied by the user. For more security, add a password.

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

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



These settings are the defaults. If you change communications settings, you must provide the remote user with the appropriate settings as well. See Chapter 11: Command Reference for more data.

Configuring Login Hosts

For a login host to be available to a login user, you must define it in the Login Hosts Table. This table contains the host name, address, selection preference, and login service port for each login host.



To allow the user to access a login host using a host name, you must first configure a DNS server using the **add dns server** command. For example:

```
add dns server 7.7.7.7 name boston preference 1 ENTER
```

To set up login host table entries, perform the following steps:

- 1 Configure Login Hosts. You may add up to 10 hosts to support your login users. Use this command:

```
add login_host <host_name>
address <ip_address>
preference <number>
rlogin_port <TCP_port_number>
telnet_port <TCP_port_number>
clearTCP_port <TCP_port_number>
```

Host Name

Name of the login host.

Address

Optional. The IP address of the login host. If you do not specify an address, HiPer ARC consults the DNS server to resolve the address.

Preference

Priority ranking for the login host, from 1 (highest) to 10. The preference number must be *unique* for each host entry.

Rlogin, TELNET and ClearTCP Ports

Optional. The Rlogin, TELNET and ClearTCP port numbers of the host.

To add a login host, type:

```
add login_host detroit address 236.135.221.167 preference 1 ENTER
```

- 2 Check Your Work. Check your host entries using the following command:

```
list login_hosts ENTER
```

For example:

LOGIN HOSTS					
Preference	Name	Rlogin Port	Telnet Port	Clear Port	Top Host Address
1	detroit	513	23	0	236.135.221.167
2	collander	513	23	0	236.135.220.179
3	zebra	513	23	0	236.135.222.157

- 3 Save Your Work. Use the following command:

```
save all ENTER
```

Configuring Login Users

Remote login users can use login services such as TELNET, Rlogin, or ClearTCP by dialing into HiPer ARC. Login users can connect directly, or be configured as callback users, meaning the Hub will call the user back at a phone number specified in the user profile. You can set up the user for a specific login service to access a specific login host, or you can let the user determine the login service and login host.



You can also specify login user information in RADIUS. When RADIUS authenticates a user, it can pass on user configuration information to HiPer ARC. For more information, refer to Appendix E: RADIUS and TACACS+ Systems.

To configure a login user:

- 1 Add the User. Use the following command:

```
add user <name>
      password [password]
      login_service [rlogin | telnet | cleartcp]
      type [login | network | callback]
```

Password

Passwords are *optional*.

Login Service

Specifies the default login service. The default is TELNET. This parameter can be one of the following:

- **TELNET** - Offered by most TCP/IP computers, TELNET lets users login to supporting hosts.



You should run RIP when setting up a global IP network if you intend to support TCP services such as TELNET, rlogin and ClearTCP. Without RIP on the local network, you will not learn of remote networks should the Ethernet interface be disabled.

- **Rlogin** - Although Rlogin was originally a UNIX protocol, it is now supported by some non-UNIX machines as well. Unlike TELNET, Rlogin allows a user logged into a host to access accounts on other (trusted) hosts without re-entering a password.
- **ClearTCP** - Unlike TELNET and Rlogin, ClearTCP is not actually a login service, but a direct connection to a given TCP port number. Eight-bit data is exchanged without interpretation.



The host type setting may override this setting. See step 2 for more information.

Type

Valid types for a login user are:

- login
- login,callback

If you include callback in the user type, you need to specify a phone number at which the user is called back using the following command:

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




*Tip: At this point, it may be helpful to use the **show user** command to display the user's default values. This lets you decide which parameters you need to set, and which parameters you can leave as defaults.*

- 2 Configure Login User Parameters. Use the following command:

```
set login user <name>
    host_type [prompt | select | specified]
    login_host_ip_address <ip_address>
    login_service [rlogin | telnet | cleartcp]
    tcp_port <port_number>
    terminal_type <string>
```

Host Type

Determines how the user is connected to a login host. The default is *select*.

- **prompt** - If the user is prompted, this setting overrides the login service setting. At the prompt, the user can enter the login service (for example, TELNET) and the host name or address, or type *connect* and enter host name or address to use the default login service.
- **select** - (*Default*) The user is automatically connected to a host selected from the Login Hosts Table. The method of choosing the host is set using the **set connection** <host_select> command by *random* or *round robin* (**default**) fashion. For example:

```
set connection host_select random ENTER
```

- **specified** - The user is connected to the host specified in the *login_host_ip_address* setting

Login Host IP Address

If login user's host type is *specified*, you must enter the IP address for the host to be connected to.

Login Service

Specifies the default login service. See Step 1 for details.

TCP Port

Optional. If the login host uses a TCP port number other than 23 (the default for TELNET), you can set the TCP port number using this command. For ClearTCP connections, make sure that the host's TCP port number matches the TCP port number you enter here.

Terminal Type

Optional. Set the terminal type for the remote connection. The default is VT100.

- 3 Save Your Work. Use the following command:

```
save all ENTER
```

IP Terminal Service Case Studies

This section provides examples of how to configure a login user to dial-in to HiPer ARC and establish a TELNET session with hosts on the network.

In Case Study A, the user is prompted for the login service and host address desired. In Case Study B, the user is connected directly to a host you designate.

Figure 2 below depicts the remote terminal connection for a user named Jack to the corporate LAN. Jack's home computer uses VT100 terminal emulation software to establish a IP terminal session with any host on the LAN that he is authorized to access. In the first example, Jack uses TELNET to access the host named Quartz. In the second example, Jill uses rlogin to access the host name Granite.

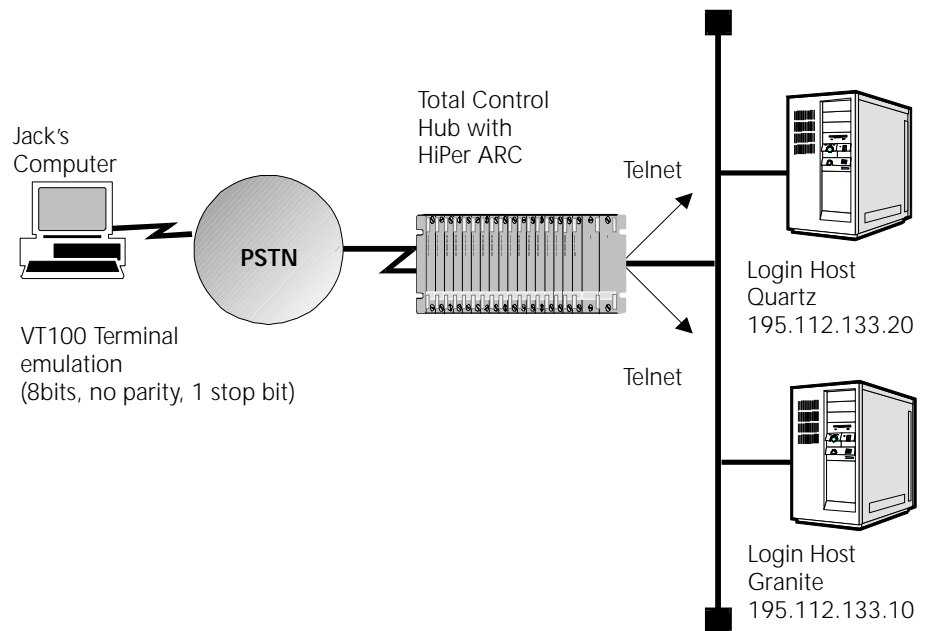


Figure 4-2 IP Terminal Service Example

Case Study A

This case study assumes the following:

- The user has set up a terminal emulation session such as Windows' *HyperTerminal* with a *phone number* and standard communications parameters described on page 4-49.
- The IP network is configured
- All other settings remain at factory defaults
- A DNS server is configured. If not, see *Chapter 2: HiPer ARC Setup*.

Follow these steps to configure the login host and user:

- 1 Add a user "Jack" of the *login* user type with a password.

add user jack type login password sprat ENTER

- 2 Add login hosts "Quartz" and "Granite" for Jack to access. You can prioritize the order these hosts will be offered to him by setting the *preference* of Quartz to 1 and Granite to 2 so if Quartz is unavailable Jack can access Granite. Type:

```
add login_host quartz address 195.112.133.2 pref 1 ENTER
```

```
add login_host granite address 195.112.133.10 pref 2 ENTER
```

- 3 Configure Jack to be able to choose a *login service* and *host name* at the command prompt. Type:

```
set login user Jack host_type prompt ENTER
```

- 4 Save your work. Type:

```
save all ENTER
```

When Jack dials in, he is prompted for his login name as shown below.

```
Welcome to 3Com Total Control HiPer ARC (TM)
Networks That Go The Distance (TM)
login:
```

After Jack is successfully authenticated, the system prompt appears (HiPer:). At this point, Jack can connect to either host by using the following command:

```
telnet quartz ENTER
```

or

```
telnet granite ENTER
```

Since Jack's default login service is TELNET, he could also enter the following command to connect to either host:

```
connect quartz ENTER
```

or

```
connect granite ENTER
```

Jack is connected to the host and prompted for a user name/password. See below..

```
Trying 195.112.133.2...
Connected to 195.112.133.2.
Hummingbird Communications Ltd., Telnet Daemon V5.1
Username: jack
Password:

Microsoft(R) Windows 95
(C)Copyright Microsoft Corp 1981-1995.
Quartz:\>
```

When Jack ends his host session, he is returned to the *HiPer:* prompt. He can access another login host, or he can exit HiPer ARC by typing **exit**. For example:

```
Quartz:\> exit
Connection refused.
HiPer: exit
NO CARRIER
```

Case Study B

This case study assumes the following:

- The user has set up a terminal emulation session such as Windows' *HyperTerminal* with a *phone number* and standard communications parameters described on page 4-49.
- The IP network is configured
- All other settings remain at factory defaults
- A DNS server is configured. If not, see *Chapter 2: HiPer ARC Setup*.

Follow these steps to configure the login host and user:

- 1 Add a user "Jill" of user type *login*, login service of *rlogin* and a *password*. Type:
`add user jill type login password hill login_service rlogin ENTER`
- 2 Configure Jill to specifically access Granite. Type:
`set login user Jill host_type specified login_host_ip_address 195.112.133.10 ENTER`
- 3 Save your work. Type:
`save all ENTER`

When Jill dials in, she's prompted for a login name/password as shown below.

```
Welcome to 3Com Total Control HiPer ARC (TM)
Networks That Go The Distance (TM)
login:
Password:
```

After Jill is successfully authenticated, she is connected to the host and prompted for a user name and password. For example:

```
Trying 195.112.133.10...
Connected to 195.112.133.10.

Hummingbird Communications Ltd., Telnet Daemon V5.1
Username: jill
Password:

Microsoft(R) Windows 95
(C)Copyright Microsoft Corp 1981-1995.
Granite:\>
```

After system authentication, Jill is up and running on the host.

When Jill logs out of her host session, she is exited from HiPer ARC as well. For example:

```
Granite:\> logout
NO CARRIER
```


NETWORK DIAL-IN ACCESS

Dial In Introduction

HiPer ARC allows remote PC users to dial in over analog lines and connect to the local network via the Internet and Internet Packet Exchange protocols.. Remote users can use either of the following protocols to communicate with the network:

- Point-to-Point Protocol (PPP)
- Serial Line Internet Protocol (SLIP)

HiPer ARC provides the remote user with access to all network services such as file servers, electronic mail, Internet services, and printers as if the remote user were connected locally to the network.

Figure 1 below depicts the card's remote network access capabilities.

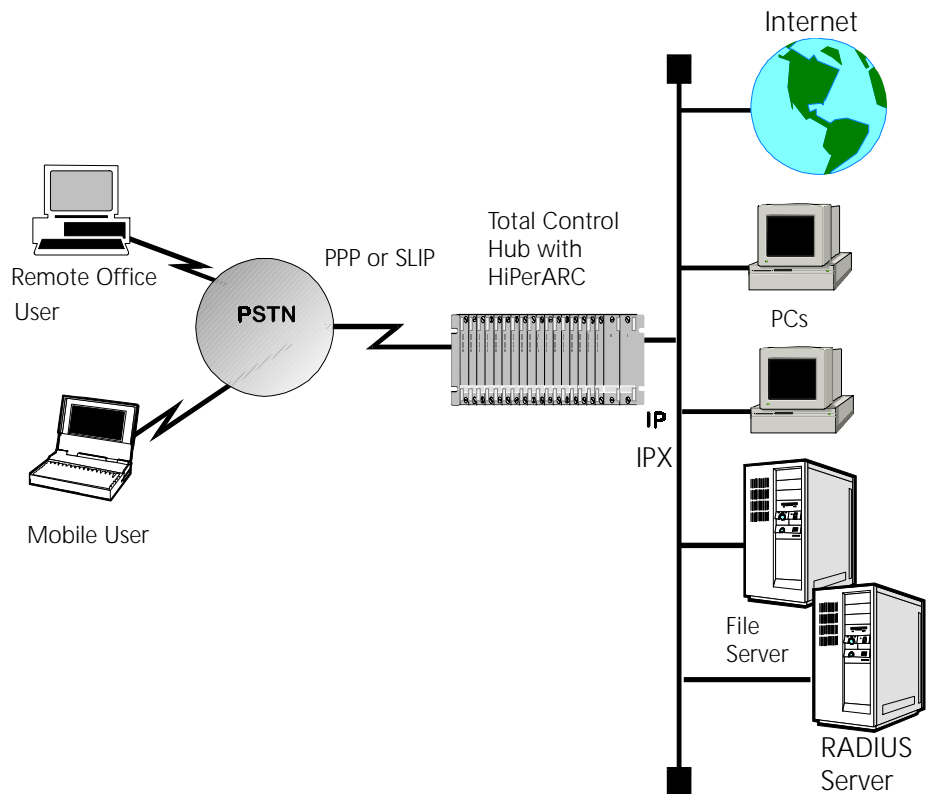


Figure 5-1 Remote Access Capabilities

Dial-in Access Overview

This section describes what you need to do to provide remote access services to dial-in network users.

Configuring for dial-in access simply involves setting up a network user profile for each remote user. The network user profile contains all of the information necessary for the user to connect to the network, such as IP/IPX protocols, remote addresses, and other unique settings.

IP Parameters

IP remote access sessions can use either the PPP or SLIP remote access protocols. You can specify a unique IP address, or you can simply assign the user an address each time he or she dials in. You should know:

- The connection protocol (PPP or SLIP) that users will employ
- The dial-in user's subnet mask
- The Maximum Transmission Unit (MTU) for PPP is 1514, and is negotiated between client and HiPer ARC. If the client uses SLIP, the MTU is 1006, and should match on both sides of the link
- Whether or not the dial-in user is configured with TCP/IP (Van Jacobson) header compression

IPX Parameters

You can configure the user profile to specify a unique IPX network number that will represent the link between the remote system and the local network for the duration of the connection, or you can configure HiPer ARC to assign an IPX network number from a pool. Be aware that:

- IPX remote access sessions must use the PPP protocol
- The IPX MTU is 1500 and is negotiated between the client and HiPer ARC.

Remote Computer Setup

Your remote clients must have a *modem* supporting the remote access protocol used (PPP or SLIP). Also, you may need other network software loaded on your remote clients' PCs such as:

- a *Dial-Up Adapter* to connect to PPP and HiPer ARC
- a *TCP/IP Dial-Up Adapter* to connect to the Internet and Wide Area Networks (WANs)
- the *Client for Microsoft Networks* to connect to other PCs and servers.

Protocol drivers supporting these network components must be loaded on your clients' PCs. Also, if you're employing *Windows 95 Dial-Up Networking*, follow the prompts after successively clicking **My Computer**, **Dial-Up Networking** and **Make New Connection** icons. See your Administrator for configuration help.

When using the Windows' Dial Up Networking facility to make a PPP connection via HiPer ARC, the following problem could arise.



*Configuring a Dial Up Networking session with the **Bring up terminal window after dialing** box checked (found by clicking the **Configure...** button in the start up screen followed by the **Options** tab) will generate a secondary screen which prompts the user for a login name and password. If the user types a name or password incorrectly and tries to backspace or delete the incorrectly spelled text, Windows will display characters which appear to be errors. If the user then tries to delete or backspace over these characters, the session will not be configured correctly.*

Simply typing the correct remaining login name or password following the blacked out characters will result in the session proceeding correctly. We recommend you do not check the **Bring up terminal window after dialing** box to avoid this problem.

In addition, you'll provide the HiPer ARC user with a:

- User name
- Telephone number to access HiPer ARC

Some other considerations:

- If *PPP receive_authentication* is set to *Any*, HiPer ARC auto-detects your remote computer's authentication settings and negotiates MTU size. It attempts CHAP authentication first, followed by EAP, MS_chap and PAP. You may specify an *IP address* for your remote computer during the session. If HiPer ARC is configured to negotiate an IP address with your remote PC, it will automatically detect this address.



If your remote computer does not have an IP address configured and the address selection type is negotiate, HiPer ARC terminates the call.

Your remote computer should be configured for the communications parameters shown below:

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



These are default settings. If you change HiPer ARC's communications settings, you must provide the remote user with the appropriate settings as well. See Chapter 10: Command Reference for more information.

Configuring Address Pools

Dialin network users can be dynamically assigned IP addresses from a pool each time they connect. HiPer ARC does this by configuring IP or IPX address pools.

The **add ip pool** command creates that pool, with the advantage of bundling several IP addresses into one to limit RIP advertisements. The pool is created as a range, starting from an initial address. As PPP or SLIP users dial in, IP allocates addresses from this pool and assigns them to users. IP addresses are automatically allocated on a public/private basis for users who are not assigned to a pool (*public*) or for those who specifically are (*private*). If configured as an *aggregate* address pool, the route will be added to the Routing Table immediately, and advertised as a *single* network route. But if defined as *no_aggregate*, a separate route will be added to the Routing Table for each user when they dial into the chassis.

Different commands are used to configure an IPX pool. See the next section.



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

Configuring an IP Address Pool

To configure an IP address pool:

- 1 Designate an IP address pool name and initial pool address:

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

For example:

```
add ip pool redsox initial_pool_address 172.32.142.2 ENTER
```

- 2 Set other variables with the **set ip pool** command. You can specify the *size* of the pool from 1 to 4096 members, the *state* of the pool, either *public* or *private*, and the pool's *route*, either *aggregate* or *no_aggregate*. Addresses from public pools can be assigned to any user while addresses from private pools are assigned to users of that particular pool only.

For example:

```
set ip pool redsox size 25 state public route aggregate ENTER
```

- 3 Save your configuration. Type:

```
save all ENTER
```

Configuring an IPX Address Pool

To configure an IPX address pool:

- 1 Set the initial pool address and number of pool members with this command:

```
set ipx system name <name> initial_pool_address <ipx_address> pool_members <number>
```

For example:

```
set ipx system name hat initial_pool_address 10 pool_members 15 ENTER
```

- 2 Save your configuration. Type:

```
save all ENTER
```

User Configuration Overview

You configure all remote networking parameters within the profile of the user that is dialing in. A user profile specifies the user's protocol, address parameters, and other unique settings.



You can also specify network user information in RADIUS or TACACS+ servers. For more information, see Appendix E: RADIUS and TACACS+ Systems.

Defaults

A remote access user is defined as a *network* user in the database. When you create a network user, the software builds an extensive user profile that includes many default parameters. These defaults reflect most common types of user configurations. This makes user configuration easier, as you may only need to change a few parameters from their default settings.



When you add a network user, the IP and IPX protocols are enabled by default.

Remote Addressing Options

The options for assigning a network address to a remote user are as follows:

Datalink Protocol	Addressing Options
PPP	From pool (assign, by default), negotiate, specified
SLIP	From pool (assign, by default), specified

Network User Types

A network user can be *one* or a *combination* of the following types. Only callback and dial_out user types are mutually exclusive.

- *network* - Access to network services (PPP, SLIP)
- *network,login* - Access to login (TELNET, rlogin, ClearTCP) or network services
- *network,dialout* - Dial out access to a remote site, with network services
- *network,callback* - HiPer ARC dials the user back with network services
- *network,login,callback* - HiPer ARC dials the user back and provides network or login services
- *manage* - Access to the CLI with full administrative privileges

Configuring an IP/IPX Network User



Use the steps in the following subsections to configure an IP user.

In most cases, connecting to a network requires a password. For HiPer ARC, only the user name is required. For additional security, use a password.

- 1 Add the User. Create a standard network user, specifying the user's *name*, *type*, *password* (optional) and default *network service*. Use the following command:

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

Password

A text string no greater than 64 ASCII characters.

Type

A network user type can be one of those shown above.

Network Service

IP/IPX users can use either SLIP or PPP as their remote access protocol. Note: *SLIP* is not supported for network users with *negotiate* address selected.



*Tip: At this point, it may be helpful to issue the **show user** command to display the user's default values. You can then decide which parameters to set, and which to leave as defaults (D). For example:*

INFORMATION FOR USER: gina

```
Status:                INACTIVE
Type:                  NETWORK
Expiration:            00- -0000
Message:                (D)
Phone Number:          (D)
```

Alternate Phone Number:	(D)
Input Filter:	(D)
Output Filter:	(D)
Modem Group:	all (D)
Session Timeout	0 (D)
Idle Timeout:	0 (D)
PARAMETERS FOR NETWORK USERS:	
Network Service	PPP (D)
Header Compression:	TCPIP (D)
MTU:	1514 (D)
IP Usage:	ENABLED (D)
Address Selection:	ASSIGN (D)
Remote IP Address:	0.0.0.0/H (D)
IP Routing:	NONE (D)
IP RIP Routing Protocol:	RIPV1 (D)
IP RIP Routing Policies:	
IP RIP Authentication Key:	
Default Route Option:	DISABLED (D)
Spoofing:	DISABLED (D)
PARAMETERS for NETWORK PPP USERS	
Max Channels	1 (D)
Channel Decrement Percent:	20 (D)
Channel Expansion Percent:	60 (D)
Expansion Algorithm:	LINEAR (D)
Receive ACC Map:	ffffffff (D)
Transmit ACC Map:	ffffffff (D)
Compression Algorithm:	AUTO (D)
Compression Reset Mode:	AUTO (D)
Min Compression Size:	256 (D)

For example, to add a network/manage user employing PPP over IP/IPX, type:

```
add user gina password cute type network/manage network_service ppp ENTER
```

- 2 Specify a Remote IP/IPX Address. If you want to explicitly *specify* the network user's remote IP/IPX address, follow the instructions in this step. If you want the remote IP/IPX address to be selected from a *pool* or *negotiated*, go to step 3. When adding a remote IP address, HiPer ARC automatically chooses the *specified* address selection method, so you do not need to configure the value.

Use either of the following commands:

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

```
set network user <name> ipx
address <ipx_address>
```

For example:

```
set network user gina ip remote_ip_address 195.114.123.16 ENTER
```

```
set network user gina ipx address 100 ENTER
```

- 3 Set the Address Selection Method. For *IP*, if the network user's address is not specified, you need to define whether the user's remote *IP* address is assigned or negotiated.

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

- *assign* - Configure an IP address from the IP address pool, which is set globally using the **set ip pool** command (see *Configuring an IP Address Pool* on page 5-59).
- *negotiate* - PPP connections only. The remote computer must have an IP address configured. HiPer ARC tries to learn the remote computer's IP address using IPCP address negotiation. If the remote computer does not have an address configured, the user is disconnected.



SLIP is not supported for network users employing this method.

For example:

```
set network user gina ip address_selection negotiate ENTER
```

When creating a *IPX* network user, the default IPX address is set to *00000000*. Be aware that:

- If the remote computer has an IPX address configured on it, and an IPX address is not specified in the user profile, HiPer ARC will negotiate the remote address.
- If HiPer ARC can't negotiate an IPX address, an IPX address is selected from the pool, which is set globally using the **set ipx system** command described in an earlier section.

- 4 Save Your Work. Use the following command:

```
save all ENTER
```

Continue with one of the following sections of this chapter for more information on setting other network user parameters:

- Configuring PPP Parameters
- Configuring Additional Parameters

Configuring PPP Parameters for Network Users



If a remote user connects using PPP, you can also define several PPP parameters that control how the remote access session is handled.

This section describes parameters that are mainly applicable for network dial-in users. Many of the configurable PPP parameters are more often used for LAN-to-LAN routing users only although channel decrement, channel expansion and max channels parameters can all be configured for callback users to employ bandwidth allocation. See Chapter 7: LAN-to-LAN Routing for more information.

Use the following command:

```
set network user <name> ppp
compression_algorithm [ascend | auto | microsoft | none | stac]
expansion_algorithm [constant | linear]
min_size_compression [value from 0-2048]
```

```

receive_acc_map [hex_number - array of 4 bits]
reset_mode_compression [auto | every_packet | every_error]
transmit_acc_map [hex_number - array of 4 bits]
channel_decrement [0-100]
channel_expansion [0-100]
max_channels [0-16]

```

Compression Algorithm

Optional. Specifies which proprietary data compression algorithm PPP should use. The default *auto* selection autodetects the correct algorithm for the connection. *Ascend*, *Microsoft*, *Stac* and *None* are other choices.



The **set ppp ccp_modemtype** [*digital,compressed_analog,uncompressed_analog,none,all*] command controls the offering of the configured PPP compression algorithm.

If you know the type of traffic your connection will bear, using this command will be beneficial. For example, type:

```
set ppp ccp_modemtype digital,compressed_analog ENTER
```

Afterwards, use the **show ppp** command to verify your settings. The default is *digital/uncompressed_analog*. For example:

PPP AUTHENTICATION

DIAL_IN Users Authenticate PAP or CHAP:	EITHER
System Transmit Authentication Name:	HiPer
PPP offloading:	ENABLED
CCP will be attempted for call type(s):	DIGITAL
	COMPRESSED_ANALOG
Primary NBNS Server address:	0.0.0.0
Secondary NBNS Server address:	0.0.0.0
Use system DNS configuration:	ON

Expansion Algorithm

Optional. Specifies which type of expansion algorithm should handle bandwidth allocation. Each algorithm measures traffic bandwidth over 60 second intervals. Use *constant* if you want to take a conservative approach to bandwidth allocation and not react to short-term bandwidth changes. Use *linear* if you want to measure more current, higher weight traffic when allocating bandwidth. Default: *linear*.

Minimum Compression Size

Optional. Specifies the minimum size at which PPP compresses a packet. Data packets smaller than this value are not compressed. Default: 256.

Receive Asynchronous Character Control Map

Optional. Determines whether HiPer ARC uses the asynchronous control character map to filter incoming data. Default: *ffffff*.

Reset Compression Mode

Optional. Determines how often PPP should examine packets to decide when to re-negotiate the optimum compression algorithm. Default: *auto*.

Transmit Asynchronous Character Control Map

Optional. Determines whether HiPer ARC uses the asynchronous control character map to filter outgoing data. Default: *ffffff*.

Channel Decrement

Indicates the channel decrement *percentage*. When total aggregate usage (specified by the number of modems in the modem group) drops below this percentage, PPP will drop a channel. Since the default is *0*, *all* channels are available for use until you set this value. Recommended setting: *20*

Channel Expansion

Indicates the channel expansion *percentage*. When total aggregate usage (specified by the number of modems in the modem group) exceeds this percentage, PPP will add another channel. Since the default is *0*, *all* channels are available for use until you set this value. Recommended setting: *60*

Maximum Channels

Specifies the maximum number of channels this user can use; in effect, turning multilink PPP on or off. Specifying one channel disables multi-link PPP. The default is 2. You can use as many channels as desired depending on the specified modem group.

Configuring Additional Parameters

In addition to protocol-specific parameters that you configure for IP, you can also set several standard network user parameters.

MTU

Determines the Maximum Transmission Unit (MTU), or largest packet size in bytes HiPer ARC will accept. The default setting is *1514* for *PPP* and *SLIP* although the maximum MTU SLIP will accept is *1006*. PPP connections negotiate the MTU while SLIP connections are not. Use the following command:

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

Receive PPP Authentication

By default, HiPer ARC detects the type of authentication used by its clients for PPP connections using either Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Microsoft CHAP (MS_chap), EAP (EAP_MD5 native mode) or none.

The default setting is *any*. When a user dials in, HiPer ARC tries to authenticate the user by first using CHAP (or an administrator-specified type using the *authentication_preference* parameter). If the client does not support it, HiPer ARC attempts to use EAP, MS_chap and PAP - in that order.

If the remote computer doesn't respond, the connection is dropped. You can change the authentication setting by typing the following:

```
set ppp receive_authentication [none | pap | chap | any | eap | ms_chap | encrypted_any | |radius_eap_proxy]
```



*If the **any** or **encrypted_any** value is selected, the authentication protocol tried first from the group can be selected by specifying the *authentication_preference* parameter (see below). Note the following choices:*

- If *receive_authentication* is set to *any*, then *authentication_preference* can be set to *CHAP*, *MS_chap*, *EAP*, *proxy_eap*, *PAP* or *default* (CHAP).
- If *receive_authentication* is set to *any*, then *authentication_preference* can be set to *CHAP*, *MS_chap*, *EAP*, *proxy_eap*, or *default* (CHAP).
- If *receive_authentication* is set to *any other value*, then the *authentication_preference* setting is ignored.

If you know what type of authentication your client will use, specify it:

```
set ppp authentication_preference <chap | default | eap | ms_chap | pap | radius_eap_proxy>
```

Phone Number

If the network user is a callback user, use the following command to set the user's phone number. *Note*: this value does not apply to other dialin users.

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

Alternate Phone Number

Callback users who want to supply an *alternate* phone number can do so with this command. *Note*: this value does not apply to other dialin users.

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

Idle and Session Timeouts

If you want to limit a user's time on the line or end a call after a specified idle period, type the following:

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

Remote Access Case Study A

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

Assumptions

This case study assumes the following:

- A *Windows 95 Dial-Up Networking* connection has been created and *Network* settings configured for the client
- HiPer ARC uses the correct IP address and netmask
- The IP network is configured
- CHAP is the preferred authentication type
- All other settings remain at factory defaults

How to Configure this User

To configure:

- 1 Add a user "Gina" of the *network/callback* type with a *password*. Type:

```
add user gina type network,callback password yellow ENTER
```



Because the default network service is PPP, it needn't be set.

- 2 Enter *phone* and *alternate phone numbers* at which HiPer ARC calls Gina back. Type:

```
set user gina phone_number 5085524438 alternate_phone_number 5085527867 ENTER
```

- 3 Gina's home PC has an IP address configured on it. HiPer ARC will detect this address by setting the address selection method to *negotiate*. Type:

```
set network user gina ip address_selection negotiate ENTER
```

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

```
set user gina idle_timeout 300 user_timeout 6000 ENTER
```

- 5 Save the changes to FLASH memory. Type:

```
save all ENTER
```

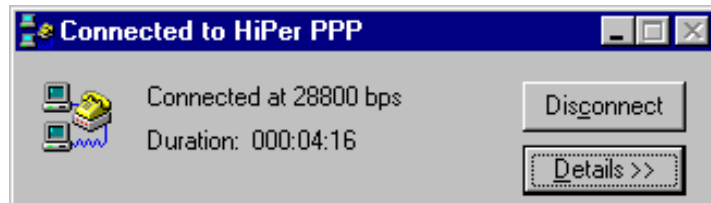
How it Works

Gina dials in to HiPer ARC using PPP (*Dial-Up Networking*) with the user name and phone number supplied by the administrator. After Gina is authenticated by CHAP (the authentication type supported on her network), the call is disconnected and HiPer ARC dials Gina back at the phone or alternate phone number. Once reconnected, HiPer ARC attaches the user to the host or gateway specified in the Windows 95 **Network** dialog box from the **Control Panel** under **Settings**. If Gina exceeds the timeouts, the call is disconnected.



By default, HiPer ARC autodetects the authentication method a remote computer uses. HiPer ARC first tries CHAP, then other authentication types. If the remote PC doesn't support one of these methods, the call is dropped.

If the PPP link to HiPer ARC succeeds, the message below appears on Gina's screen:



Remote Access Case Study B

In this case study, a *network* user is configured for the IP protocol. This user's *IP address* is *assigned* by HiPer ARC, the *authentication preference* is PAP, and *session* and *idle timeouts* are specified.

Assumptions

This case study assumes the following:

- A *Windows 95 Dial-Up Networking* session has been made and the client's *Network* settings configured
- HiPer ARC uses the correct IP address and netmask
- The IP network is configured
- All other settings remain at factory defaults

How to Configure this User

To configure:

- 1 Create *network* user "Bridget" of *network* user type and a *password*. Type:
`add user bridget password holliston type network ENTER`
- 2 Set the type of authentication preferred by Bridget's PC. Type:
`set ppp authentication_preference pap ENTER`
- 3 Bridget's home PC has no IP address configured on it. The IP address will be assigned by HiPer ARC to authenticate. Since the address selection method is *assign* by default from an IP address pool, you do not need to configure the value. But you need to create an *IP pool* with an *initial pool address*. Type:
`add ip pool redsox initial_pool_address 177.143.045.9 ENTER`
- 4 Now that you've added the address pool, set its *size*, *state*, and *route*.

For example, type:

```
set ip pool redsox size 25 state public route aggregate ENTER
```

- 5 Add *idle (90 seconds)* and *session timeouts (1800 seconds)* to limit Bridget's time on the line. Type:

```
set user bridget idle_timeout 90 session_timeout 1800 ENTER
```

After 90 seconds of idle time, Bridget's PC will hang up; after 1800 seconds, her session will end.

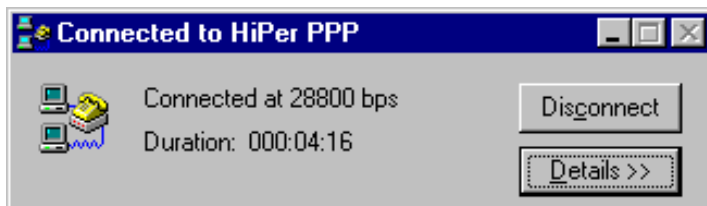
- 6 Save the changes to FLASH memory. Type:

```
save all ENTER
```

How it Works

Bridget dials into HiPer ARC using PPP (*Dial-Up Networking*) with the user name and phone number supplied by the administrator. Bridget is authenticated by PAP (the authentication type supported on her network), and a network login and password is prompted by Windows. If approved, the user is connected to the host or gateway specified in the Windows 95 **Network** dialog box from the **Control Panel** under **Settings**. If Bridget exceeds the timeout periods, the call will be disconnected.

If the PPP link to HiPer ARC succeeds, the following message appears on Bridget's screen:



Remote Access Case Study C

In this case study, a *network* user is configured for the IPX protocol. This user's *IPX address* is *assigned* by HiPer ARC from a pool, the *authentication preference* is CHAP, and *session* and *idle timeouts* are specified.

Assumptions

This case study assumes the following:

- A *Windows 95 Dial-Up Networking* session has been made and the client's *Network* settings configured
- The IPX network is configured and HiPer ARC uses the correct IPX address
- All other settings remain at factory defaults

How to Configure this User

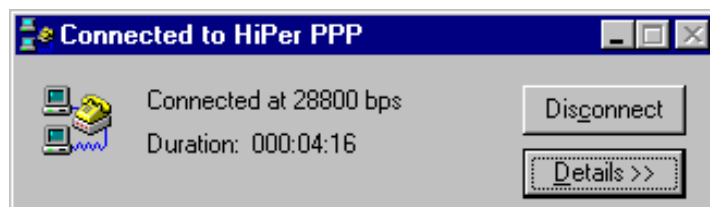
To configure:

- 1 Create *network* user "Brad" of *network* user type and a *password*. Type:
`add user brad password holliston type network ENTER`
- 2 Set the type of authentication preferred by Brad's PC. Type:
`set ppp authentication_preference chap ENTER`
- 3 Brad's home PC has no IP address configured on it. The IPX address will be assigned by HiPer ARC to authenticate. Since the address selection method is *assign* by default from an IPX address pool, you do not need to configure the value. But you need to create an *IPX pool* with an *initial pool address* and number of *pool members*. Type:
`set ipx system redsox initial_pool_address 100 pool_members 8 ENTER`
- 4 Add *idle (90 seconds)* and *session timeouts* (1800 seconds) to limit Brad's time on the line. Type:
`set user bridget idle_timeout 90 session_timeout 1800 ENTER`

 After 90 seconds of idle time, Brad's PC will hang up; after 1800 seconds, his session will end.
- 5 Save the changes to FLASH memory. Type:
`save all ENTER`

How it Works

Brad dials into HiPer ARC using PPP (*Dial-Up Networking*) with the user name and phone number supplied by the administrator. Brad is authenticated by CHAP (the authentication type supported on his network), and a network login and password is prompted by Windows. If approved, Brad is connected to the host or gateway set in the Windows 95 **Network** dialog box from the **Control Panel** under **Settings**. If Brad exceeds the timeouts, the call is dropped. If the PPP/HiPer ARC link succeeds, the message below appears on Brad's screen:



6

NETWORK DIAL-OUT ACCESS

Introduction

Modem ports on the Total Control Hub with HiPer ARC can be accessed by network PCs and workstations to provide dial-out services. This allows network users to send faxes, and connect to Bulletin Board Systems (BBS), information services such as CompuServe, or the Internet over a dial-up PPP link.

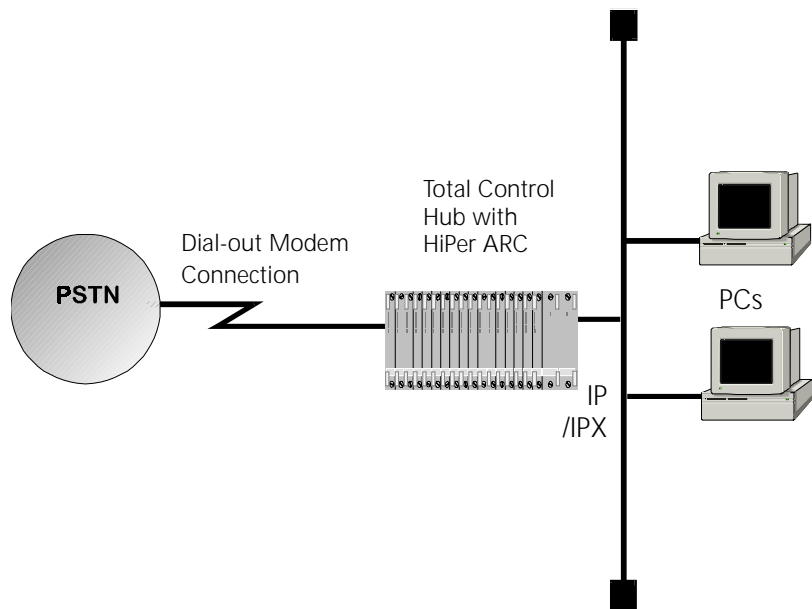


Figure 6-1 Dial-Out Topology

Overview

HiPer ARC provides these network dial-out services:

- IP/IPX dial-out (modem sharing)
- ClearTCP
- TELNET dial-out

IP/IPX Dial-Out

IP/IPX dial-out is commonly known as modem sharing, meaning that any number of network Hubs can be configured for modem pools allowing network user connections on a first-come, first-serve basis.

ClearTCP Dial-out

HiPer ARC supports ClearTCP daemon as a network service. ClearTCP is used by some Internet providers to tunnel user data through a socket in rough form without network protocols being applied.

Network Communications Services Interface (NCSI)

To perform IP/IPX dial-out, a client PC can use any Network Communications Services Interface (NCSI)-compatible application to gain access to HiPer ARC on the network. IP/IPX users can use any NCSI- or non-NCSI compatible Windows 95 communication application.

NCSIPort

Most Windows 3.x and Windows 95 communication applications support NCSI. In case you happen to have an application that doesn't support NCSI, you can bridge that gap by using Network Products Corporation's NCSIPort application. This application allows non-NCSI-aware communication applications to connect to HiPer ARC. NCSIPort is a Windows virtual driver that redirects data meant for a local COM (serial) port to the Hub's modems without the communication application knowing the difference.

How It Works

From the client's perspective, when a network user wants to use a Hub modem port to dial-out, the user executes the communication application from the client PC (with the assistance of NCSIPort if necessary).

NCSI provides a network naming service that allows you to name each device on your network, as well as the ability to name ports by both the type of service they perform (for example, MODEM) and by a specific name (for example, *slot:9/mod:1*). The user can then select a specific service, modem group, or modem port from a list.

From the server's perspective, a *network service* and *modem group* are made available to the user. If authentication is required on that group's port, the user is prompted for a login name and password. Once authentication is successful, a user can issue AT commands, initialization scripts or directly dial out the port.

TELNET Dial-Out

HiPer ARC supports modem sharing for TELNET users in a manner similar to IP dial-out. A network user can TELNET to HiPer ARC and access an interface or modem group for dial-out.

After a modem is allocated to a user either individually or via a modem group, the user is connected to a TELNET session. All characters received from the user are sent to the modem (for example, AT command strings) and all characters received from the modem are sent to the user. Once connected, the TELNET user can issue AT commands and dial out the modem port.

Network Dial-Out Configuration Overview

To configure HiPer ARC for network dial-out services, follow these steps:

- Add modem groups or a specific interface (TELNET dialout).
- Add the dial-out service.
- Add dial-out users (TELNET users disregard).
- Set global dial-out service parameters.
- Optional - set TELNET Dial-Out parameters.
- Load and configure NCSI client software (TELNET users disregard).



This section assumes you have completed basic system configuration, including adding and enabling the IP network.

Network Dial-Out Configuration

Configure Modem Groups

By default, all modem ports on your HiPer ARC belong to modem groups *all*, *slot:1*, *slot:2*, *slot:3*, etc. But, you can define modem groups (for all network services *except* DialOut) that contain a range of interfaces in slots throughout the Hub - modem interfaces can belong to more than one modem group.



To configure an **interface** rather than a modem group, skip to the next section.

When network users request the use of a modem group, they are assigned the first available modem from that group. If all modems in the modem group are being used, users receive a message indicating a modem could not be made available. Users can either re-submit the request for a modem or select another modem group.

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

```
add modem_group <group_name>
interface [slot:x/mod:[1-y], slot:x/mod:[1-y],etc.]
```

For example, configure two modem groups, one called abc, the other xyz:

```
add modem_group abc interface slot:2/mod:1,slot:2/mod:9,slot:2/mod:10,slot:2/mod:12 ENTER
```

```
add modem_group xyz interface slot:3/mod:2,slot:4/mod:[3-7] ENTER
```



Modem groups specified above for DialOut network service must match **exactly** (case-sensitive) the modem group specified for the DialOut user to insure a proper dial-out connection. For instance, if you create a DialOut network service for the default modem group **all**, then the DialOut user you create must also specify the modem group **all**.

Configure Dial-Out Service

Adding a dial-out service configures HiPer ARC to listen for client requests (TELNET users, skip to the *Configure Dial-Out Users* section). Use this command:

```
add network_service <name up to 8 characters>
server_type dialout
data <modem group information>
socket <number>
close_active_connections <true | false>
```

name	Name you specify for the service. Limit: 8 ASCII characters.
server_type	Designates the type of service. The parameter in this case is <i>dialout</i> .
data	Used to assign one or more modem groups to the dial-out service. <i>Note:</i> You must assign an interface or modem group but not more than one to the DialOut service or it will not be enabled.
socket	Dialout service uses TCP port 32773 which can't be changed for this service type
close_active_connections	Indicates whether or not to close any active connections when a service is disabled by the disable network_service command. Default is <i>FALSE</i> .

You'll start by specifying an interface or modem group, expressed as follows:

```
data modem_group=<group_name>\
```

or

```
data interface=slot:x/mod:y
```



See Chapter 10: Command Reference and Chapter 9: Administrative Tools for more on **data** values.

For example: add the network service "modems", server type "dialout", that specifies the default modem *all*, type:

```
add network service modems server_type dialout data modem_group=all ENTER
```

or, create the same network service but on a particular interface:

```
add network service modems server_type dialout data interface=slot:3/mod:1 ENTER
```



If any **data** value includes a space, enclose it in double quotations and backslashes.

Configure Dial-Out Users

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

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

```
set user <name> modem_group <name>
```

For example:

```
add user gil password fish type dial_out ENTER
```

```
set user gil modem_group abc ENTER
```

Set Global Dial-Out Parameters

You can set three *global* configuration parameters with the following command.



This command does not apply to TELNET Dial-Out Service.

```
set dial_out
  idle_timeout <minutes>
  recovery_timeout <minutes>
  security no
```

idle_timeout	Determines the interval that HiPer ARC will wait before closing an inactive dial-out connection. Default: 5 minutes . Limit: 65535 minutes .
recovery_timeout	When a client terminates a connection, this setting determines the interval that HiPer ARC will wait before closing the session. For example, if a user accidentally disconnects his LAN connection, he can plug it back in without losing his session with the Hub. Default: 5 minutes . Limit: 65535 minutes .
security	Determines whether to require a user name and password to dial out. Default: yes <i>Note:</i> Set value to no . Use the NCSI Security Login to build a secure link.

For example:

```
set dial_out idle_timeout 2 recovery_timeout 2 security no ENTER
```

Configure Telnet Dial-out Service

Follow these steps to configure TELNET dial-out service:

- 1 If you've already added a *modem group* and *dial-out* user as directed earlier, set *network service*:
 - *server_type* as *telnetd*
 - *socket* number higher than 1024 (to avoid conflicts with existing sockets)
 - *DATA* parameters:
 - *service_type=dialout*
 - *interface=<name>* or *modem_group=<name>* Specify an individual modem (*interface=slot:3/mod:1*), a default modem group (*all*) or create a modem group.

Optionally, if you want to provide a *login banner* or *login prompt*, they are expressed as:

- *login_banner*="string"
- *login_prompt*="string"



Adding backslashes and control characters \r\n\ to banners or prompts places a carriage return after the string.



*If you don't want dial-out callers seeking authentication, add *auth=off* to the *DATA* value of the network service (*auth=on* is the default). In this case, do not add a user when setting *auth=off*.*

An example using a *modem group*:

```
add network service modems server_type telnetd socket 6666
data service_type=dialout,login_banner=\"Hi y'all\r\n\", modem_group=all ENTER
```

An example using a specific modem:

```
add network service modems server_type telnetd socket 6666 data
service_type=dialout,login_banner=\"Hi y'all\r\n\", interface=slot:3/mod:1 ENTER
```



IMPORTANT: *You cannot assign more than one modem group to a TELNET network service.*

The previous example makes available modem ports assigned to the default modem group *all*. If you want to make only *one* port available for TELNET service, type the following and save your changes:

```
add modem_group telnet_users interface slot:6/mod:5 ENTER
```

```
add network service t1 server_type telnetd socket 6666 data
service_type=dialout,login_banner=\"Hi y'all\r\n\",
modem_group=telnet_users ENTER
```

```
save all ENTER
```

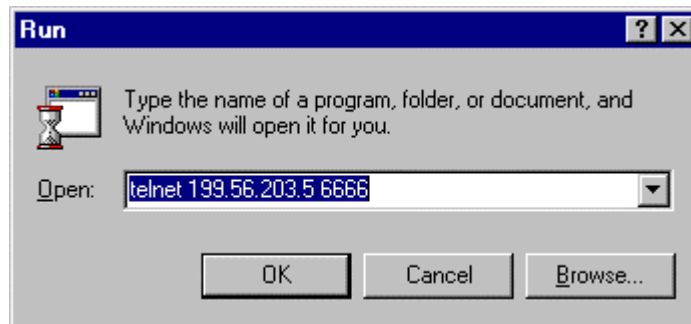


*If any **data** string value contains a space, enclose it in double quotations and backslashes as shown above.*

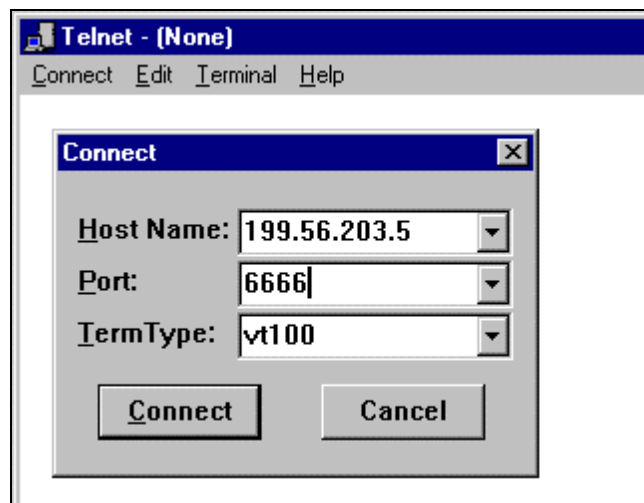
- 2 Type **list network services** to review network service settings. Be sure that *Administrative Status* is *enabled*. If *disabled*, you'll need to try again.
- 3 For example:

CONFIGURED NETWORK SERVICES				
Name	Server Type	Socket	Close	Admin Status
modems	TELNETD	6666	FALSE	ENABLED
DATA: modem_group="all",service_type=dialout,login_banner="Hi y'all"				
tftpd	TFTPD	69	FALSE	ENABLED
DATA:				
telnetd	TELNETD	23	FALSE	ENABLED
DATA:				

- 4 TELNET to Hiper ARC's IP address with a TCP Port number matching the socket number set earlier.
 - WIN 95 users: from the **Start** icon, click on **Run** and, in the dialog box, type *telnet 199.56.203.5 6666* in the **Open** field as shown below.



- *or*, after opening the **Run** box, type *telnet*, press **OK**, and when the session begins click **Connect** and **Remote System** to bring up the **Connect** box below. Replace TELNET with socket number *6666* in the **Port** field.



- 5 Configured users are prompted to login and upon authentication can issue AT commands to the modem. Be aware that callers with the DATA value *auth=off* are not prompted to login.



Important: Characters you type after providing a login and password do not display on the screen.

For example, issue the *AT/4* command:

login: gil

Password:.

USRobotics Analog/Digital Quad Settings...

Copyright, 1988-97, U.S. Robotics. All rights reserved.

B0 C1 E0 F1 Q0 V0 X0

BAUD=38400 PARITY=N WORDLEN=8 DTE=GATEWAY NAC

DIAL=TONE ON HOOK TIMER LINE=STANDARD ANALOG

&A0 &B0 &C1 &D2 &G0 &H0 &I0 &K1 &L0 &M4 &N0 &P0 &R1 &S0
&T4 &U0 &X0 &Y1%N6 *U1=0 *U2=0 *U3=1 *V2=0 *X0=2048 *X1=2

S00=000 S01=000 S02=255 S03=013 S04=010 S05=008 S06=002 S07=060
S08=002 S09=006 S10=007 S11=070 S12=050 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=005 S26=001 S27=000 S28=008 S29=020 S30=000 S31=000
S32=009 S33=000 S34=000 S35=000 S36=000 S37=000 S38=000 S39=011
S40=000 S41=000 S42=126 S43=200 S44=015 S45=000 S46=255 S47=032
S48=000 S49=016 S50=100 S51=000 S52=005 S53=000 S54=064 S55=000
S56=000 S57=000 S58=000 S59=000 S60=000 S61=000 S62=000 S63=000
S64=000 S65=000 S66=000 S67=001 S68=000 S69=000 S70=000 S71=001
S72=000 S73=001 S74=000 S75=000 S76=004 S77=000 S78=000

LAST DIALED #: T918479825092

LAST DNIS #: LAST ANI #:

or, for example, call the 3Com BBS site at 847 982 5092:

login: gill

Password:

CONNECT 28800/ARQ/V34/LAPM/V42BIS

CONNECT 115200 / 10-14-97 (13:23:44)

(Error Correcting Modem Detected)

USR Support BBS - Node 12 - Total Control Rack

PCBoard (R) v15.3/250 - Node 12

CONNECT 28800/ARQ/V34/LAPM/V42BIS

Testing your system capability...



Modem LEDs light only when modem calls are unhooked (amber) and connected (green), not before. A TELNET connection (SHRMOD) will not light the modem unless a call is placed.

Editing Network Services

You can change network service values using the **set network service** command. But two caveats apply:

- Some DATA parameters may be lost when you re-issue the **set network service** command. So re-enter any unsaved options.
- Before using the **set network service** command, you must first disable the network service. Enable the network service again once the change is made. The network service is enabled by default when you add it. To disable the service, type:

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

To enable network service, type:

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



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

NCSI Client Software Installation and Setup

The NCSI Client Setup program is designed to run on any LAN workstation using Windows 95 over the IP/IPX protocol connected to HiPer ARC. Support is *not* available for DOS and 3.x clients.

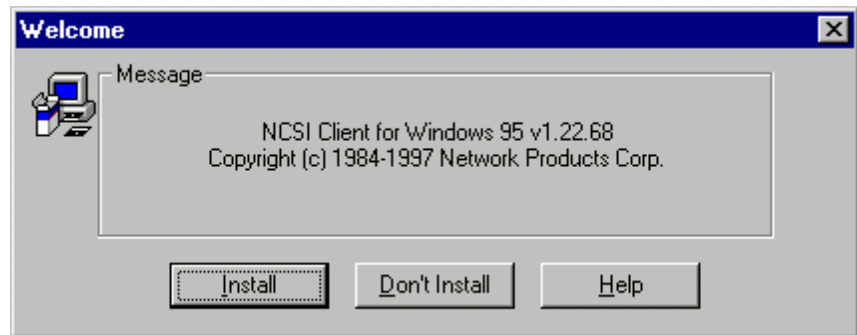
Installing NPC Client for Windows 95

To install the NPC Client software for Windows 95:

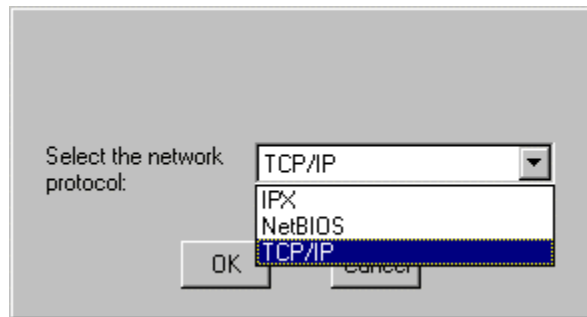
- 1 Start Windows 95, click on the **Start** button on the Windows Taskbar, then click **Run**.
- 2 Insert the Windows 95 Client Installation diskette into the floppy disk drive. At the **Run ...** command line, type:

```
a:\setup.exe ENTER
```

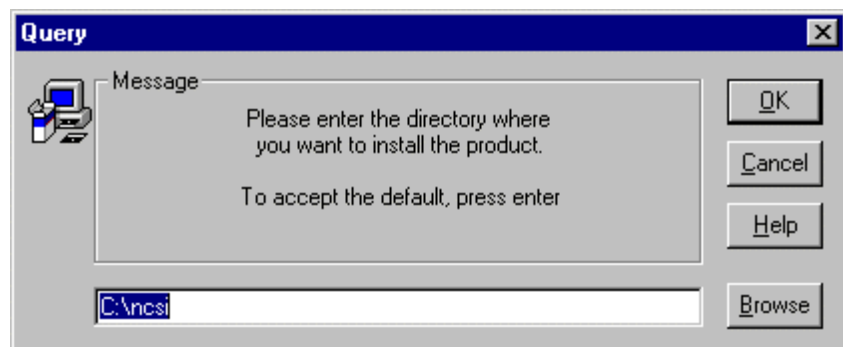
- 3 At the **Welcome** screen, click on **Install**. See illustration below.



Select the network protocol - **TCP/IP** and click **OK**. See illustration below.



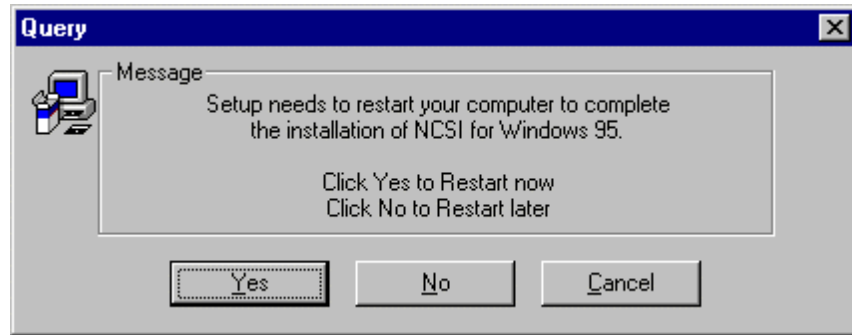
In the **Query** panel, accept the displayed default directory where you want to install NCSI, or enter a different directory in the open field, or click on **Browse**. Click **OK**. See illustration below.



- 4 After a few moments when installation is complete, remove the Installation Diskette and click on **Yes** to reboot your computer now. See illustration below.



You must restart Windows before using NCSI. We recommend you do it now.



- 5 Continue setup with *Configuring NCSIport for 95* below.

Configuring NCSIport for 95

NCSIport for 95 is a 32-bit Windows application that redirects communications calls to NCSI. It supports:

- NCSI-compatible DOS applications
- 16-bit Windows applications that support NCSI
- Native 32-bit Windows 95 applications

The NCSI Setup utility now automatically installs the NCSI Client Redirector on COM4 so it isn't necessary to go through the **Add New Hardware** step in **Control Panel**. There are two steps to perform:

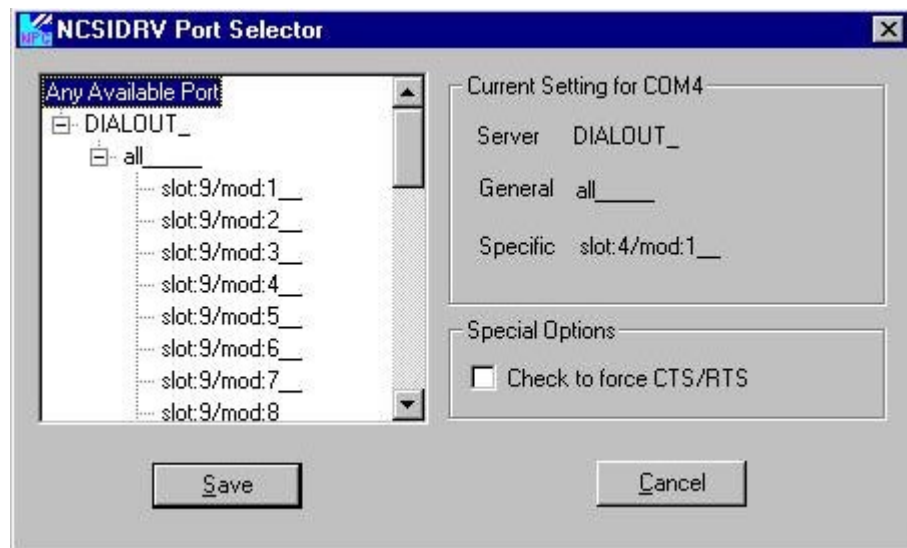
- Tell the Redirector where to get the name to connect to via the **Port Setup for NCSIPort 95** applet
- Set up *security* with a *login name* and *password*

To set up NCSIport for 95, follow the steps below.

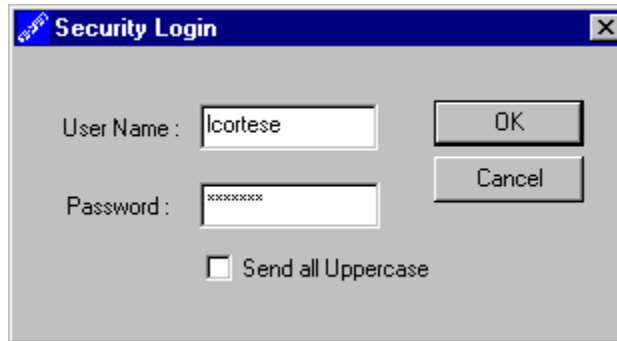
- 1 In the **Network Products Corp** icon group, click on the **NCSI Redirector Port Setup** icon. See illustration below.



- 2 Select the Communications Server (a HiPer ARC-named network service). Click on **Any Available Port**, and when NCSI finds the HiPer ARC network service you specified, choose the **Server**, and a **Specific** slot and port. Do not select a **General** port. Click on **Save** when you're finished. See figure below.



- Back in the **Network Products Corp** icon group, click on the **Password Setup** icon. In the Security Login box, type a **User Name** and **Password** and click **OK**. See the following illustration.



- Now that you have configured NCSIport for 95, it will be available for any communications application every time. To change this initial configuration, simply follow the steps above to reconfigure.

Dialing Out Using a NCSI Port

Once NCSIport for 95 has been setup, you can begin using IP dial-out by setting up a Windows-based **Dial-Up Networking** session to use the specified COM4 port.



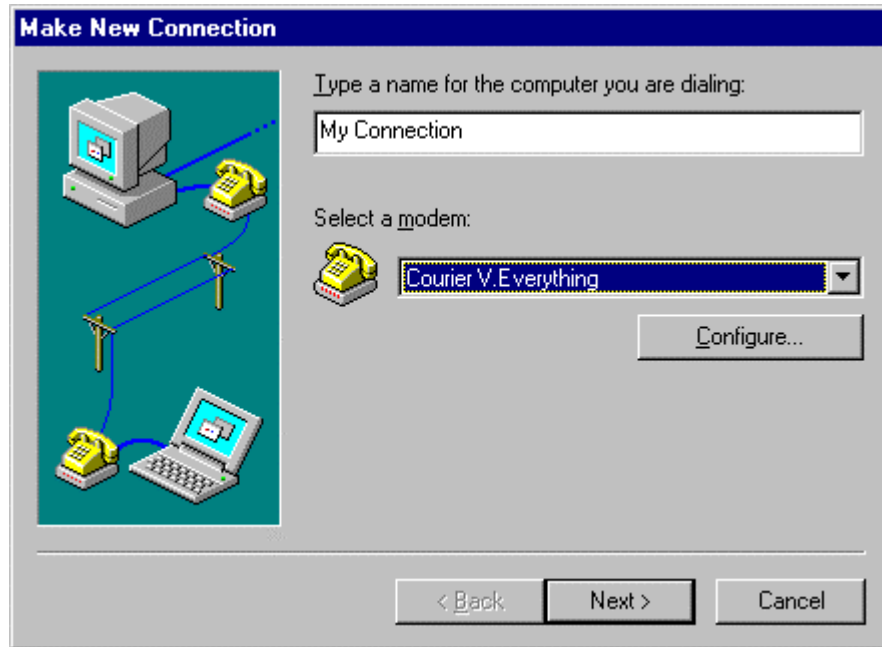
Windows 95 has a feature that disables whatever protocol you are using over a Dial-Up connection on the Local Area Network. Since the NPC Client program for Windows 95 uses IP to communicate with HiPer ARC, you can only use a server type of NetBEUI or TCP/IP. If you select IPX/SPX, this will cause your PC to lock because that protocol will be disabled on the LAN.

To dial out a NCSI port, follow the steps below.

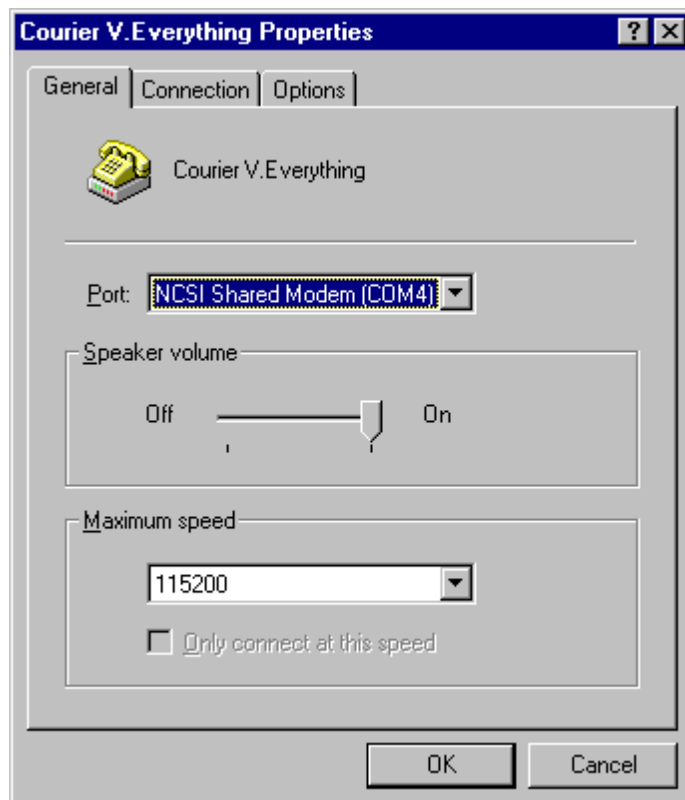
- From your PC, double-click on the **My Computer** icon, double-click on the **Dial-Up Networking** icon, and double-click on the **Make New Connection** icon. See illustration below.



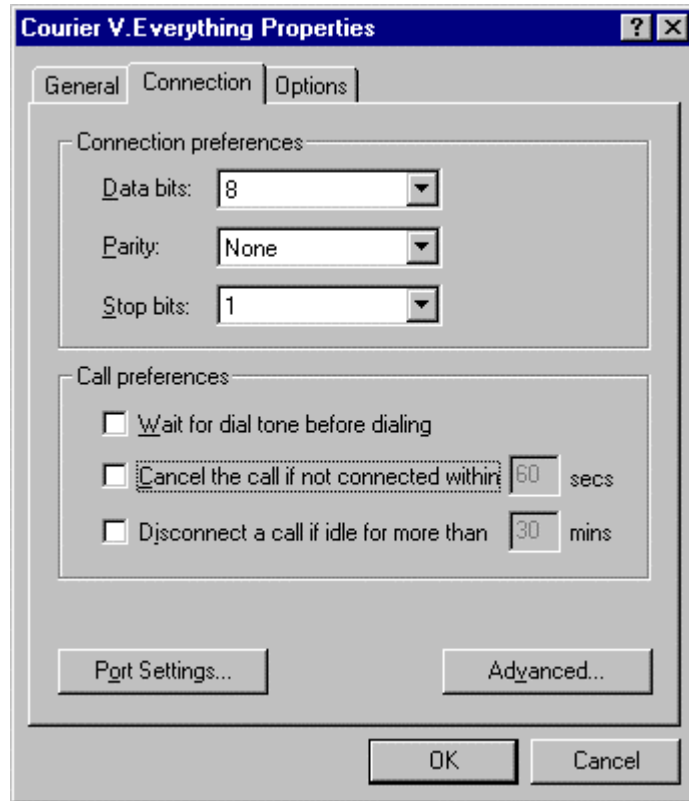
- 2 In the **Make New Connection** panel, name your connection in the field provided and select a modem: **Courier V. Everything**, if available, or **Standard Modem**, if not. Click on **Configure...** See illustration below.



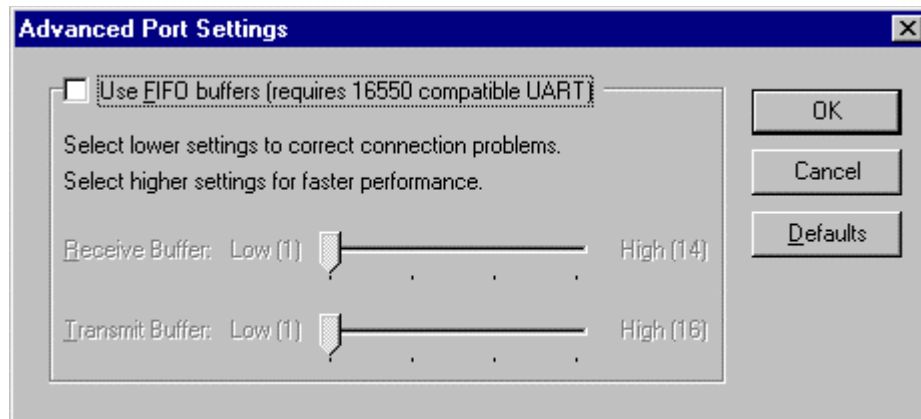
- 3 In the **General** tab select **NCSI Shared Modem (COM4)** and click on the **Connection** tab. See illustration below.



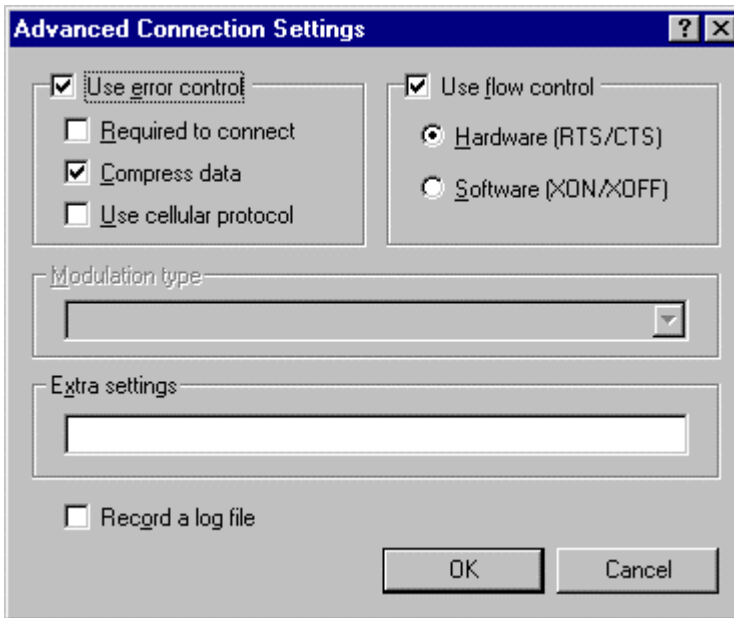
- 4 In the **Connection** panel, don't change the standard **8 Data bits**, **Normal Parity** and **1 Stop bits** values and leave all **Call preferences** boxes blank. Click on **Port Settings...** See graphic below.



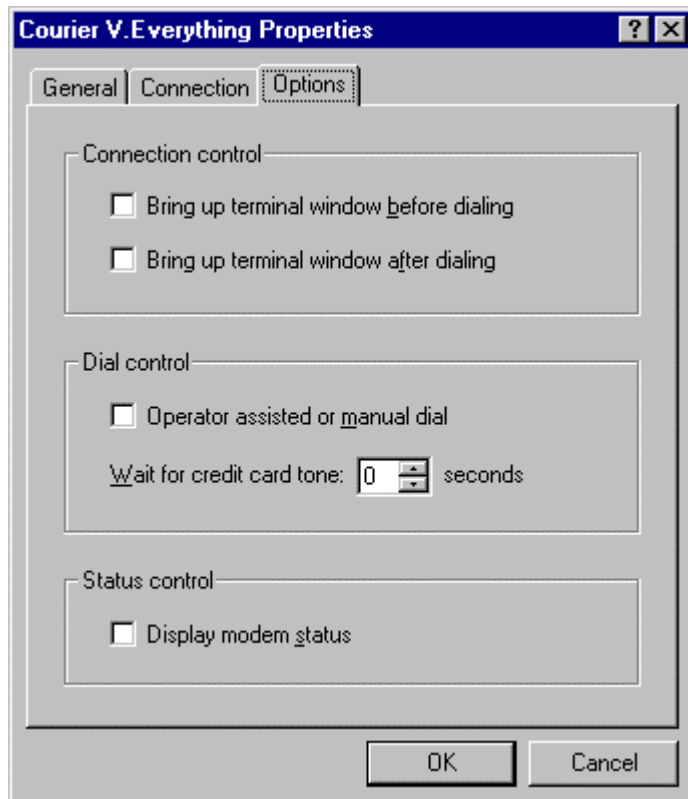
- 5 Leave the **Use FIFO buffers** field blank and click **OK**. See illustration below.



- 6 Click on the **Advanced...** button. In the **Advanced Connection Settings** panel, leave the fields at their default settings unless you want to change the **flow control** default. Click **OK**. See illustration below.



- 7 Click on the **Options** tab. Leave all boxes blank and click **OK** and **Next >**. See illustration below.

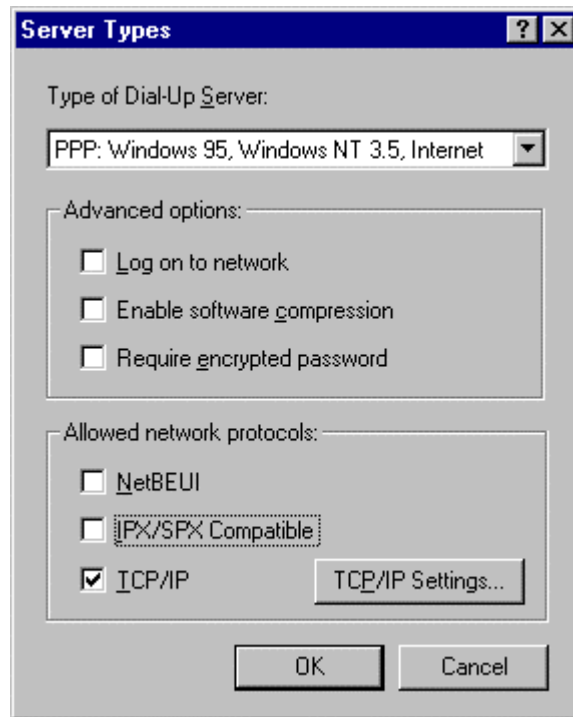


Back at the **Make New Connection** panel, enter a **Telephone number**, **Area code** and **Country Code**, (if necessary). Click on **Next >**. Click on **Finish**.

- 8 Hover over your new connection icon and click the *right* mouse button. Click on **Properties** from the menu that appears. See illustration below.



- 9 In the **My Connection** panel, click on **Server Type...** In the **Server Types** box, deselect all the check boxes except **TCP/IP** and click **OK** and **OK** again in **My Connection**. See illustration below.



- 10 Your new connection icon is added to the **Dial-Up Networking** screen. Double-click on the icon, select **Dial Properties...** and enter appropriate information. Click **OK**, and click **Connect**.

An Overview of NPC's Windows 95 Based Options

The following table lists NPC's Windows-based options. You may prefer the NCSI-compliant Windows Btty program to non-NCSI compliant *HyperTerminal*.

Option	Purpose
NCSI ELS Environment Program	This is the TSR (Terminate and Stay Resident) program file which is loaded upon Windows start-up allowing you to set up particular COM Port parameters to be used by the client software.
NCSIPort 95	This COM Port re-director re-routes Windows communications calls to the NCSI driver. NCSIPort 95 allows both 16 and 32-bit applications to access the NCSI interface.
Windows Btty	This option allows you to connect to the first available idle device dial-out port and issue AT commands to that modem or dial-out port.
Uninstall	This option un-installs, or removes, the Client software from your Windows environment and any related files.
Monitor	This option allows you to view the activity on a specified port.
Clist32 for Windows 95	This option displays the communications servers available for use by NCSI and IP Dial-out.
Security	This option allows you to password protect NCSI Client programs
NCSIPort Information	This option provides an overview of the NCSIPort program and instructions on its setup.

For more information on NCSI options, read the product documentation included in your package.

Dial-out Case Studies

This section provides examples of how to configure IP and TELNET dial-out service. Case Study A configures IP dialout with NCSI. Case Study B configures TELNET dial-out service without NCSI.

Case Study A

This configuration sets up IP dialout service on the HiPer ARC using the NCSI client to access the desired destination. The example assumes the following:

- user "surfer" is on a Windows 95 network
- HDM cards are installed in the Hub
- all basic system and network configuration is complete
- NCSI client software is loaded on surfer's PC
- NCSIPort parameters are configured
- user name "surfer" and password "dude" is supplied by the System Administrator
- A *Windows 95 Dial-Up Networking* session is configured for surfer
- Proper Windows *Network* settings are configured for surfer

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

- 1 If you don't wish to use existing default modem groups, add a *modem group* specifying *slot* and *interface* numbers. Type:

```
add modem_group boston interface slot:2/mod:1-24,slot:3/mod:12-24 ENTER
```

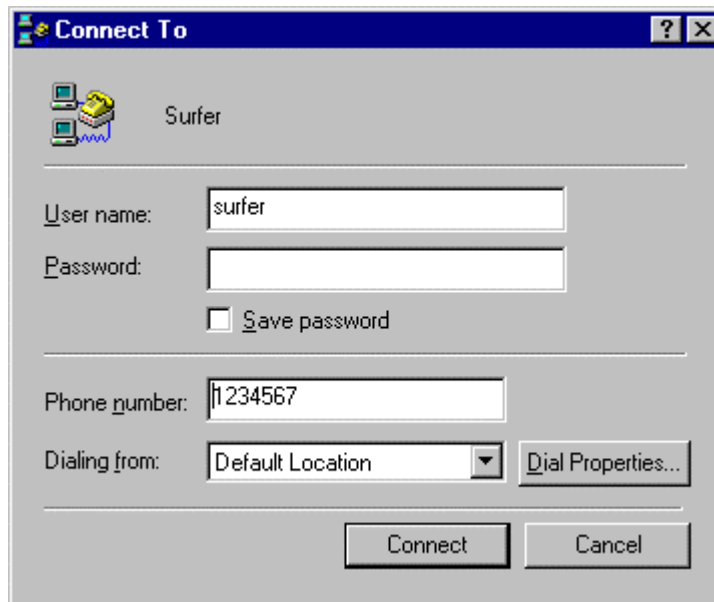
- 2 Configure the dial-out network service, specifying the *server_type* and mandatory *data* parameters:

```
add network service internet_service server_type dialout data "modem_group=\"boston\"" ENTER
```

- 3 Add user "surfer" *name*, *password* and *type*:
`add user surfer password dude type dial_out ENTER`
- 4 Set *global* dial-out service parameters to limit on-line usage. Be sure that *Security* is **disabled** on HiPer ARC - you'll enable *NCSI Security Login* below.
Type:
`set dial_out idle_timeout 2 recovery_timeout 2 security no ENTER`
- 5 Save your HiPer ARC configuration. Type:
`save all ENTER`
- 6 Double click on the **Port Set Up** icon in the NCSI95 icon group.
- 7 Select a *General* or *Specific* NCSI port on HiPer ARC by clicking on the displayed fields.
- 8 In the **Network Products Corp** icon group, click on the **Password Setup** icon shown on page 6-82. In the **Security Login** box, type a **User Name** and **Password** and click **OK**.
- 9 Click on your earlier-configured *Dial-Up Networking* icon (bringing up the screen shown on the next page) with a preconfigured user name and phone number and click on **Connect** to dial-out.



If you want a simple, NCSI-compliant terminal emulation session, select the Windows BTTY option in the NCSI icon group.



How it Works

The user accesses the HiPer ARC modem interface as the virtual COM4 port using IP via NCSI. The user is then queried for the name and password supplied by the Administrator and authenticated. Next, the user dials out to the destination of choice. If the call exceeds the specified timeout periods, the user is disconnected.

Case Study B

This configuration sets up TELNET dialout service on the HiPer ARC, using a modem to access the desired destination. The example assumes the following:

- user "rock" is on a Windows 95 PC
- Quad modem cards are installed in the Hub
- all basic system and network configuration is complete

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

- 1 If you don't wish to use existing default modem groups, add a *modem group*, specifying *slot* and *interface* numbers. Type:

```
add modem_group boston interface slot:4/mod:1-4 ENTER
```

- 2 Add user "rock" *name*, *password* and *type*:

```
add user rock password climber type dial_out ENTER
```

- 3 Configure the TELNET network dial-out service, specifying the *server_type*, *socket_number* and mandatory and optional *data* parameters. Type (abbr.):

```
ad ne se modems ser telnetd so 6666 da "service_type=dialout,login_banner=\"Hello\\n\\n\",  
modem_group=\"boston\\n\" ENTER
```

- 4 Save your configuration. Type:

```
save all ENTER
```

- 5 TELNET to Hiper ARC's IP address with a TCP Port number matching the socket number set earlier.

- WIN 95 users: from the **Start** icon, click on **Run** and, in the dialog box, type *telnet 199.56.203.5 6666* in the **Open** field as shown earlier.
- or, after opening the **Run** box, type *telnet* and click on **Connect** and click on **Remote System** to bring up the **Connect** box below. Replace TELNET with the socket number in the **Port** field, as shown on page 6-76.

- 6 Configured users are prompted to login and upon authentication can issue AT commands to the modem and either dial-out to a remote location or issue other commands as shown below.

For example:

```
atdt918479825092 ENTER
```

For example:

```
ati4 ENTER
```

How it Works

The TELNET user is configured to "share" a HiPer ARC modem allocated in a modem pool for dial-out service. The user is prompted to login and provide a password. Once the TELNET session is authenticated and established on the modem over the predetermined socket, the user dials out to a remote location via AT commands.

LAN-TO-LAN ROUTING

HiPer ARC can perform IP or IPX routing with a remote Hub or third-party router over analog/digital lines.



This chapter assumes that basic installation of all routing devices has already been performed, and that networks on the LAN (Ethernet) side of the Total Control Hub have been configured.

Figure 1 below depicts a typical LAN-to-LAN routing scheme.

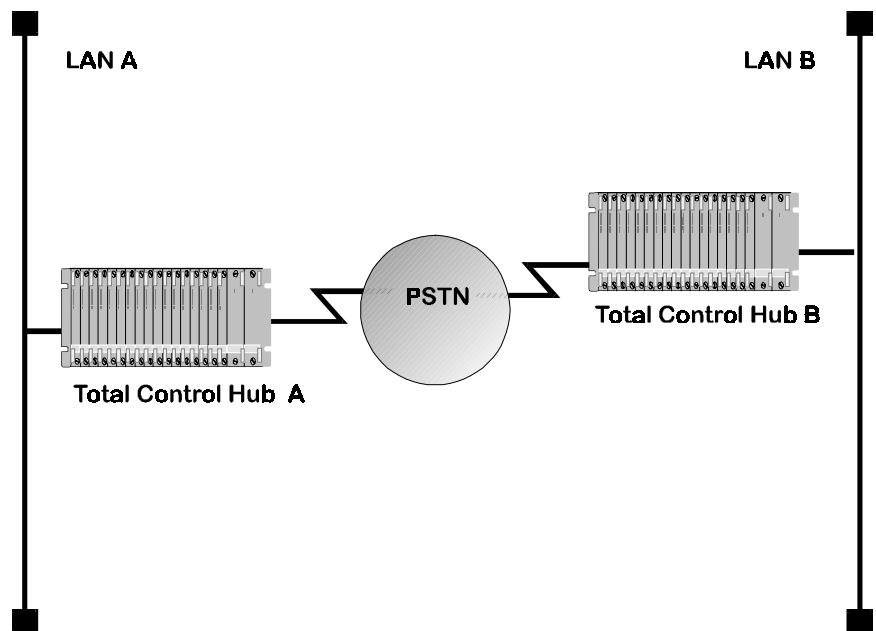


Figure 7-1 LAN-to-LAN Topology

LAN-to-LAN Routing Overview

The concept of users is not limited to end users who connect to the Total Control Hub from a terminal or PC. You can also configure users that represent remote routing devices. The remote routing device and the Hub work together to create a LAN-to-LAN routing link over analog or digital lines.

A remote routing device is defined as a network/dialout user by HiPer ARC. So, configuring a LAN-to-LAN routing connection is very similar to configuring a network user, with some additional dial-out and routing parameters such as:

- How the connection is established: on-demand, timed, continuous or manual

- How dynamic routing protocol packets (RIP and SAP) are handled
- What Dial-out scripts are used to connect to the remote location
- How bandwidth can be increased or decreased automatically

Connection Establishment

You can establish remote LAN connections in the following ways:

- *On-Demand* - An on-demand connection is established when a user attempts to access an address that is located at a remote site. The connection is closed after it has been idle for a specified interval.
- *Timed* - A timed connection is established and closed at a particular time of day.
- *Continuous* - A continuous connection is always open, as long as HiPer ARC is on-line.
- *Manual* - A manual connection is initiated by the system administrator using a **dial** command.

Dynamic Routing Settings

When HiPer ARC establishes a remote connection to a user (i.e., a user endstation) it is not usually necessary to send periodic router updates such as RIP and SAP messages. But, in a LAN-to-LAN connection, when the remote connection is to a routing device, these messages *may* be needed. HiPer ARC can be configured to send and receive these messages on a per "user" (router) basis for IP or IPX protocols. Be sure to "turn on" routing, though, since the default value is *none* (see instructions on page 7-100).

Dial-Out Scripts

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



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

Bandwidth Allocation

HiPer ARC can provide variable bandwidth automatically, depending on the amount of traffic delivered. This bandwidth allocation capability is provided using multi-link PPP (MLPPP).

It works this way. Every 5 seconds, PPP takes a sampling of network traffic, a snapshot that consists of the number of characters received on a bearer channel divided by its line speed (baud rate). This result is used to calculate the percentage of channel use during the sample. If that percentage is higher than the expansion value you specify, a second channel will be brought up.

If, on a second sample, line usage drops below the decrement value you set, the second bearer channel is dropped. The sampling interval is hard-coded and can not be changed but you can configure expansion and decrement thresholds to meet your system's needs. MLPPP is *on* by default with expansion/decrement defaults of 0.

IP Routing To perform IP routing, you should know the following:

- The IP address to be used for the point-to-point routing link. Both a local and remote address are specified for the configured user. You can use an un-numbered interface or a numbered interface:
 - *un-numbered interface* - defaults to address of HiPer ARC. The advantage is you save addresses
 - *numbered interface* - the traditional specification of an address for each end of the link



Some routers have an IP address assigned to each interface rather than one IP address for the entire device. If this is the case with your remote device, use the address of the interface you want to link to.

- The remote access protocol (PPP) HiPer ARC will use
- The remote system's netmask
- MTU for PPP is 1514, and is negotiated between the client and HiPer ARC
- Whether the remote device is set for TCP/IP (Van Jacobson) compression

IPX Routing Configure the user profile to specify a unique IPX network number that will represent the link between HiPer ARC and the remote device for the duration of the connection, or configure HiPer ARC to assign an IPX network number from a pool. You should know:

- IPX remote access sessions must use PPP
- MTU is 1500 and is negotiated between the remote device and HiPer ARC

Dynamic and Static Routes Fortunately, most networks do not require you to build routing tables manually. All IP/IPX networks can use a dynamic routing protocol that builds routing tables dynamically to reflect changing network conditions. Dynamic routing protocols supported by HiPer ARC include IP RIPv1 and RIPv2, and IPX RIP.

For example, network devices running RIP (either version) broadcast the destination addresses to which they can forward packets. Routing tables are built by listening to the broadcasts of other devices. If HiPer ARC does not periodically hear a broadcast for a given (dynamic) route, the route will be assumed unavailable and deleted from the table. Static routes remain in the table until removed by the administrator.

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

How Packets are Routed When HiPer ARC receives a packet, it looks up the packet's destination in its routing table. If a static route is found, the packet is sent to the gateway listed. If a static route is not found, the Hub will use a dynamic route. If the routing table contains no routes to the destination, it will send the packet to the specified defaultroute gateway. If no such gateway has been defined, the packet is discarded.

Establishing Connections to Remote Gateways

HiPer ARC can easily forward a packet to a gateway for which there is an established connection, such as a gateway on the same segment of the local LAN or at the other end of an active dial-up connection. All the Hub has to do in these situations is send the packet out the correct interface.

However, when there is no existing connection, HiPer ARC has to do a bit more work. When you define a dial-out user in HiPer ARC that is intended to connect to another routing device, the entry contains a list of remote gateways that HiPer ARC can dial into. When HiPer ARC does not have a connection to a packet's next hop, it looks up the address of the gateway in the user table.

The user table should contain a dial script and other information which tells HiPer ARC how to contact the remote location. Dial scripts are most useful for on-demand routing sessions. In these situations, HiPer ARC connects to a remote gateway only when it has packets queued for that location.

You can also create a defaultroute gateway as a means of reaching a remote network your router is not aware of by manually specifying such a gateway. Besides the advantage of successfully forwarding traffic across an unknown route, this approach avoids having to run RIP across the connection.

Configuring an Internal Network for Unnumbered Links

HiPer ARC provides a global or *internal* IP address for simple and secure network connectivity over an unnumbered link. We **recommend** this mechanism for:

- Administrators who want to maintain *connectivity* to remote networks even if a LAN interface goes down, and,
- Administrators who want to maintain a *uniform* view of the dial-in network - with users given the same local IP address (internal) and assigned remote IP addresses from a pool.

Configuring an internal address on the same network as your primary data interface will help ensure continued routing even if an Ethernet interface fails. And a single internal IP address can serve a supernet totaling dozens of IP addresses. Behind the scenes, the proxy arp protocol is utilized to sort out traffic going to remote and local hubs, automatically obtaining host IP addresses at the remote end of PPP or SLIP connections when their addresses match the network address portion of a LAN/WAN interface.

Spoofing

HiPer ARC supports spoofing between other Total Control chassis. Spoofing is a cost-saving way to make two sides of a disconnected circuit believe that the connection still exists in order to limit network traffic and maintain the advantages of on-demand service. HiPer ARC spoofs RIP broadcasts.

Authentication

HiPer ARC supports auto-detecting the PAP and CHAP methods of login authentication on PPP links.



HiPer ARC also provides comprehensive RADIUS authentication support for PPP connections. For more information on using RADIUS to provide authentication services, refer to Appendix E: RADIUS and TACACS+ Systems.

PAP Authentication

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

The Hub *will* respond to a dial-in PAP authentication request, though. All you need is a User Table entry for the remote device.

CHAP Authentication

CHAP is a bit different from PAP. Instead of actually sending a clear text password over the link, CHAP relies on a "shared secret", a password that both sides of the connection know, but never send. When a remote system requests CHAP authentication, the authenticating host replies with a challenge packet. The challenge packet contains (among other things):

- A user name for the host. The challenged system needs this to look up the correct "shared secret" password.
- A "challenge value" (a randomly generated string of characters).

The challenged system then concatenates the challenge value with the shared secret and passes the new string through a hashing algorithm. When the hashing algorithm forms a response based on this string, the challenged system replies with a packet containing both the response value and a user name.

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



Both ends of the connection must use the same hashing algorithm to work. HiPer ARC uses the MD5 or MD4 Microsoft (Win95) algorithm.

**Configuring
LAN-to-LAN Routing**

This section provides instructions and examples for setting the required parameters necessary to perform LAN-to-LAN routing. Since connecting to a remote LAN is really no different than connecting to a remote user station (with the requirement that a few more parameters be defined), remote LANs are simply defined as users.



For detailed information about CLI commands, refer to Chapter 10: Command Reference.

To configure a LAN-to-LAN routing connection:

- 1 Add the User. Create a standard network user, specifying the user's *type* of *dialout/network* and *password* (optional). Type:

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

Type A LAN-to-LAN user is always a dialout and network user type since HiPer ARC dials out to the remote router and performs framed network services.



It may be helpful now to issue the **show user** command to display the user's default parameters (labeled as **(D)**). This allows you to decide which parameters you need to set, and which parameters you can leave as defaults.

An example of a network/dialout user:

```
add user main_user password boston type dialout,network ENTER
```

- 2 Configure IP/IPX Network Parameters. Set network parameters you'll need for LAN-to-LAN routing. You do not need to specify *network service* since only *PPP* is supported for this link. Type:

```
set network user <name>IP or IPX
  header_compression [tcpip | none]
  mtu <number>
  spoofing <enable | disable>
  usage <enable | disable>
```

Header Compression Applies or turns off TCP compression to the header portion of the packet. The default is *TCPIP*

MTU The MTU specifies the size of the largest packet that may be sent to this location. The default is *1514*.

Spoofing Enables or disables spoofing. The default is *disable*.

Usage Turns IP or IPX on or off. Default: *enable*.

A network user example:

```
set network user main_user mtu 1000 spoofing enable ENTER
```

- 3 Specify a Remote Address. Unlike a remote end user connection, you must specify a remote IP address for the type of LAN-to-LAN connection you are configuring. You can choose an:
 - *un-numbered interface* - uses the HiPer ARC IP address with the advantage of saving IP addresses
 - *numbered interface* - uses the IP address of a specific port on the remote device

If you plan to run RIP over an *unnumbered* IP connection, we recommend you specify a global or *internal* IP address to the remote and local Hubs.

With this method, when an ondemand user is configured, the link between the Hubs comes up and RIP runs across it. The local Hub learns about any networks the remote Hub knows about. If no additional traffic needs to be sent the link comes down. When the local Hub has any traffic to send to the remote networks, the ondemand link comes up again and packets are sent. This global IP address is useful by letting RIP preserve awareness of remote networks even if a LAN interface goes down.

If you elect *not* to run RIP over an unnumbered link, you'll still configure a global IP address on both the remote and local HiPer ARC and, configure a framed route to each remote network on the remote Hub. When the user is enabled the framed routes are added to the Forwarding Table.

So if the local Hub has any traffic to send to these networks the ondemand link will come up and the packets be sent.

An IPX address requires an eight numeral number of the remote network.

Remote IP Address Sets the IP address a user accesses on a remote system. This, also, is the remote system's *local* IP address, set by **set dialout user**.

For a remote IP connection, the IP network address is assigned to a client in the format *nnn.nnn.nnn.nnn*, with or without a mask specifier. The mask specifier can be in IP address format (255.0.0.0 or greater and contiguous) or 'A', 'B', 'C', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If setting a *user's* IP address, the mask specifier is set to 'H' (for Host) or a numeric value of 32. If you do not specify a mask, the system will generate it for you from the network address. The default is **0.0.0.0/H**



You can set this value with **either** of the following commands:

```
set network user <name> ip
    remote_ip_address <host_name or ip_address of remote network/mask_specifier>
set dialout user <name> site
    remote_ip_address <host_name or ip_address of remote network/mask_specifier>
```

Remote IPX Address Configures the remote IPX network address in the format *xxxxxxx. fffffff* or *fffffffe* values are prohibited. Use this command:

```
set network user <name> ipx address <ipx network address>
```

Global IP Address To specify a *global* (internal) IP address and enable routing on the LAN where the HiPer ARC exists, use the following commands.



*Important: If more than one HiPer ARC exists on your LAN, **do not** specify identical internal IP addresses for them.*

```
add ip network <name>
    interface internal
    address <IP_address of remote HiPer ARC>

set ip network <name>
    routing_protocol [ripv1 | ripv2 | none]
```



*You can verify the newly added internal network by issuing **list interfaces**. Issuing **show ip settings** will also display this internal network. But, be aware that if you do not configure a global IP network, the IP System Host Address displayed by **show ip settings** will be the IP address of the first Ethernet interface enabled on your system.*

Framed Route User Add this user when using an unnumbered link:

```
add framed_route user <name>
    gateway <host_name or IP_address of remote HiPer ARC>
    ip_route <host_name or IP_address of remote network>
    metric <number>
```



You should run RIP when setting up a global IP network if you intend to support a TCP service such as TELNET. Without RIP on the internal network, you will not learn of remote networks should the Ethernet interface be disabled.

Examples of remote IP and IPX addresses:

```
set network user main_user remote_ip_address 244.175.124.243/c ENTER
```

```
set network user name main_user ipx address ffff111f ENTER
```

- 4 Set the Remote Device Phone Number and Modem Group. Specify the remote device's *phone number* and *modem group* using the following command. Setting a modem group lets you allocate modems use. Specify a *default* modem group (e.g.: *slot:4*) or create one with the **add modem_group** command.

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

Optionally, specify an *alternate phone number* that HiPer ARC will dial if it cannot connect using the primary phone number. Use the following command:

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

For example (abbr.):

```
set user main_user phone 5555555555 modem slot:4 alternate 6666666666 ENTER
```



*Dial scripts specified with the **set user** command are **not** used in conjunction with phone and alternate phone numbers specified here. You can specify either one or the other value - not both.*

- 5 Configure Dialout Parameters. Dialout parameters determine how HiPer ARC initiates and handles the dialout connection to the remote router. Use the following command as well as the **set user** command described later:

```
set dialout user <name> site
address_selection specified
type [on_demand | timed | manual | continuous]
start_time <hh:mm:ss>
end_time <hh:mm:ss>
```



*When a remote IP address is configured, address selection is automatically set to **specified**. Assign and negotiate parameters are not applicable.*

Type Determines when HiPer ARC will dial out to the remote device. The default is *manual*. Choices are:

- *On Demand* - HiPer ARC dials out to the remote device when it has packets queued for that location. It then maintains the connection as long as there is traffic on the line, closing the link when the *idle timeout* lapses. Note that dynamic routing information is updated while there is a connection between the two devices, but not before HiPer ARC dials or after it hangs up unless *spoofing* is on.
- *Timed* - HiPer ARC dials out at the time of day that you specify. See the *start time* and *end time* parameters for more information.
- *Manual* - (Useful for troubleshooting). The Hub dials out only when it receives a **dial** command from the CLI. See *Chapter 10: Command Reference* for more information on the dial command.
- *Continuous* - The Hub will attempt to maintain the connection at all times. If the connection is broken it will dial again.

Start Time Specifies the time to start a timed connection in *hours:minutes:seconds*. The default is *00:00:00* (connection always up).

End Time Specifies the time to end a timed connection in *hours:minutes:seconds*. The default is *00:00:00* (connection always up).

Idle Time-out - Configured with the set user command Applies to *manual* and *ondemand* locations only. These values configured using the **set user** command specify the interval a dial out connection can remain idle (no packets sent or received) or how long the user session can last before HiPer ARC disconnects. The idle timer ignores RIP, SAP and keepalive packets, allowing ports to time-out even though RIP is running. The default is *0* (not active). Range: *1-86,400 seconds*. If spoofing is enabled, though, it accomplishes the same purpose as setting an idle or session timeout.



You must set the Idle Time-out field to something other than its default (no time-out) for on-demand sites. If not, the initial connection always stays up.

Use the following additional command for time-out values:

```
set user <name> idle_timeout <hh:mm:ss> session_timeout <hh:mm:ss>
```

An example of a dialout user configuration with the addition of time-outs:

```
set dialout user main_user site type on_demand start_time 05:00:00 end_time 17:00:00 ENTER
```

```
set user main_user idle_time 00:03:00 session_timeout 00:20:00 ENTER
```

- 6 Configure IP/IPX Routing Parameters. These values set periodic router updates (RIP and SAP) parameters on a per user basis, “turning on” the type of routing you prefer. Use these commands:

```
set network user <name> ip
  default_route_option [disable | enable]
  rip [ripv1 | ripv2]
  rip_authentication_key [string]
  rip_policies_update [see Chapter 11: Command Reference]
  routing [listen | send | both | none]
  usage enable
```

```
set network user <name> ipx
  rip_age_multiplier [1-1080]
  rip_update [1-500]
  routing [all | listen | send | respond | none]
  sap_age_multiplier [1-1080]
  sap_update [1-500]
  usage [disable | enable]
  wan [enable | disable]
```

Default Route Automatically sets the IP address of a remote default route gateway. If your destination is remote, and the router is unaware of the remote network, and you do not wish to run RIP, select *enabled*. Default: *disabled*

RIP Specifies the RIP version used for IP. The default is *RIPv1*.

RIP Authentication Key Authorizes RIP updates using a stored password with a maximum string length of *64 ASCII* characters

IP/IPX Routing Sets the level of RIP messaging the devices exchange on a connection. For IP routing, you **must** select *listen*, *send* or *both* since the default is *none*. The IPX routing options are similar although the default is *respond*.



IP routing need not be set on a user basis when setting an unnumbered link.

- *Listen* - Listen for RIP (IPX: & SAP) packets destined for nets (but not send)
- *Send* - Transmits RIP (IPX: & SAP) packets destined for the remote network (but not listen)
- *Both (IPX: All)* - Listen for and send RIP (IPX: & SAP) packets to remote nets
- *None* - Ignore all RIP (IPX: & SAP) packets. **Default**
- *Respond (IPX)* - if requested, will send RIP & SAP packets to remote networks



*IP users: Be sure to activate RIP on **both** sides of the WAN, otherwise it will not work. Also, if IP routing is set to **none**, you will need to enter static routes to networks not directly connected.*



A user dialing up the Internet typically would not want to run RIP, while a user making a LAN-to-LAN connection would.

Usage Enables or disables the IP or IPX protocol. Both are *on* by default.

Rip and SAP Age Multiplier These parameters set a holding multiplier for data received in RIP/SAP periodic updates. The default is 4.

RIP and SAP Update These values configure an interval, in seconds, between RIP/SAP periodic updates. The default for both parameters is 60.

WAN Enables/disables the IPX WAN protocol which is used between two IPX networks negotiating the network number for a WAN connection. Both ends of the connection must enable this protocol for it to work. The default is *disabled*

Examples of IP and IPX routing with most defaults retained:

```
set network user main_userip rip_authentication_key secret routing both ENTER
```

```
set network user main_user ipx rip_update 350 routing listen sap_update 350 wan enable ENTER
```

- 7 Configure Dialing Scripts - *Optional*. You can configure up to six send and reply scripts per connection. Send/reply scripts specify modem commands to establish and close remote connections.



*Dial scripts specified with **set user** are **not** used in conjunction with phone/alternate phone numbers. Specify either one or the other value - **not both**.*

Set up dialing scripts using the following command:

```
set dialout user <name>
  send1_script <"string">
  send2_script <"string">
  send3_script <"string">
  send4_script <"string">
  send5_script <"string">
  send6_script <"string">
  reply1_script <"string">
  reply2_script <"string">
```

```

reply3_script <"string">
reply4_script <"string">
reply5_script <"string">
reply6_script <"string">

```

- 8 Configure PPP Parameters. If you are using PPP, configure several PPP-specific values with this command:

```

set network user <name> ppp
channel_decrement <0-100%>
channel_expansion <0-100%>
compression_algorithm [ascend | auto | microsoft | none | stac]
expansion_algorithm [linear | constant]
max_channels <maximum number of channels used>
min_size_compression <0-2048>
receive_acc_map <hexadecimal value - array of 4 bytes>
transmit_acc_map <hexadecimal value - array of 4 bytes>
reset_mode_compression [auto | every_packet | every_error]

```

Channel Decrement Sets the channel decrement *percentage*. For Quad modem cards, when second channel usage drops below this percentage, PPP will use the first channel only. For HDM cards, when usage of up to 16 channels drops below this percentage, PPP uses fewer channels. Since the default is *0*, *all* channels are available for use until you set this value. Recommended setting: *20*

Channel Expansion Sets the channel expansion *percentage*. For Quad modem cards, when first channel usage exceeds this percentage, PPP adds a second channel. For HDM cards, when first channel usage exceeds this percentage, PPP add ups to 16 additional channels. Since the default is *0*, *all* channels are available for use until you set this value. Recommended setting: *60*

Compression Algorithm Specifies which proprietary algorithm PPP negotiates to use for compression. The default is *auto*, which automatically chooses the method satisfactory to both sides of the link. *Ascend*, *Microsoft*, *Stac* and *None* are the other choices.

Expansion Algorithm Specifies which type of expansion algorithm is used to handle bandwidth allocation. Each algorithm measures traffic bandwidth over 60 second intervals. Use *constant* if you want to take a conservative approach to bandwidth allocation and not react to short-term bandwidth changes. Use *linear* if you want to measure more current, higher weight traffic when allocating bandwidth. The default is *constant*.

Maximum Channels Specifies the maximum number of channels this user can use. This value either invokes PPP to negotiate for multilink PPP with the remote system (more than 1) or does not try to negotiate for multi-link PPP (1). The default is 2. If using Quad modem cards, you are limited to four channels per card. If using HDM cards, you can employ up to 16 channels (modems) per card for multilink provided you've provisioned your phone service.

Minimum Compression Size Specifies the minimum size at which PPP compresses a packet. Data packets smaller than this value are not compressed. The default value is 256.

Receive Asynchronous Character Control Map Determines whether HiPer ARC uses the asynchronous control character map to filter incoming data. The default value is *ffffff*.

Transmit Asynchronous Character Control Map Determines whether HiPer ARC uses the asynchronous control character map to filter outgoing data. The default value is *ffffff*.

Reset Compression Mode Determines how often PPP should examine packets to decide when to re-negotiate the optimum compression algorithm. The default is *auto*.

A network user example with MLPP and bandwidth allocation enabled (abbr.):

```
set net us main_user ppp channel_d 20 channel_e 60 max 16 co stac ex lin min 200 ENTER
```

- 9 Configure PAP/CHAP Authentication Parameters. You can set PAP and CHAP-related authentication parameters using the following commands:

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

```
set system transmit_authentication_name <remote_user_name> name <system_name>
```

```
set network user <name> send_password <password>
```

PAP or CHAP Authentication By default, HiPer ARC is configured *globally* to accept **either** PAP or CHAP authentication for PPP connections. For example:

```
set ppp receive_authentication pap ENTER
```

Set System Authentication Name This *name* is sent to the remote system for authentication. It is needed by PPP, which requires a *user* at the remote system with the *same authentication name*. It is employed when HiPer ARC receives a challenge while making a PPP connection to a remote system or router over the WAN. For example:

```
set system transmit_authentication_name main_user name main_office ENTER
```

Send Password This parameter is needed for a two-way LAN-to-LAN routing connection. It must match the password specified by the user at the remote location. For example:

```
set network user branch_user send_password boston ENTER
```

- 10 Save Your Work. Use the following command:

```
save all ENTER
```

LAN-to-LAN Routing Case Study

This case study provides an example of how to set up two Total Control Hubs located on separate LANs to perform LAN-to-LAN routing over a dial-up PPP link. The diagram below depicts two LANs connected by two Hubs: *main_office* and *branch_office*. This configuration enables the IP protocol to be routed across a standard PPP link with CHAP/PAP authentication. Users of the type *specified* (with remote and local IP addresses configured on numbered or unnumbered networks) can make dial up, *on-demand* calls to *modem groups* on either side of the connection. *Spoofing* is activated to contain expenses and *multilink PPP* enabled if necessary to maximize channel utilization of the HDM cards. The configuration can then be tested by manually dialing out or pinging either HiPer ARC.

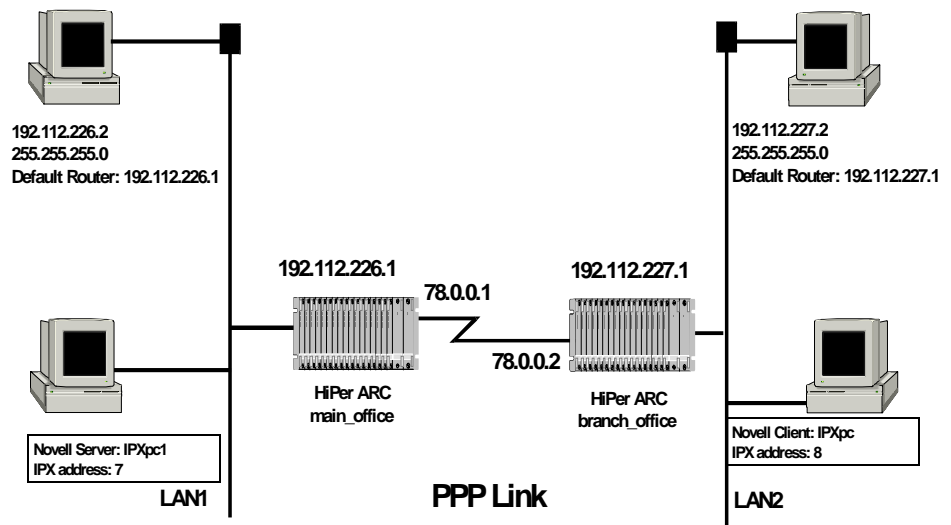


Figure 7-2 Sample LAN-to-LAN Routing Case with a Numbered IP Network

Assumptions This case study assumes the following:

- HiPer ARC's Main Office system name is *main_office*
- HiPer ARC's Branch Office system name is *branch_office*
- HiPer ARC main_office is on LAN1, the main data center of the company
- HiPer ARC branch_office is on LAN2, a remote office
- HiPer ARC main_office establishes an on-demand link to HiPer ARC branch_office, and vice versa
- A user configured on each HiPer ARC, each of which is supplied with a password known to the opposite HiPer ARC, negotiates the connection
- Each Hub is populated with *HDM-24* cards
- Enough phone numbers are provisioned by the phone company to support multilink PPP (optional)
- If traffic on the connection becomes too great, HiPer ARC main_office will open additional channels; if traffic on the connection diminishes, HiPer ARC main_office will close those channels
- Each Hub is populated with *one* HiPer ARC

Configuring HiPer ARC main_office

Configuration of HiPer ARC *main_office* is broken down into these sections:

- Configuring LAN Networks
- Adding User Parameters
- Configuring Connection Parameters
- Setting Authentication
- Configuring Multilink PPP - Optional
- Saving the Configuration
- Testing the Connection - Optional
- Capsule Summaries A, B and C

Configuring LAN Networks

Follow these steps to establish an IP network on HiPer ARC *main_office*'s LAN interface (eth:1):

- 1 Add an *IP network* called "ipnet-1" with the class C IP address 192.112.226.1, ethernet_II frame type on interface eth:1:. Type:

```
add ip network ipnet-1 address 192.112.226.1/c interface eth:1 ENTER
```



Since the default network frame type is ethernet_II, you do not need to set it.

- 2 Add an *IPX network* called "ipxnet-1" with the IPX address 7, ethernet_II frame type on eth:1:. Type:

```
add ipx network ipxnet-1 address 7 interface eth:1 ENTER
```

- 3 Configure the LANs on which HiPer ARC *main_office* reside to do routing. Type:

```
set ip network ipnet-1 routing ripv1 ENTER
```

```
set ipx network ipxnet-1 routing on ENTER
```

Adding User Parameters

Follow these steps to add a user:

- 1 Add "branch_user" of *network/dial-out* user type with the password "chicago".

```
add user branch_user password chicago type network,dialout ENTER
```

- 2 Set the user's *remote IP address* to 78.0.0.2 and *IPX address* to 8. This command assumes you want to configure a numbered network. If you'd prefer to set up an unnumbered network, see the note below.

```
set network user branch_user ip remote_ip_address 78.0.0.2 ENTER
```

```
set network user branch_user ipx address 8 ENTER
```



Alternatively, you can configure an unnumbered IP network by specifying the IP address of HiPer ARC branch_office (192.112.227.1). We recommend that if you want unnumbered links you set an internal interface and enable RIP. Type:

```
add ip network branch_office interface internal address 192.112.227.1/32 ENTER
```

In addition, if you do not plan to run RIP over an unnumbered link, you will still configure a global IP address to the remote HiPer ARC and configure a framed route to each remote network on the remote Hub. Type:

```
add framed_route user branch_user gateway 192.112.227.1 ip_route 192.112.227.2/32 metric 1 ENTER
```

If you specify HiPer ARC's IP address with either method above, your user supports IPX only, or you want an unnumbered IP link, skip step 3.

- 3 Set the user's *local IP address* to 78.0.0.1:

```
set dialout user branch_user local_ip_address 78.0.0.1 ENTER
```

- 4 Configure the user to *listen* for RIP packets destined for main_office's networks and send RIP packets destined for branch_office's networks. But, if you've configured an unnumbered network, skip this step.

```
set network user branch_user ip routing both ENTER
```

```
set network user branch_user ipx routing all ENTER
```

- 5 Specify *phone number* and *modem_group* to use for branch_office. The modem groups used below are *default* groups.

```
set user branch_user phone_number 5085555555 modem_group slot:1,slot:2 ENTER
```

Configuring Connection Parameters

Connection parameters determine how the LAN-to-LAN connection is handled by HiPer ARC. Follow these steps:

- 1 Configure the user as an *on-demand* user. Type:

```
set dialout user branch_user site type ondemand ENTER
```

- 2 Enable *spoofing* to fully benefit from the ondemand connection. Type:

```
set dialout user branch_user site spoofing enable ENTER
```

Setting Authentication

Configure authentication parameters. This example sets *PAP* authentication on *both* sides of the link (you may also choose *CHAP*, *either* or *none*):

- 1 Specify the *system authentication name* to match the name of the *user* (main_user) created on the remote HiPer ARC and *name* for this HiPer ARC:

```
set system transmit_authentication_name main_user name main_office ENTER
```

- 2 Set the authentication *type* to PAP:

```
set ppp receive_authentication pap ENTER
```

- 3 Set branch_user user's authentication *password* to correspond to remote main_user's password:

```
set network user branch_user send_pass boston ENTER
```

Configuring Multilink PPP - Optional

Enable MLPPP for user branch_user. Type:

```
set network user branch_user ppp channel_decrement 20 channel_expansion 60 max_channels 16 ENTER
```

Saving the Configuration

Save your configuration using the following command:

```
save all ENTER
```

Testing the Connection - Optional

Test your configuration by performing a *manual* dialout to bring up the connection or, additionally, issuing **ping** commands. Follow the steps below:

- 1 Manually dialup the remote HiPer ARC. Type:
`dial branch_office ENTER`
- 2 Test a dynamic dialout by pinging the remote HiPer ARC. Type:
`ping branch_office ENTER`

Configuring HiPer ARC branch_office

Configuration of HiPer ARC branch_office is very similar to HiPer ARC main_office configuration, except for some network address and user values.

Configuring LAN Networks

Set an *IP network* on HiPer ARC branch_office's LAN interface (eth:1) as follows:

- 1 Add an *IP network* called "ipnet-2" with the Class C IP address 192.112.227.1, ethernet_II frame type on interface eth:1:
`add ip network ipnet-2 address 192.112.227.1/c frame eth interface eth:1 ENTER`
- 2 Add an *IPX network* called "ipxnet-2" with the IPX address 8, ethernet_II frame type on eth:1:. Type:
`add ipx network ipxnet-2 address 8 interface eth:1 ENTER`
- 3 Set the LAN on which HiPer ARC branch_office resides to do routing. Type:
`set ip network ipnet-2 routing ripv1 ENTER`
`set ipx network ipxnet-2 routing on ENTER`

Adding User Parameters

Follow these steps to add a user:

- 1 Add "main_user" of *network/dial-out* user type with the password "boston":
`add user main_user password boston type network,dialout ENTER`
- 2 Set the user's *remote IP address* to 78.0.0.1 with a Class A address mask and *IPX address* to 7:
`set network user main_user ip remote_ip_address 78.0.0.1/a ENTER`
`set network user main_user ipx address 7 ENTER`



Alternatively, you can configure an unnumbered IP network setup by specifying the IP address of HiPer ARC branch_office (192.112.227.1). We recommend that if you are using unnumbered links you configure a global (internal) interface and enable RIP. Use this command:

```
add ip network main_user interface internal address 192.112.226.1/32 ENTER
```

In addition, if you do not plan to run RIP over an unnumbered link, you will still configure a global IP address to the remote HiPer ARC as well as configure a framed route to each remote network on the remote Hub. Type:

```
add framed_route user main_user gateway 192.112.226.1 ip_route 192.112.226.2/32 metric 1 ENTER
```

If you specify HiPer ARC's IP address with either method above, the user supports IPX, or you want an unnumbered IP link, skip step 3 below.

- 3 Set the user's *local IP address* to 78.0.0.2:

```
set dialout user main_user local_ip_address 78.0.0.2/a ENTER
```

- 4 Configure the user to *listen* for RIP packets headed to HiPer ARC branch_office's networks and send RIP packets destined for HiPer ARC main_office's networks. But, if you've set an unnumbered network, skip this step.

```
set network user main_user ip routing both ENTER
```

```
set network user main_user ipx routing all ENTER
```

- 5 Specify *phone number* and *modem_group* to use for main_office. The modem groups used below are *default* groups.

```
set user main_office phone_number 5085556666 modem_group slot:3,slot:4 ENTER
```

Configuring Connection Parameters

Connection parameters determine how the LAN-to-LAN connection is handled by HiPer ARC. Follow these steps:

- 1 Configure the user as an *on-demand* user type:

```
set dialout user main_user site type ondemand ENTER
```

- 2 Enable spoofing to fully benefit from the ondemand connection. Type:

```
set network user main_user spoofing enable ENTER
```

Setting Authentication

This example uses *PAP* authentication on *both* sides of the link (you may also choose *CHAP*, *either* or *none*):

- 1 Set the *system authentication* name to match the name of the *user* (branch_user) created on the remote HiPer ARC and *name* for this HiPer ARC:

```
set system transmit_authentication_name branch_user name branch_office ENTER
```

- 2 Set the authentication *type* to PAP:

```
set ppp receive_authentication pap ENTER
```

- 3 Set main_user's *authentication password* to match remote branch_office user's password:

```
set network user main_user send_pass chicago ENTER
```

Configuring Multilink PPP - Optional

Enable MLPPP for user main_user. Type:

```
set network user main_user ppp channel_decrement 20 channel_expansion 60 max_channels 16 ENTER
```

Saving the Configuration

Save your configuration using the following command:

```
save all ENTER
```


Testing the Connection - Optional

Test your configuration by performing a *manual* dialout to bring up the connection or, additionally, issuing **ping** commands. Follow the steps below:

- 1 Manually dialup the remote HiPer ARC. Type:
`dial main_office ENTER`
- 2 Test a dynamic dialout by pinging the remote HiPer ARC. Type:
`ping main_office ENTER`

Capsule Summary A

This script is one possible configuration derived from the previous section. Issue the following commands to build this IP/IPX LAN-to-LAN with single HiPer ARC and HDM cards installed on each Hub, all modems on slots 1-4 enabled, a numbered network, multilink PPP, RIPv1 routing and PAP authentication set.

HiPer ARC main_office

```
add ip network ipnet-1 address 192.112.226.1/c interface eth:1 ENTER
set ip network ipnet-1 routing ripv1 ENTER
add ipx network ipxnet-1 address 7 interface eth:1 ENTER
set ipx network ipxnet-1 routing on ENTER
add user branch_user password chicago type network,dialout ENTER
set network user branch_user ip remote_ip_address 78.0.0.2 ENTER
set network user branch_user ipx address 8 ENTER
set dialout user branch_user local_ip_address 78.0.0.1 ENTER
set network user branch_user ip routing both ENTER
set network user branch_user ipx routing all ENTER
set user branch_user phone_number 5085555555 modem_group slot:1,slot:2 ENTER
set dialout user branch_user site type ondemand ENTER
set dialout user branch_user site spoofing enable ENTER
set system transmit_authentication_name main_user name main_office ENTER
set ppp receive_authentication pap ENTER
set network user branch_user send_pass boston ENTER
set network user branch_user ppp channel_decrement 20 channel_expansion 60 max_channels 16 ENTER
save all ENTER
dial branch_office ENTER
ping 78.0.0.2 ENTER
```

HiPer ARC branch_office

```
add ip network ipnet-2 address 192.112.227.1/c frame eth interface eth:1 ENTER
set ip network ipnet-2 routing ripv1 ENTER
add ipx network ipxnet-2 address 8 interface eth:1 ENTER
set ipx network ipxnet-2 routing on ENTER
add user main_user password boston type network,dialout ENTER
set network user main_user ip remote_ip_address 78.0.0.1/a ENTER
set network user main_user ipx address 7 ENTER
set dialout user main_user local_ip_address 78.0.0.2/a ENTER
set network user main_user ip routing both ENTER
set network user main_user ipx routing all ENTER
set user main_office phone_number 5085556666 modem_group slot:3,slot:4 ENTER
set dialout user main_user site type ondemand ENTER
set network user main_user spoofing enable ENTER
set system transmit_authentication_name branch_user name branch_office ENTER
set ppp receive_authentication pap ENTER
set network user main_user send_pass chicago ENTER
set network user main_user ppp channel_decrement 20 channel_expansion 60 max_channels 16 ENTER
save all ENTER
```

Capsule Summary B This script is another possible configuration derived from the previous section. Issue the following commands to build this LAN-to-LAN with dual HiPer ARC and HDM cards installed on each Hub, all modems on slots 1 and 2 enabled, an unnumbered network created, CHAP authentication configured, and multilink PPP and RIP disabled.

HiPer ARC main_office

```
set chassis slot 1 card_type quad_modem owner yes ports 24 ENTER
add ip network ipnet-1 address 192.112.226.1/c interface eth:1 ENTER
add user branch_user password chicago type network,dialout ENTER
set network user branch_user ip remote_ip_address 192.112.227.1/c ENTER
set user branch_user phone_number 5085555555 modem_group slot:1 ENTER
set dialout user branch_user site type ondemand ENTER
set system transmit_authentication_name main_user name main_office ENTER
add framed_route user branch_user gateway 192.112.227.1 ip_route 192.112.227.2/32 metric 1
set ppp receive_authentication chap ENTER
set network user branch_user send_pass boston ENTER
set network user branch_user ppp max_channels 1 ENTER
save all ENTER
dial branch_office ENTER
ping 192.112.227.1 ENTER
```

HiPer ARC branch_office

```
set chassis slot 2 card_type quad_modem owner yes ports 24 ENTER
add ip network ipnet-2 address 192.112.227.1/c frame eth interface eth:1 ENTER
add user main_user password boston type network,dialout ENTER
set network user main_user ip remote_ip_address 192.112.226.1/c ENTER
set user main_office phone_number 5085556666 modem_group slot:2 ENTER
set dialout user main_user site type ondemand ENTER
set system transmit_authentication_name branch_user name branch_office ENTER
add framed_route user main_user gateway 192.112.226.1 ip_route 192.112.226.2/32 metric 1
set ppp receive_authentication chap ENTER
set network user main_user send_pass chicago ENTER
set network user main_user ppp max_channels 1 ENTER
save all ENTER
```

Capsule Summary C

This script is another possible configuration derived from the previous section. Issue the following commands to build this LAN-to-LAN with dual HiPer ARC and HDM cards installed on each Hub, all modems on slots 1-4 enabled, and an unnumbered network, framed users added, CHAP authentication configured, and RIP and multilink PPP disabled.

HiPer ARC main_office

```
set chassis slot 1-4 card_type quad_modem owner yes ports 4 ENTER
add ip network ipnet-1 address 192.112.226.1/c interface eth:1 ENTER
set ip network ipnet-1 routing ripv2 ENTER
add user branch_user password chicago type network,dialout ENTER
set network user branch_user ip remote_ip_address 192.112.227.1/c ENTER
set user branch_user phone_number 5085555555 modem_group slot:1-4 ENTER
set dialout user branch_user site type ondemand ENTER
set dialout user branch_user site spoofing enable ENTER
set system transmit_authentication_name main_user name main_office ENTER
set ppp receive_authentication chap ENTER
set network user branch_user send_pass boston ENTER
set network user branch_user ppp max_channels 1 ENTER
save all ENTER
dial branch_office ENTER
ping 192.112.227.1 ENTER
```

HiPer ARC branch_office

```
set chassis slot 5-8 card_type quad_modem owner yes ports 4 ENTER
add ip network ipnet-2 address 192.112.227.1/c frame eth interface eth:1 ENTER
set ip network ipnet-2 routing ripv2 ENTER
add user main_user password boston type network,dialout ENTER
set network user main_user ip remote_ip_address 192.112.226.1/c ENTER
set user main_office phone_number 5085556666 modem_group slot:5-8 ENTER
set dialout user main_user site type ondemand ENTER
set network user main_user spoofing enable ENTER
set system transmit_authentication_name branch_user name branch_office ENTER
set ppp receive_authentication chap ENTER
set network user main_user send_pass chicago ENTER
set network user main_user ppp max_channels 1 ENTER
save all ENTER
```

Introduction

HiPer ARC supports two, largely similar methods of tunneling IP/IPX traffic: the Layer Two Tunneling Protocol (L2TP), an open tunneling protocol, and the Point-to-Point Tunneling Protocol (PPTP), the Microsoft protocol supporting connections to a Windows NT host.

These protocols provide a path and secure environment for PPP sessions over a Virtual Private Network (VPN). By creating a L2TP or PPTP tunnel, HiPer ARC extends a dial-in user's PPP session across a TCP/IP network without granting access to that network. This allows a private network to set up a host with the power to grant or deny access to that user as if the host were the Network Access Server terminating the user's call.

HiPer ARC also supports another kind of tunneling using the Virtual Tunneling Protocol (VTP). This protocol is employed by multiple HiPer ARC clients when Multi-link PPP traffic is passed between them and a HiPer ARC server. VTP is used in conjunction with the Multi-link PPP Interspan Protocol (MPIP) which allows links of a PPP Multilink bundle to be physically terminated at different HiPer ARCs on the network - VTP tunnels channel these links logically to a single HiPer ARC. While L2TP can support multi-link PPP, it doesn't support MPIP.

This chapter provides instructions to configure the following protocols:

- L2TP
- PPTP
- MPIP

Using L2TP

The Layer Two Tunneling Protocol (L2TP) provides "virtual dial-up" - the tunneling of PPP client sessions to a host network server located across the Internet from the HiPer ARC where clients initially connect. This flexible topology provides:

- non-proprietary, multi-protocol sharing of network resources such as modems, Remote Access Servers and ISDN routers
- the use of *unregistered IP* and private IPX addresses
- the placement of *local* calls by clients
- *multilink PPP* support even for physically dispersed Remote Access Servers
- end-system transparency for remote clients and their home-site hosts
- various types of authentication support (MS-CHAP, PAP, EAP)
- addressing and authorization by the home site, not the ISP
- RADIUS and TACACS+ support for those requiring it

How it Works

A remote client dials into a HiPer ARC serving as the L2TP Access Concentrator (LAC) and initiates an asynchronous or synchronous PPP connection through the Internet over either a Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN). HiPer ARC establishes the PPP link and begins authentication of the client based on its user name and a specified endpoint - the L2TP Network Server (LNS). After authentication is accepted, client data is passed to the LNS (another HiPer ARC or any Network Access Server) and this host either accepts or rejects the dialup call. See illustration below.

Then, using the User Datagram Protocol (UDP), a tunnel (defined as a LAC-LNS pair) to a specified LNS is initiated. Once the tunnel is up, control messages are passed between the LAC-LNS to manage the tunnel. An unused slot within the tunnel - a session - is then prompted from the LNS, as well as authentication data. If the LNS successfully authenticates the dialup session a second time (using CHAP, PAP or MS CHAP) a virtual interface for PPP is created, allowing the passage of packets through the tunnel in both directions.

At this point, connectivity is established via a point-to-point PPP session whose endpoints are the remote user's networking application on one end and the termination of this connectivity at the LNS's PPP support on the other. Because the remote user has become simply another dial-up client of the LNS, client connectivity can now be managed using traditional methods of authorization, protocol access, and packet filtering. Accounting can be performed on both the HiPer ARC (LAC) and host network server (LNS).

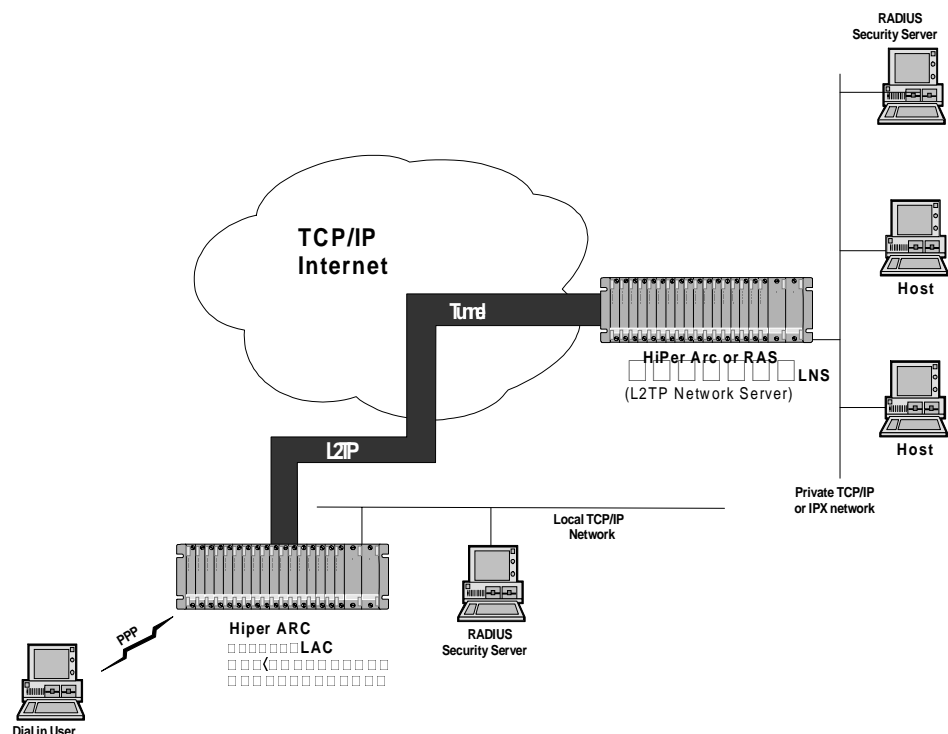


Figure 8-1 L2TP Implementation

Tunnels can presently be established only on the LAC side of the LAC-LNS pair although PPP traffic can be transmitted in either direction.

Configuring an L2TP Tunnel on HiPer ARC

Tunneling over L2TP is configured on HiPer ARC by creating fully-fledged dial-in tunnel users or, creating dial-in tunnel users mapped to an associated LNS. These users can share data transmitted from either side of the tunnel originating from a LAC. Support is not available for dial-out calls originating from an LNS. See illustration below.

L2TP tunnels are enabled by configuring *users* or up to 9 *LNS*'s. If you want to keep accounting records for users, create a *user* and specify a *server_endpoint* (LNS name or IP address), and *type* (tunneling protocol - L2TP). Alternatively, you can create one user to be shared by multiple users provided a global LNS is configured with one tunnel server endpoint rather than separate endpoints for each user. Optionally, you can ensure that no accounting records are maintained for users by not specifying an endpoint in their profile.

Authentication is available both for users (*password*) and tunnels (*security*). Tunnel security can be set at one of four layers: *data packets only*, *control packets only*, *both data and control packets* or *none*. *Group* values are optional while *medium_type* (ipv4) is set by default. Similar security is available if you choose to configure an LNS instead of individual users.



If you specify a LNS name, be sure that a DNS server is up and running to resolve the server's IP address.

Configuring a Tunneled Dialin User

To create a dial-in tunnel user, use the following commands:

```
add user <user_name>
    password <string>

set tunnel user <user_name>
    group <name>
    medium_type ipv4
    type l2tp
    password <string>
    security <both_data_and_control | control_only | data_only | none>
    server_endpoint <LNS_name or IP_address>
```

Parameters	Description
<user_name>	Name of user, previously defined using add user . Limit: 64 ASCII chars.
type	The tunneling protocol this user will employ. Choices: <ul style="list-style-type: none"> ▪ none - No tunneling specified ▪ pptp - Point-to-Point Tunneling Protocol. Default ▪ l2tp - Layer 2 Tunneling Protocol
medium_type	The transport layer of the tunnel medium used to create tunnels: ipv4
client_endpoint	IP address required for dialout calls only. Limit: 64 ASCII characters
server_endpoint	IP address of the server-end of the tunnel. Limit: 64 ASCII characters
password	The shared secret between tunnel server and client. Limit: 63 ASCII chars.
group	Group ID of the tunneled session. Limit: 64 ASCII characters
security	Additional security to perform on control or data packets for this tunnel. Choices: none , control-only , data-only , or both-data-and-control .

save all

- 1 Create a user with a password provided for user authentication. Type:

```
add user nancy password gina ENTER
```

- 2 Configure this new user as a *tunnel* type user with the default *medium* type of ipv4, *type* l2tp and *server_endpoint* of 2.2.2.2. Type:

```
set tunnel user nancy password gina type l2tp server_endpoint 2.2.2.2 ENTER
```

If you'd rather create a tunnel user that'll be shared by many dialin callers, set an LNS *ID*, *server_endpoint*, *shared_secret* and *security*. Be aware that no accounting records are kept for users without endpoints. Use these commands:

```
add l2tp lns <1-9>
```

```
set l2tp lns <1-9>
```

```
address <LNS IP_address>
```

```
security_level <both | control | data | none>
```

```
shared_secret <secret>
```

Parameters	Description
<l2tp server number>	An indexed value for the specified L2TP network server. Range: 1-9
shared_secret	The password shared by the L2TP network server and access concentrator (LAC). Limit: 256 ASCII characters.
security_level	Type of HMAC-MD5 packet encryption the L2TP network server performs: <ul style="list-style-type: none"> n data - encryption for data packets only n control - encryption for data packets only n both - encryption for data and control packets n none - no encryption performed. <i>Default</i>

For example:

```
set tunnel user earth password watch type l2tp security none ENTER
```

```
add l2tp lns 1 address 2.2.2.2 shared_secret watch security_level none ENTER
```

- 3 Save your work. Type:

```
save all ENTER
```

- 4 After a tunnel has been established, verify it is properly configured by issuing the **list l2tp tunnel** command. Also, issue the **list connections** command to verify the Data Link Layer (DLL) type is L2TP for all tunneled calls on the LAC only. The **list l2tp tunnels** command displays information on the LNS only, for example:

L2TP TUNNELS

TunID	Status	IP Address
1		2.2.2.2

The **list connections** command will display, for example:

IfName	User Name	Type	DLL	Start Date	Start Time
slot:3/mod:1	nancy	DIALIN	L2TP	05-AUG-1998	13:56:1

Configuring a Tunneled Dialout User

L2TP also supports outgoing (dialout) calls (*manual* dialout only). A tunneled (L2TP) outgoing call is initiated from the tunnel server (LNS) by issuing the **dialout l2tp** command. Once the dialout command is executed the LNS initiates a tunnel from the LNS to the tunnel client (LAC). The LAC then dials the phone number specified for the dialout user at the LNS. That phone number is sent by L2TP from the server to the client.

In the following section, you configure:

- Dialout using a HiPer ARC as the tunnel server endpoint
- Dialout using a HiPer ARC as the tunnel client endpoint
- Dialout using another router/HiPer ARC where PPP session is terminated

1 Dialout with one HiPer ARC acting as the LNS

To configure this part of a dialout tunneled call, you create a *user* and *password*, set a *client endpoint name* or *address* (for the LAC), provide *remote* and *local IP addresses* at either end of the connection, specify a *phone number* to access that connection, turn on *routing*, configure the *system transmit authentication name* (the same name as the user at the remote end of the connection) and set a *system name* on the LNS.



*You don't have to specify the following parameters because they are correct by default: **dialout user type** <manual>, **tunnel user medium_type** <ipv4>, and **tunnel user type** <l2tp>.*

Use the following commands:

```
add user <user_name>
    password <password>
    type <dialout/network>

set tunnel user <user_name>
    client_endpoint <LAC_name or IP address>

set network user <user_name>
    remote_ip_address <IP_address>
    ip_routing <both>

set user <user_name>
    phone_number <number>

set dialout user <user_name>
    local_ip_address <IP_address>

set system transmit authentication <user_name>

set system name <name>
```

For example:

```
add user gina password gina type network,dialout ENTER
set tunnel user gina client_endpoint 4.4.4.4
set network user gina remote_ip_address 5.5.5.5 ip_routing both ENTER
set user gina phone 5554545 ENTER
set dialout user gina local_ip_address 9.9.9.9 ENTER
set network user gina send_password gina ENTER
set system transmit authentication gina ENTER
set system name hiperarc ENTER
```

2 Dialout with a second HiPer ARC acting as the LAC.

This part of the dialout call involves creating a dialout *user name* and *password*, a network type of *dialout/network*, and a *phone number* on the LAC. Be sure that the user name is identical to the system name of the tunnel server (LNS). Also, note that the phone number you specify will be overwritten by the phone number of the user you created earlier (this value is optional). Use the following commands:

```
add user <user_name>
  password <password>
  type <dialout/network>

set user <user_name>
  phone_number <number>
```

For example:

```
add user hiperarc password none type network,dialout ENTER
set user hiperarc phone_number 4445656 ENTER
```

3 Dialout call terminates on third HiPer ARC/Windows NT or other router

This part of the dialout call involves another router to which the tunnel client (LAC) dials out using a phone number obtained from the user configured on the LNS. The *remote IP address* you set here will be the *local IP address* you set on the **LNS** while the local IP address set here will match the remote IP address set on the LNS.

For example:

```
add user gina password gina type network,login ENTER
set network user gina remote_ip_address 9.9.9.9 ip routing_both ENTER
set network user gina send_password gina ENTER
set dialout user gina local_ip_address 5.5.5.5 ENTER
set network user gina send_password gina ENTER
set system transmit authentication gina ENTER
```

4 Save your configuration.

Save your settings on *both* HiPer Arcs with the following command:

```
save all ENTER
```

5 Dial the call

Use the following command to dial the call:

```
dialout l2tp <user_name>
```

For example:

```
dialout l2tp gina ENTER
```

Once the dialout call is established, PPP negotiation will occur between the LNS and the “other” router on which the call is terminating.

Configuring an L2TP Tunnel on a RADIUS Server

Setting up L2TP on a RADIUS server is similar to HiPer ARC configuration in that users can be set up on either the LAC or LNS side of the tunnel. Follow the steps detailed below.

- 1 On the LAC side of the tunnel, configure a PPP user of tunnel type *l2tp*, with a user *password*, *tunnel password*, *tunnel security* and other framed values on the RADIUS server.

For example:

```
User-Name=gina
User-Password=bean
Service-Type=Framed
Framed-Protocol=PPP
Framed-IP-Netmask=255.255.255.255
Framed-MTU=1500
Framed-IP-Address=0.0.0.0
Tunnel-Type=L2TP
Tunnel-Server-Endpoint=<IP_address of LNS>
Tunnel-Security=both_data_and_control
```

- 2 Set the *transmit authentication name* for the LAC. This name is sent to the remote system for authentication. It is needed by PPP, which requires a *user* at the remote system with the *same authentication name*. It is employed when HiPer ARC receives a challenge while making a PPP connection to a remote system or router over the WAN. This value **must** match the name of the user configured on the LNS. Type the following:

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

For example:

```
set system transmit_authentication_name boston ENTER
```

- 3 On the LNS side of the tunnel, configure a standard PPP user (with the same user name created earlier) on the RADIUS server *and*, if you want to employ tunnel security, configure a *second* user matching the *system transmit authentication name* created earlier.

For example, the first user with no security specified:

```
User-Name=gina
User-Password=bean
Service-Type=Framed
Framed-Protocol=PPP
Framed-IP-Netmask=255.255.255.255
Framed-MTU=1500
Framed-IP-Address=0.0.0.0
```

For example, a second user with security provided:

```
User-Name=boston
User-Password=bean
Tunnel-Password=candy
```

Using PPTP

The Point-to-Point Tunneling Protocol (PPTP) provides Virtual Private Network (VPN) support for corporate networks across the Internet in much the same fashion as L2TP. "Virtual dial-up" is provided, tunneling PPP client sessions to a host network server located across the Internet from the HiPer ARC where clients initially connect.

The chief differences between the protocols is PPTP's support for a Windows NT server acting as the PPTP Network Server (PNS) and its lack of tunnel security. PPTP relies on PPP's built-in security and other IP-based mechanisms (such as IPSEC) because it is designed primarily for IP network while PPTP utilizes security mainly for non-IP networks.

The protocols also differ in that PPTP uses TCP for control channel and GRE for data channel communications while PPTP uses UDP for control as well as data channel communications.

Configuring a PPTP Tunnel on HiPer ARC

Tunneling over PPTP is configured on HiPer ARC by creating fully-fledged dial-in tunnel users or, creating dial-in tunnel users mapped to an associated PNS. These users can share data transmitted from either side of the tunnel originating from a PAC. Support is not available for dial-out calls originating from an PNS.

PPTP tunnels are enabled by configuring *users* or up to 9 *PNS*'s. If you want to keep accounting records for users, create a *user* and specify a *server_endpoint* (PNS name or IP address), and *type* (tunneling protocol - PPTP). Alternatively, you can create one user to be shared by multiple users provided a global PNS is configured with one tunnel server endpoint rather than separate endpoints for each user. Optionally, you can ensure that no accounting records are maintained for users by not specifying an endpoint in their profile.

Authentication is available both for users (*password*) and tunnels (*security*). Tunnel security can be set at one of four layers: *data packets only*, *control packets only*, *both data and control packets* or *none*. *Group* values are optional while *medium_type* (IPv4) is set by default. Similar security is available if you choose to configure an PNS instead of individual users.



If you specify a PNS name, be sure that a DNS server is up and running to resolve the server's IP address.

How it Works

A remote client dials into a HiPer ARC serving as the PPTP Access Concentrator (PAC) and initiates an asynchronous or synchronous PPP connection through the Internet over either a Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN). HiPer ARC establishes the PPP link and begins authentication of the client based on its user name and a specified endpoint - the PPTP Network Server (PNS). After authentication is accepted, client data is passed to the PNS (another HiPer ARC or any Network Access Server) and this host either accepts or rejects the dialup call. See illustration below.

Then, using the Transmission Control Protocol (TCP), a tunnel (defined as a PAC-PNS pair) to a specified PNS is initiated. Once the tunnel is up, control messages are passed between the PAC-PNS to manage the tunnel. An unused slot within the tunnel - a session - is then prompted from the PNS, as well as authentication data. If the PNS successfully authenticates the dialup session a

second time (using CHAP, PAP or MS CHAP) a virtual interface for PPP is created, allowing the passage of packets through the tunnel in both directions.

At this point, connectivity is established via a point-to-point PPP session whose endpoints are the remote user's networking application on one end and the termination of this connectivity at the PNS's PPP support on the other. Because the remote user has become simply another dial-up client of the PNS, client connectivity can now be managed using traditional methods of authorization, protocol access, and packet filtering. Accounting can be performed on both the HiPer ARC (PAC) and host network server (PNS).

Configuring a Tunneled Dialout User

PPTP also supports outgoing (dialout) calls (*manual* dialout only). A tunneled (PPTP) outgoing call is initiated from the tunnel server (PNS) by issuing the **dialout PPTP** command. Once the dialout command is executed the PNS initiates a tunnel from the PNS to the tunnel client (PAC). The PAC then dials the phone number specified for the dialout user at the PNS. That phone number is sent by PPTP from the server to the client.

In the following section, you configure:

- Dialout using a HiPer ARC as the tunnel server endpoint
 - Dialout using a HiPer ARC as the tunnel client endpoint
 - Dialout using another router/HiPer ARC where PPP session is terminated
- 1 Dialout with one HiPer ARC acting as the PNS. To set up this part of a dialout tunneled call, you create a *user* and *password*, set a *client endpoint name* or *address* (for the PAC), provide *remote* and *local IP addresses* at either end of the connection, specify a *phone number* to access that connection, turn on *routing*, configure the *system transmit authentication name* (the same name as the user at the remote end of the connection) and set a *system name* on PNS.



*You don't have to specify the following parameters because they are correct by default: **dialout user type** <manual>, **tunnel user medium_type** <ipv4>, and **tunnel user type** <PPTP>.*

Use the following commands:

```
add user <user_name>
    password <password>
    type <dialout/network>

set tunnel user <user_name>
    client_endpoint <PAC_name or IP address>

set network user <user_name>
    remote_ip_address <IP_address>
    ip_routing <both>

set user <user_name>
    phone_number <number>

set dialout user <user_name>
    local_ip_address <IP_address>

set system transmit authentication <user_name>

set system name <name>
```

For example:

```
add user gina password gina type network,dialout ENTER
set tunnel user gina client_endpoint 4.4.4.4
set network user gina remote_ip_address 5.5.5.5 ip_routing both ENTER
set user gina phone 5554545 ENTER
set dialout user gina local_ip_address 9.9.9.9 ENTER
set network user gina send_password gina ENTER
set system transmit authentication gina ENTER
set system name hiperarc ENTER
```

- 2 Dialout with a second HiPer ARC acting as the PAC. This part of the dialout call involves creating a dialout *user name* and *password*, a network type of *dialout/network*, and a *phone number* on the PAC. Be sure that the user name is identical to the system name of the tunnel server (PNS). Also, note that the phone number you specify will be overwritten by the phone number of the user you created earlier (this value is optional). Use the following commands:

```
add user <user_name>
password <password>
type <dialout/network>

set user <user_name>
phone_number <number>
```

For example:

```
add user hiperarc password none type network,dialout ENTER
set user hiperarc phone_number 4445656 ENTER
```

- 3 Dialout call terminates on third HiPer ARC/Windows NT or other router

This part of the dialout call involves another router to which the tunnel client (PAC) dials out using a phone number obtained from the user configured on the PNS. The *remote IP address* you set here will be the *local IP address* you set on the **PNS** while the local IP address set here will match the remote IP address set on the PNS.

For example:

```
add user gina password gina type network,login ENTER
set network user gina remote_ip_address 9.9.9.9 ip_routing_both ENTER
set network user gina send_password gina ENTER
set dialout user gina local_ip_address 5.5.5.5 ENTER
set network user gina send_password gina ENTER
set system transmit authentication gina ENTER
```

- 4 Save your configuration. Save your settings on *both* HiPer Arcs with the following command:

```
save all ENTER
```

- 5 Dial the call. Use the following command to dial the call:

```
dialout PPTP <user_name>
```

For example:

```
dialout PPTP gina ENTER
```

Configuring a PPTP Tunnel on a RADIUS Server

Once the dialout call is established, PPP negotiation will occur between the PNS and the "other" router on which the call is terminating.

Setting up PPTP on a RADIUS server is similar to HiPer ARC configuration in that users can be set up on either the PAC or PNS side of the tunnel. Follow the steps detailed below.

- 1 On the PAC side of the tunnel, add a PPP user of tunnel type PPTP, on the RADIUS server.

For example:

```
User-Name=gina
User-Password=bean,
Tunnel-Type = PPTP,
Tunnel-Server-Endpoint = <IP_address of LNS or fully qualified domain name>
```

- 2 Set the *transmit authentication name* for the PAC. This name is sent to the remote system for authentication. It is needed by PPP, which requires a *user* at the remote system with the *same authentication name*. It is employed when HiPer ARC receives a challenge while making a PPP connection to a remote system or router over the WAN. This value **must** match the name of the user configured on the LNS. Type the following:

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

For example:

```
set system transmit_authentication_name boston ENTER
```

- 3 On the PNS side of the tunnel, configure a standard PPP user (with the same user name created earlier) on the RADIUS server *and*, if you want to employ tunnel security, configure a *second* user matching the *system transmit authentication name* created earlier.

For example, the first user with no security specified:

```
User-Name=gina
User-Password=bean
Service-Type=Framed
Framed-Protocol=PPP
Framed-IP-Netmask=255.255.255.255
Framed-MTU=1500
Framed-IP-Address=0.0.0.0
```

- 4 Verify the PPTP tunnel as the PNS side by issuing the **list tunnel connection** command.

For example:

IfName	User Name	Type	Start Date	Start Time
tun:1	gina	PPTP	19-SEP-2041	03:39:58

Using MPIP

Multi-link PPP Protocol (MPPP) provides greater bandwidth for a PPP connection by allowing multiple physical PPP links to comprise a single logical link. As a rule, multi-link PPP logical connections require termination on the same router (HiPer ARC), but MPIP overcomes this limitation by communicating among multiple physical terminating endpoints (within a HiPer ARC client-server configuration) and specifying a single logical endpoint. MPIP uses the User Datagram Protocol (UDP) to communicate between clients and server.

So, if more than one HiPer ARC accepts dial-in calls in a Point-of-Presence (POP) or same numbering plan, the possibility exists that calls for the same user may terminate on different HiPer ARCs. MPIP helps to solve this problem. It does so by selecting one of the HiPer ARC to logical terminate each call. Other HiPer ARCs then use the Virtual Tunneling Protocol (VTP) to tunnel their calls on the selected HiPer ARC while MPIP helps decide which HiPer ARC terminates the calls. Be sure that NTP is enabled, otherwise VTP won't work. Otherwise, no other configuration is required for VTP - it functions mostly as a data pathway.

How it Works

A remote user dials in to a HiPer ARC *client* configured to accept multi-link PPP traffic. This *first* physical connection where the multi-link PPP call is terminated (the destination) is specified as the *bundle owner* of all packets associated with the call. When traffic reaches a certain level on this HiPer ARC client, another link is established on a second configured HiPer ARC client and so forth for any additional clients. See the illustration below.

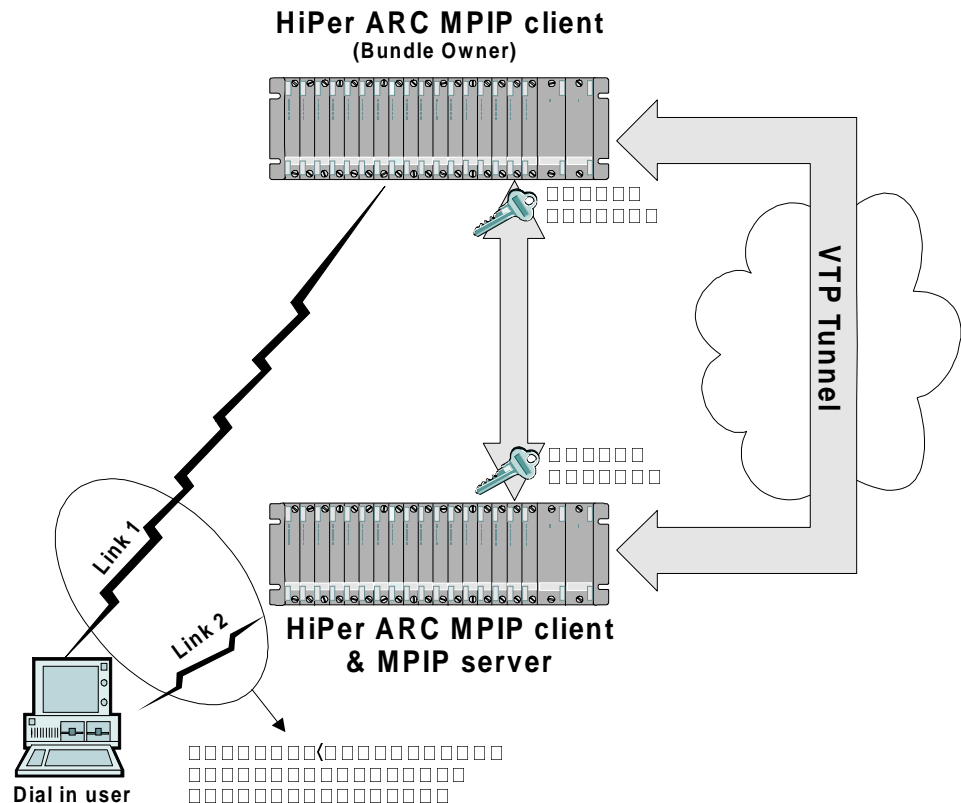


Figure 8-2 MPIP Connection

Next, configuring either HiPer ARC as an *MPIP server* allows the second HiPer ARC client to learn the existence and primacy of the first HiPer ARC client, enabling the passage of packets to their correct endpoint. The MPIP server, which can reside on any UNIX machine (and in this case can be on either HiPer ARC or even a separate HiPer ARC not participating in PPP call handling), acts as a central database for link information regarding all MPIP clients and resolves bundle ownership of any incoming MPIP packets.

MPIP clients and servers are configured with a shared secret known to each other for authentication purposes. Multiple MPIP servers can be configured for purposes of redundancy but all MPIP clients must share the same secret with their MPIP server pairs. When more than one MPIP server is configured, they communicate with each other periodically to synchronize their link databases.

Once all MPIP clients and servers have communicated and are aware of each other, the bundle owner MPIP client uses VTP to build a tunnel between itself and all other MPIP clients, establishing the user's PPP connection. At this point connectivity is established and data traffic is transmitted over the tunnel between the user and HiPer ARC terminator.

Configuring a Multi-link PPP connection with MPIP

Configuring a multi-link PPP connection using MPIP is accomplished by adding MPIP clients with a *shared secret* for each client-server pair and adding one or more MPIP servers with a *priority* value for each server, the *shared secret* (1-16 ASCII characters) associated with its clients, and a *type* (*hiper* or *netserver*). Servers and clients can be located on the same HiPer ARC.

Optionally, a *port* number specifying the UDP port on which the server listens for control traffic can be specified although the default port setting is *5912*.

No special user configuration is required to configure MPIP (dialin users are still configured though).



If two MPIP servers have the same priority setting, the MPIP server with the smaller IP address takes precedence.

Follow the steps below:

- 1 Create an MPIP client using the following command:

```
add mpip client <IP_address>
sharedsecret [string]
type [hiper | netserver]
```

For example, add two MPIP clients:

```
add mpip client 149.112.214.140 sharedsecret cashews type hiper ENTER
```

```
add mpip client 149.112.214.142 sharedsecret cashews type netserver ENTER
```

- 2 Create an MPIP server using the following command:

```
add mpip server <IP_address>
sharedsecret [string]
```

For example, add two MPIP servers:

```
add mpip server 149.112.214.140 priority 1 sharedsecret cashews ENTER
```

```
add mpip server 149.112.214.142 priority 2 sharedsecret cashews ENTER
```

- 3 HiPer ARC doesn't normally act as an MPIP server, and therefore is disabled by default. You must turn the server on (MPIP clients are *ON* by default). Use the following global command:

```
set mpip
  server_state [on | off]
  client_state [on | off]
```

For example:

```
set mpip server_state on ENTER
```

- 4 Save your configuration. Type:

```
save all ENTER
```

- 5 You can verify your MPIP settings by issuing the **show mpip settings**, **list mpip clients** and **list mpip servers** commands. The commands will return the following information, for example:

```
HiPer>>show mpip servers ENTER
```

MPIP Server State	ON
MPIP Client State	ON
MPIP UDP Port	5912

```
HiPer>>list mpip clients ENTER
```

Client	Type
149.112.214.140	HIPER
149.112.214.142	NETSERVER

```
HiPer>>list mpip servers ENTER
```

MPIP Servers		
IP Address	UDP Port	Priority
149.112.214.142	5912	1

- 6 Set parameters for the Simple Network Time Protocol client process, which references a server-based clock for HiPer ARC to synchronize with VTP. Use these commands:

```
set ntp primary_server <ip_address>
```

```
enable ntp
```

```
show ntp
```

- 7 Once the VTP tunnel is established and the multi-link PPP connection is up, you can use the **list mpip bundles** and **list mpip links** commands to verify packet transmissions. For example:

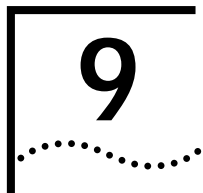
HiPer>>list mpip bundles ENTER

MPIP Bundles				
Bundle Owner	EndPoint Value	Descriminator Type	No. Links	User Name
149.112.214.140	61626364656600000000	1	3	john
149.112.214.142	78787879797900000000	1	2	larry

HiPer>>list mpip links ENTER

MPIP Links			
Bundle Owner	Link Owner	Link ID	User Name
149.112.214.140	149.112.214.140	11	john
149.112.214.140	149.112.214.140	12	john
149.112.214.140	149.112.214.142	13	john
149.112.214.142	149.112.214.142	14	larry
149.112.214.142	149.112.214.140	13	larry





PACKET FILTERS

This chapter describes how to set up packet filters on HiPer ARC. The topics are:

- Filtering Overview
- Filter Types
- Creating Filters
- Configuring Filters
- Managing Filters
- General Filter Setup
- Filter Examples



This chapter describes how to use a text editor and the CLI to use filters. HiPer ARM provides the same functionality using a graphical interface - for more information, see HiPer ARM on-line Help.

Filtering Overview

Packet filters are used primarily in networks that cross organizational or corporate boundaries. They control inter-network data transmission by accepting or rejecting the passage of specific packets through network interfaces based on packet header information.

When data packets are received by a network interface such as a modem, a packet filter analyzes packet header data against its set of rules. Based on rules that you define, the filter permits the packet to pass through or discards it.

Filtering Capabilities

HiPer ARC supports the following filtering capabilities:

- Input/output filtering - packet filters can be used to control inbound or outbound data packets
- Source/destination address filtering - a packet filter can accept or deny access to a host or user based on the address of the source and/or destination
- Protocol filtering - inbound or outbound network traffic can be evaluated based on the protocol
- Source/destination port filtering - a packet filter can control what services local or remote users can access
- Call filtering can control whether a packet can initiate an outgoing call
- Controls the content of IP Routing Information Protocol (RIP) packets sent or received on specific ports.
- RADIUS and TACACS+ filtering; see *Appendix E: RADIUS and TACACS+ Systems* for more information.

Information Sources Internet packet filtering and security are complex issues. The chapter aims to provide an overview of the filtering capabilities provided by HiPer ARC. For more detailed information on this topic, refer to the following information sources:

- Cheswick and Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison Wesley, 1994, ISBN 0-201-63357-4
- Siyan and Hare, *Internet Firewalls and Network Security*, New Riders Publishing, 1995, ISBN 1-56205-437-6

Filter Types

Filters can be classified by the following types:

- Data filters - based on protocol-specific packet information
- Advertisement filters - based on broadcast packet information
- Generic filters - based on packet structure
- Call filters - based on outgoing/incoming calls

Data Filters Data filters control network access based on protocol, source/destination address, and source/destination port designation (e.g., TCP/UDP port designations) of the packet.

HiPer ARC supports IP and IPX-related filters. This filter type controls network access based on the protocol and source/destination address. IP filter rules allow filtering on source address, destination address, protocol type, source port, and destination port of the IP packet. IPX filter rules allow filtering on source network, destination network, protocol type, source socket, destination socket, source node, and destination node of the IPX packet.

Advertisement Filters Advertisement filters act on network protocol packets that contain information such as RIP. Filtering these packets is performed by the specific protocol process.

IP-RIP, IPX-RIP and IPX-SAP are supported by HiPer ARC. The IP-RIP filter type controls the content of IP Routing Information Protocol (RIP) packets that are sent out or received. The IP- and IPX-RIP filtering process filters addresses from the RIP packet upon transmission (output filter), and does not enter routes into the Routing Table upon receipt (input filter).

The IPX-SAP filter type controls the content of Service Advertising Protocol (SAP) packets which are transmitted or received. The IPX-SAP filter rules allow filtering on service type, server name, network address, node address, and the socket number fields of the service entry. The forwarding process uses the filter information to prevent service data from being included in the SAP packet.

Call Filters IP-Call filters are employed to screen outgoing calls for an ondemand user or a per interface basis. Filtering rules can comb source, destination and host addresses, port numbers of TCP, and UDP protocols, ICMP messages and protocols.

Generic Filters Generic filters are set by byte and offset values in a packet. Packets are filtered by comparing their offset value and byte information with the values you define in the filter. The Hub accepts or rejects the packet based on the result.



Creating generic filters can be a complex task. Only experienced users should use generic filters, and strictly in cases where data and advertising filters cannot provide necessary filtering capabilities.

Creating Filters

HiPer ARC performs packet filtering based on rules you create. This section describes how to create packet filters

Filter File Components

Filter rules are defined within filter files. Filters are text files stored either in FLASH memory or on a RADIUS server. You can create and modify filter using:

- The CLI **edit** command
- The Windows-based *HiPer ARM* (refer to HiPer ARM on-line documentation)
- An off-line text editor

File Descriptor

To be valid, a filter file must always have this file descriptor on the first line:

#filter



Eliminate blank space before the descriptor, otherwise an error will occur.

The remainder of the filter file is partitioned into protocol sections. Each protocol section has a descriptive header preceding filter rules for that protocol.

Protocol Sections

A single filter file can contain protocol sections in any order, but sections cannot be repeated. The following conditions cause errors or prevent filtering:

- If you don't specify a protocol section in the filter file, no filtering will occur and packets of that protocol type will be accepted
- If you specify a protocol section but don't define rules, an error will occur.
- If you omit a line number or insert a line out of sequence, errors will occur.



To comment out a protocol section, you must place a pound (#) sign before the section header and before all rules defined in that section.

The table below describes valid protocol sections you can define in the filter file:

Protocol Section	Description
IP:	IP protocol data filter section
IP-CALL:	IP protocol call filter section
IP-RIP:	IP RIP advertising filter section
IPX:	IPX protocol data filter section
IPX-CALL:	IPX protocol call filter section
IPX-RIP:	IPX RIP advertising filter section
IPX-SAP:	IPX SAP advertising filter section
LOGIN-ACCESS:	Login Access filter section

Protocol Rules

You define protocol rules within each protocol section in the filter file. These rules set which packets may and may not access the network. The rule syntax is:

```
<line #> <verb> <keyword> <operator> <value>;
```

The combination of keyword, operator, and value forms a condition which, when combined with a verb, sets whether packets are accepted or rejected.

When a packet is filtered, an IP packet for example, HiPer ARC parses each rule defined in the IP protocol section sequentially according to the line number. Filtering is performed based on the first occurring match. Without a match, the packet is accepted by default. For this reason, you should order your protocol rules so that rules you expect to be most frequently matched are situated early in the section to reduce parsing time during filtering.

The following table describes each field used in the rule syntax:

Field	Description
line #	Each rule must have a unique line number (1-999). You must arrange rules in increasing order.
verb	This field can be one of the following: <ul style="list-style-type: none"> ■ ACCEPT - allow packet access if condition is met ■ REJECT - do not allow packet access if condition is met ■ AND - logically use the AND condition with condition of the next rule to determine if packet is accepted or rejected: both defined conditions must be met. <i>IMPORTANT:</i> No more than 15 consecutive AND rules are permitted.
keyword	For descriptions, see page 9-147
operator	Describes the relationship between the keyword and its value. The operator field must be one of the following that applies to the specific keyword used: <ul style="list-style-type: none"> = Equal != Not equal > Greater than < Less than >= Greater or Equal <= Less or Equal => Generic
value	Contains an entity appropriate for the keyword. For descriptions, see page 9-147.



The OR operation can be implemented by successive ACCEPT rules. For example, to accept a packet if the source address is xxx, or the destination address is yyy, the following rules are used:

```
IP:
010 ACCEPT src-addr = xxx;
020 ACCEPT dst-addr = yyy;
```

Generic Filter Rules

Generic filter rules are similar in format to protocol filter rules. The following shows the rule syntax. The rule syntax is:

```
<line #> <verb> <keyword> <operator> origin = <DATA | FRAME>/
offset = <value>/length = <value>/mask = <hexadecimal value>/
value = <hexadecimal value>;
```

The following table describes each field used in the rule syntax:

Field	Description
line #	Each rule must have a unique line number (1-999). You must arrange rules in increasing order.
verb	This field can be one of the following: <ul style="list-style-type: none"> ■ ACCEPT - allow packet access if the condition is met ■ REJECT - do not allow packet access if the condition is met ■ AND - logically use the AND condition with condition of the next rule to determine if packet is accepted or rejected. Both defined conditions must be met. <i>IMPORTANT:</i> No more than 15 consecutive AND rules are permitted.
keyword	The keywords for a generic filter rule is always GENERIC .
operator	The operator for a generic filter rule is always: =>
origin	Can be either FRAME or DATA
offset	Number of bytes offset from the origin.
length	Number of bytes to compare and mask.
mask	Bit mask in hexadecimal format for logical and packet content.
value	Value in hexadecimal format used to compare with contents of masked packet

For example, a generic filter rule might look like this:

```
010 ACCEPT generic => origin = data/offset = 22/length = 6/
mask = 0xFFFFFFFFFF/value = 0x0800096f39c8;
```

Specifying the Filtering Action

You can specify the filtering action for each protocol section that determines whether a packet is accepted or rejected if no match occurs with any of the rules defined in the section. To do so, enter one of the following values as the *last* rule line of the section:

- ACCEPT
- DENY

For example, the following entry would reject IP packets that did not match any of the rules defined in the IP protocol section:

```
#filter
IP:
010 ACCEPT tcp-dst-port> = 24;
020 ACCEPT src-addr = 128.100.033.001;
030 ACCEPT dst-addr = 200.135.038.009;
040 DENY;
```



*If you do not specify a filtering action, the default filtering action is **permit**.*

Creating Filter Files

There are two methods to create and edit filter files. One method uses **edit**, a simple line editor on the CLI. Edit is most effective when creating small or editing large filter files. It is less convenient *creating* large filter files. Edit is described in *Chapter 10: CLI Reference* and *Chapter 9: Administrative Tools*. If you want to use edit, go to step 1.

The alternative is to use a text editor on your PC to create or edit a filter file. You'll then use the Trivial File Transfer Protocol (TFTP) to load the file in HiPer ARC's FLASH memory (TFTPing an edited file to HiPer ARC replaces the original file).

Be careful, the following steps require frequent switching between your PC and HiPer ARC. To create a filter file on your PC:

- 1 Create a new text file. Enter a file descriptor on the first line:

```
#filter
```



Eliminate blank space before the descriptor, otherwise an error will occur.

- 2 Enter a file section header followed by a colon to begin a protocol section. For example, to define IP filtering rules, enter the following section header:

```
IP:
```



If you want to comment a section header out, put a # (pound) sign before the header. It's useful to insert a placeholder for a protocol section you'll define later.

- 3 Enter the protocol rules for the protocol section you are defining. Be sure to:

- Begin each rule with a unique line number (1-999)
- Arrange rules in increasing order within each protocol section
- Arrange rules so that the rules you expect to be matched *most frequently* are at the top of the list
- Delimit each rule with a semi-colon (;)

For example:

```
#filter
IP:
010 ACCEPT src-addr = 128.100.033.001;
020 ACCEPT dst-addr = 200.135.038.009;
```

- 4 Add filtering action if different from the default value of PERMIT.

For example:

```
030 DENY;
```

- 5 Continue to define protocol rules for each protocol section you want to filter, then check the file to ensure it meets HiPer ARC requirements. And save the file. If you're using the **edit** command, skip to step 8.



To set up RADIUS filter files, see Appendix E: RADIUS and TACACS+.

- 6 Access the CLI on HiPer ARC. Configure your PC as a Trivial File Transfer Protocol (TFTP) *client* by entering the following command:

```
add TFTP client <hostname or IP address>
```

- 7 Return to your PC. From a machine that has access to the same network as HiPer ARC, use the following *TFTP commands* to transfer the filter file to HiPer ARC 's FLASH memory.

```
tftp <HiPer_IP_ address>
```

```
put <filter_filename>
```

- 8 Return to the CLI on HiPer ARC. HiPer ARC does not recognize a filter file stored in its FLASH memory until you add it to the Managed Filter Table. Use the following command:

```
add filter <name>
```

When the filter is added, HiPer ARC automatically verifies filter file syntax. If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, an error message is generated detailing the error source.



Type **list files** to ensure the filter file was successfully stored in FLASH memory.

- 9 Use the **verify filter** command to ensure filter file syntax is correct. Type:

```
verify filter <filter name>
```

If a filter fails to verify, used the CLI **edit** command or, return to your text editor, edit the file, TFTP the file back to HiPer ARC and re-verify. Go to the *Configuring Filters* section.



Any subsequent entry of same name filter files requires they be reverified and reapplied using **set interface**. Use **show filter <filter name>** to view your file. If you are applying a filter to a RADIUS user, use **show remote user**.

Configuring Filters

Once a filter has been added to the managed filters list, turn *filter access* on or off, and *assign* the filter to HiPer ARC's interfaces or users.

Setting Filter Access

When filters are assigned to an interface, the *filter access* parameter must remain off (*default* setting). But, if configuring a filter for a user, you **must** enable filter access. This parameter acts as a toggle switch for interface or user filtering and, when enabled, overrides the default *interface* setting.



If your filters are inoperative, it more than likely is because you have not correctly set filter access.

To enable filter access for a specific *user*, use the following command:

```
set interface <slot:x/mod:[1-y]> filter_access on
```

To enable filter access for a specific *interface*, use the following command:

```
set interface <slot:x/mod:[1-y]> filter_access off
```



*Filter file changes take effect on an interface immediately when you issue the **set interface** command. The **set switched interface** and **set modem_group** commands can also be issued to turn filter access on or off.*

Interface Filters

You can configure interface filters for any *interface* or *modem group*. Interface filters control access to all networks available for both modem and non-modem (eth:1 or eth:2) interfaces.

You can specify whether a filter applies to packets entering the interface (input filter), leaving the interface (output filter), and packets that can initiate a call out (call filter). HiPer ARC examines the filtering rules to determine whether the

interface accepts or rejects the packet. Interface filters can be applied dynamically without having to disable and re-enable each network on that interface.



*If you prefer to configure a filter through a modem group, first issue the **add modem group <name> interfaces <slot:x/mod [1-y]>** command.*

Use either of the following commands:

```
set interface <slot:x/mod [1-y]> input_filter <filter_name> output_filter <filter_name>
```

```
set modem_group <name> input_filter <filter_name> output_filter <filter_name>
```

Input Filter

If an input filter is configured on an interface, all received packets are checked against the filtering rules before being forwarded to another interface. In other words, an input filter handles data *from* an interface.

Output Filters

If an output filter is configured on an interface, all outbound packets are checked against the filtering rules before exiting the interface. In other words, an output filter handles data *to* an interface.

Call Filters

If a call filter is configured on an interface, all transmitted packets are checked against the filtering rules. The filtering rules determine whether the packet can initiate an outgoing call. Call filters are checked only after the packet has passed the output filter check. An interface without a call filter configured will allow packets from all properly configured users to initiate an outgoing call.

This filter is used for an ondemand call only.

Input Filters vs. Output Filters

When possible, use the input filter to filter an incoming packet rather than wait to catch a packet as it attempts to exit.. This is recommended because:

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

User Filters

You can configure filters for a specific user to control network access for that user. This filter type is applied for the duration of the user's network connection only. As with interface filters, a user filter can be configured as an input, output or call filter. Remember, input filters handle data *from* a user, while output filters handle data *to* a user.



User filters are dynamic only via RADIUS. Filter access must be turned ON before the user connects and attempts a RADIUS request for filters.

Assigning a Filter to an Interface

To configure input or output filters on a specified interface, use the following command. The default *filter access* setting (*off*) need not be set *unless* you have previously enabled filtering for a *user*. Use the following command:

```
set interface <slot:x/mod:[1-y]>
  input_filter <filter_name>
  output_filter <filter_name>
  filter_access off
```

For example, if you *haven't* enabled a user filter on the interface, type:

```
set interface slot:4/mod:8 input_filter infilter.fil ENTER
```

If you *have* enabled a user filter on the interface, you must reset access. Type:

```
set interface slot:4/mod:8 output_filter outfilter.fil filter_access off ENTER
```

If you want to set slot:4/mod:8 input and output filters at the *same time*, type:

```
set interface slot:4/mod:8 input_filter infilter.fil output_filter outfilter.fil ENTER
```



Filter files take effect on an interface immediately on enabled networks when you issue the **set switched interface** or **set modem_group** commands.

Assigning a Filter to a User



To configure an input or output filter for a specific user, use these commands.

Filter access **must** be turned on (*off* by default) on the interface to be used when setting a **user** filter.

```
set user <user_name>
  input_filter<filter_name>
  output_filter<filter_name>
```

```
set interface <slot:x/mod:[1-y]> filter_access on
```

For example:

```
set user nancy input_filter infilter.fil ENTER
set interface <slot:5/mod:[1-24]> filter_access on ENTER
```



Filters take effect for a user the **next** time that user makes a connection.

Managing Filters

This section provides information about how to manage filters, including:

- Displaying the managed filter list
- Adding filters to the managed filter list
- Deleting filters from the managed filter list
- Verifying filter file syntax
- Displaying the contents of a filter



An important consideration to remember about managing filters: If you edit an existing filter and do not first remove it from **every** interface or user profile for which it is configured and then reapply the new filter, the previously unedited version will still apply. See *Removing a Filter ...* sections on the next page.

Displaying the Managed Filter List

To display the list of managed filters, use the following command:

```
list filters <filter_name>
```

The resulting display might look like this:

FILTERS		
Filter Name	Status	Protocols
xfilter.in	NORMAL	IP IP-RIP
xfilter.out	VERIFY FAILED	IPX
ljc_filter.fil	NORMAL	IP-CALL

Adding Filters to the Managed List

The **add filter** command verifies filter syntax before adding a filter to the managed list. If syntax is valid, no message is generated and the command prompt returns. If syntax errors exist, messages are sent describing them.

If the syntax is invalid, the filter is still added to the managed list with a status of *verify failed*. To correct filter file errors, you must make the changes to the original filter file using a text editor, and re-TFTP the file to FLASH memory. You must then use the **verify filter** command to check the filter file syntax. For more information about **verify filter**, see *Verifying Filter File Syntax*.

To add a filter file to the list of managed filters, use the following command:

```
add filter <filter_name>
```



*It's helpful to use **list files** to see files successfully stored in flash memory.*

Removing a Filter from an Interface

Removing a filter assigned to an interface is mandatory when editing it. The "" value is a null value which removes a defined filter from the interface. Type:

```
set interface <interface_name>
input_filter ""
output_filter ""
```

For example, to remove an output filter from the *eth:1* interface, type:

```
set interface eth:1 output_filter "" ENTER
```

Now be sure to reapply the filter with the **set interface** command. Type:

```
set interface eth:1 output_filter <filter_name>
```

Removing a Filter from a User Profile

Removing a filter assigned to a user profile is mandatory when editing it. The "" value is a null value which removes the defined filter from the user profile. Type:

```
set user <user_name>
input_filter ""
output_filter ""
```

For example, to remove an input filter from a user named "john_d", type:

```
set user john_d input_filter "" ENTER
```

Now be sure to reapply the filter with the **set user** command. Type:

```
set user john_d input_filter <filter_name>
```



This command does not dynamically remove a filter from a user profile.

Deleting a Packet Filter

To delete a specific packet filter, removing the filter file from the filter list and permanently from FLASH memory, use the following commands:

```
delete filter <filter_name>
```

```
delete file <file_name>
```

Verifying Filter File Syntax

The **verify filter** command is useful if you make changes to a filter file that has already been added to the managed list and re-TFTP the file back into FLASH memory (using the same filename). This command checks the filter syntax, compiles it and if valid, generates no message and returns the command prompt. If invalid, error messages are generated detailing the error sources.



*Filter file changes are designed to take effect on an interface immediately after you issue the **set interface** command. So remember to **remove** and **reapply** the filter to ensure new filter rules apply to all affected interfaces.*

To verify a filter file, use the following command:

```
verify filter <filter_name>
```

Showing Filter File Contents

To view the contents of an entire filter file that has been added to the managed list of filters, use the following command:

```
show filter <filter_name>
```

To display the contents of the filter file by protocol, use the following command:

```
show filter <name> protocol [ ip | ip-call | ip-rip | ipx | ipx-call | ipx-rip | ipx-sap | login-access ]
```

Generating SYSLOG Messages for Filtered Packets

You can save filtered packets to a configured SYSLOG server, allowing you to track down a potentially malicious user. Due to the large amount of traffic this command could generate, its anticipated use would only be for a short time.



Remember to configure the SYSLOG server before using these commands. See Appendix D: Event Messages for information on using SYSLOG.

Use the following command:

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

A description of each parameter follows.

- *All* - Creates SYSLOG messages globally for all filtered packets.
- *Radius* - Checks the RADIUS profile (Filter-Log-Packet attribute in the Access-Accept packet) on a per-user basis.
- *None* - No SYSLOG messages generated.
- *0-493 bytes* - Use a number between 0 and 493 to specify how many bytes of the discarded packet to send to SYSLOG. Setting to 0 causes the entire packet to be included in the SYSLOG message.

General Filter Setup

This section describes the steps to configure a filter on HiPer ARC.

- 1 Create a filter using the filter rules described in the *Creating Filters* section. You may use the CLI **edit** command or an off-line editor and TFTP the file to HiPer ARC. For the purposes of this example, the input filter is named: **hiper.fil**
- 2 If you're configuring a *user* filter - not an *interface* filter - enable filter_access (*off* by default) with the following command. Filter access should remain off for an interface filter.

```
set interface slot:x/mod:y filter_access on ENTER
```

- 3 Add the filter to HiPer ARC's Managed Filter Table with the following command:

```
add filter hiper.fil ENTER
```

- 4 HiPer ARC automatically verifies that new filters are syntactically correct. For added insurance, issue the following command:

```
verify filter hiper.fil ENTER
```

- 5 Issue the following command to ensure the filter was stored in HiPer ARC's FLASH memory:

```
list files ENTER
```

- 6 Assign the filter to a previously created user with the following command. If using RADIUS, specify the Framed-Filter-ID attribute.

```
set user <any_user_name> input_filter hiper.fil ENTER
```

- 7 Verify that the filter was applied to the user with either of the following commands:

```
show user <user_name>
```

```
show remote user <user_name>
```

Filter Examples

This section provides specific filter examples.

IP Packet Filter Rule Examples

This section briefly describes IP packet filtering options, and provides rule examples for each IP packet filtering capability. It includes the following topics:

- Source and Destination Address Filtering
- Masks
- TCP and UDP Parameter Filtering
- IP/IPX-RIP Packet Filtering
- IPX-SAP Filtering
- ICMP Packet Filtering
- IP/IPX-Call Filtering
- Login-Access Filtering

Source and Destination Address Filtering

Source and destination address filtering is generally used to limit permitted access to trusted hosts and networks only, to explicitly deny access to hosts and networks that are not trusted, or to limit external access to a given host (for example, a Web server or a firewall).



Only the part of the IP address specified by the mask field is used in the comparison. If a match is found, the packet is forwarded (rules containing *accept*) or discarded (rules containing *reject*).

The following rule example rejects forwarding of IP packets with a source address of *192.77.100.32*:

```
#filter
IP:
010 REJECT src-addr = 192.77.100.32;
```

The following rule example prevents forwarding of IP packets with destination addresses that match the *first 24 bits* of the given IP address (that is, addresses beginning with *188.039.150*):

```
#filter
IP:
010 REJECT dst-addr = 188.039.150.000/24;
```

The following rule example allows forwarding of IP packets with source address *192.077.100.032* **and** destination address *201.128.011.034*:

```
#filter
IP:
010 AND src-addr = 192.077.100.032;
020 ACCEPT dst-addr = 201.128.011.034;
```

The following rule example limits a user to one host with an input filter:

```
#filter
IP:
010 ACCEPT dst-addr = 143.134.45.56;
020 DENY;
```

Masks

These fields specify the number of bits to be used in the source address and destination address comparisons. Valid values are:

- 0 - Match all packets with any IP address. The contents of *source address* or *destination address* fields are unimportant
- 8 - Compare the first byte (octet) in the IP addresses.
- 16 - Compare only the first two bytes of the IP addresses
- 24 - Compare only the first three bytes of the IP Addresses
- 32 - Match the entire IP address (*default*)

The masks are separated from *source address* and *destination address* by forward slashes (/).

TCP and UDP Parameter Filtering

TCP and UDP packets are typically sent from and destined for standard port numbers that provide common network services, such as Domain Name Service, SNMP, and TELNET. You can filter TCP and UDP packets by source and destination ports by defining filter rules that compare the port number in a TCP or UDP packet to a specific value.

The following rule example accepts only TCP packets that have a source port number of 24 or greater.

```
#filter
IP:
010 ACCEPT tcp-src-port >= 24;
020 DENY;
```

The following rule example accepts only TCP packets that have a destination port number that is in the range of 24 to 39:

```
#filter
IP:
010 AND tcp-dst-port > 23;
020 ACCEPT tcp-dst-port < 40;
030 DENY;
```

The following rule example accepts only UDP packets that have a destination port number that is in the range of 24 to 39:

```
#filter
IP:
010 AND udp-dst-port > 23;
020 ACCEPT udp-dst-port < 40;
030 DENY;
```

The following rule example rejects TCP and UDP packets:

```
#filter
IP:
010 REJECT protocol = tcp;
020 REJECT protocol = udp;
```

Standard Port Numbers

The table below lists standard port numbers for common services. For a complete list, see the most recent "Assigned Numbers" RFC.

TCP	UDP	Description
20	-	File Transfer Protocol (data)
21	-	File Transfer Protocol (control)
23	-	Telnet
25	-	Simple Mail Transfer Protocol
43	43	Who Is
53	53	Domain Name Service
-	69	Trivial File Transfer Protocol
70	70	Gopher
79	79	Finger
80	-	World Wide Web HTTP
88	88	Kerberos
110	-	Post Office Protocol - Version 3
111	111	Sun Remote Procedure Call
113	113	Authentication Service
119	-	Network News Transfer Protocol
123	123	Network Time Protocol
161	161	SNMP (Total Control Manager)
162	162	SNMP trap
220	220	Interactive Mail Access Protocol v3
512	-	remote process execution
513	-	remote login (rlogin)
-	513	remote who (rwhod)
514	-	remote command (rsh)
-	514	Syslog accounting
515	-	lpd spooler
517	517	talk (terminal to terminal chat)
518	518	ntalk (new terminal chat)
-	520	RIP
540	540	uucp (UNIX to UNIX copy)
540	540	uucp-rlogin
543	543	klogin (Kerberized login)
1642	-	PortMux daemon
-	1645	RADIUS security
-	1646	RADIUS accounting

IP and IPX-RIP Packet Filtering

Routing Information Protocol (RIP) packets identify all attached networks and the number of router hops required to reach them. These responses are used to update a router's routing table. Define IP/IPX-RIP filtering rules in the IP-RIP and IPX-RIP protocol sections of the filter.

For example, to filter all routes except the IP network address *195.120.254.145*:

```
#filter
IP-RIP:
010 ACCEPT network = 195.120.254.145;
020 DENY;
```

This filter allows route *195.120.254.145* into the table, rejecting all others.

For example, if you want to filter all but the following IPX networks, type:

```
#filter
IPX-RIP:
010 REJECT network != 00-00-99-ff;
020 REJECT network != 99-88-0-45;
030 REJECT network != 0-8-7-5;
```

To filter an IP route based on a subnet mask (all but 195.223.0.0 networks):

```
#filter
IP-RIP:
010 REJECT network = 195.223.87.225/16;
```



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

IPX-SAP Filtering

IPX-SAP filtering rules are defined in the IPX-SAP protocol section of the filter file. The IPX-SAP filtering process compares advertised server name, service type, network number, node (host) address and socket number values to values defined in the IPX-SAP filter rules.

For example, to allow a packet to pass if it is advertised from the server named *sales_1* and its socket number is less than 32, type:

```
#filter
IPX-SAP:
010 ACCEPT server sales_1;
020 ACCEPT socket < 32
```

When applied to an input filter, the following example will permit SAP service type 04 and deny everything else from entering:

```
#filter
IPX-SAP:
010 ACCEPT service 04
```

ICMP Packet Filtering

ICMP packets contain messages exchanged by IP modules in both hosts and gateways to report errors, problems and operating information. ICMP message types are listed below. Note that most are error messages necessary for the correct operation of TCP/IP:

Type	Description
0	Echo Reply (Ping)
3	Destination Unreachable
4	Source Quench
5	Redirect (change route)
8	Echo Request (Ping)
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request

14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

If you're concerned about security, filter out incoming *type 5* messages. Sending ICMP redirects is an easy way for a vandal to change your routing tables. Although *ping* is a troubleshooting aid, it allows a potential intruder to obtain a map of your network by systematically pinging every possible address. If you're worried, filter out incoming *type 8* packets or outgoing echo replies (*type 0*).

For example, to prevent vandals from changing your routing tables by sending ICMP redirects, type:

```
#filter
IP:
010 REJECT icmp-type = 5
```

IP/IPX-Call Filtering

You define IP/IPX-call filtering rules in the IP-CALL, IPX-CALL protocol sections of the filter file. Like the rules defined in the IP protocol section, the IP-CALL filtering rules compare the advertised source or destination network address, host address and port number and values defined in the IP-CALL filter rules. IPX-CALL filtering rules compare source/destination network addresses, hosts and socket numbers.



Note: Call filtering occurs after output filters are processed and are used for ondemand calls only.

For example, to allow outgoing calls from the user of IP address *192.112.42.6*:

```
#filter
IP-CALL:
010 ACCEPT src-addr = 192.112.42.6;
020 DENY;
```

For example, to allow outgoing calls to IPX host *77-88-99-aa-bb-cc*, and reject calls from the source socket number *0x3f00*, type:

```
#filter
IPX-CALL:
010 ACCEPT dst-host = 77-88-99-aa-bb-cc;
020 REJECT src-socket = 0x3f00;
```

Login-Access Filtering

Login-Access filters are used to restrict login user accessibility to hosts connected to HiPer ARC. Filtering rules are set in the LOGIN-ACCESS protocol section of the filter file, using a subnet mask to restrict access from approved networks.

For example, to filter the host where login users initially connect to, type:

```
#filter
LOGIN-ACCESS:
010 ACCEPT dst-addr = 187.243.71.54/24
```

This filter allows users on network 187.243.71.0 to access the configured host but rejects all others.

HiPer ARC Global Filtering

HiPer ARC can filter packets globally traveling in and out of dial-up ports as well as the network port. The options below provide tighter network security.

Global Switch to Drop IP Fragments with Offset = 1

This global switch lets you discard all IP packets with an offset value equal to 1. This packet type typically occurs when a system is under attack from a user trying to bypass installed filters on an interface by sneaking the packet by the filter in fragmented form.

HiPer ARC never generates a packet with an offset of 1. Some routers used on the same network HiPer ARC may be configured to filter out specific traffic. In some cases, these routers may not apply the filter correctly. Should this happen, those packets will be discarded. In accordance with RFC 1858, this security feature syslogs every instance of a packet being discarded. The commands associated with this feature are:

```
enable ip security_option drop_all_fragoffset1 (default)
```

```
disable ip security_option drop_all_fragoffset1 ENTER
```

Global Switch to Drop Packets with a Partial TCP Header

This global option allows the global configuration to discard all IP packets with a partial TCP header. This command is similar to and a subset of the **enable ip security drop_all_fragoffset1** command. The default setting is *enabled* meaning these packets will be discarded. When a packet is discarded the event is syslogged. The commands associated with this feature are:

```
enable ip security_option drop_tcp_fragoffset1 (Default)
```

```
disable ip security_option drop_tcp_fragoffset1 ENTER
```

Global Switch to Filter Out All IP Options

Sometimes IP options may be generated from an outside source in an attempt to get past routing tables in a network. HiPer ARC provides a global feature to filter out all IP packets with IP options. By using the command below, you can discard all packets like this, which will create a SYSLOG message each time one of these packets is discarded. The commands associated with this feature are:

```
enable ip security_option allow_all_header_options ENTER
```

```
disable ip security_option allow_all_header_options (Default)
```

Global Switch to Filter Out IP Source Route Options

This global option addresses the particular path a sender chooses to take through the network to reach its destination, as specified in the sender packet's IP header. Using this command, you can discard packets of this type although this is a lower level of security than All Header Options. The commands associated with this feature are:

```
enable ip security_option disallow_source_route_options ENTER
```

```
disable ip security_option disallow_source_route_options (Default)
```

Keywords

This section describes valid keywords you can use for each protocol section.

IP and IP-CALL Sections

Keyword	Description	Operators	Value
src-addr	source IP address	= or !=	ddd.ddd.ddd.ddd/mask
dst-addr	destination IP address	= or !=	ddd.ddd.ddd.ddd/mask
tcp-src-port	TCP source port #	all	1-65536
tcp-dst-port	TCP destination port #	all	1-65536
tcp-one-way	Not supported in this release		
udp-src-port	UDP source port #	all	1-65536
udp-dst-port	UDP destination port #	all	1-65536
icmp-type	ICMP message type	= or !=	0-255
protocol	protocol-specific field	= or !=	udp, tcp, icmp
generic	field offset, length, mask values	generic	generic

IP-RIP Section

Keyword	Description	Operators	Value
network	IP network address	= or !=	ddd.ddd.ddd.ddd/mask

IPX and IPX-CALL Section

Keyword	Description	Operators	Value
src-net	source network address	= or !=	xx.xx.xx.xx
dst-net	destination network address	= or !=	xx.xx.xx.xx
src-host	source host address	= or !=	xx.xx.xx.xx.xx.xx
dst-host	destination host address	= or !=	xx.xx.xx.xx.xx.xx
src-socket	source socket number	all	1-ffff in form 0Xxxxx
dst-socket	destination socket number	all	1-ffff in form 0Xxxxx

IPX-SAP Section

Keyword	Description	Operators	Value
network	network address	= or !=	xx.xx.xx.xx
node	node address	= or !=	xx.xx.xx.xx.xx.xx
server	server name	= or !=	character string (max 32)
service-type	service type	= or !=	0-ffff in form 0Xxxxx
socket	socket number	all	1-ffff in form 0Xxxxx

LOGIN-ACCESS Section

Keyword	Description	Operators	Value
dst-addr	destination host address	= or !=	ddd.ddd.ddd.ddd



10

ADMINISTRATIVE TOOLS

This chapter covers administrative commands used for:

- Reconfiguring your system
- Communicating with a remote or local site
- Troubleshooting
- Displaying system information
- Performing a FLASH or network download

Reconfiguring Your System

Customizing CLI Parameters

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

Command Prompt

Use **set command** if you have more than one HiPer ARC and want to differentiate between them or you just want to customize your prompt from the default. The prompt can be up to 64 characters. Type:

```
set command prompt <"prompt message">
```

For example:

```
set command prompt Welcome! ENTER
```

Command History

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

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

Idle Timeout

If you want to ensure that a console login user is employing the link constructively - and not leaving the system vulnerable to a security breach - set an *idle timeout* using the following command:

```
set command idle_timeout <0-60 minutes>
```

For example:

```
set command idle_timeout 5 ENTER
```

Login Required

You can force a console user to login after the idle timeout interval has elapsed. Type:

```
set command login_required [yes | no]
```

Local Prompt

If you want to specify a separate prompt for a command file process, use the *local_prompt* parameter. This value is useful if you are running a number of processes and want to differentiate between the global and session prompts. Or, if you are Telnetting to the system, for instance, and want to create a separate, easily identifiable prompt. If your prompt consists of more than one word, remember to enclose it in quotes. Type:

```
set command local_prompt <string>
```

For example:

```
set command local_prompt "TELNET Session" ENTER
```

Setting the System

The **set system** command designates a name and location for your system, contact information and a keyword necessary to make a PPP connection to a remote router over the WAN. Use this command:

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

For example:

```
set system name "big house" location DC contact "staff, ext 555" transmit_system_na "FOB" ENTER
```

Running Script Files

The **do** command is a powerful tool to configure multiple users, protocols or other functionality by running a script file containing CLI commands. To use this command, create a file containing the CLI commands you want to implement, TFTP the file to the FLASH ROM, and type **do** <filename>. See the example below covering many system functions. Some commands are commented out or abbreviated.

```
;  HIPERARC CONFIGURATION FILE;
;  FACILITIES LOGLEVEL;
set facility ip loglevel verbose
set facility ppp loglevel verbose
set facility user loglevel verbose
set facility call loglevel verbose
;
;  SYSTEM INFO;
set system name "marauder"
set system contact "Henry Stimson"
set system location "3Com Lab"
;
;  SETTING THE SYSTEM COMMAND PROMPT;
```

```

;set command prompt "HiPer ARC"
;
;   SETTING THE SYSTEM COMMAND HISTORY;
;set command history 100
;
;   SNMP COMMUNITIES;
add snmp community sqatest a 0.0.0.0 a rw
add snmp community bearcat a 0.0.0.0 a rw
add snmp community public a 0.0.0.0 a ro
add snmp trap sqatest a 157.172.248.54
;
;   IP NETWORKS;
add ip network "ipnet-157.172.248.0" address 157.172.248.38/c int eth:1
set ip network "ipnet-157.172.248.0" routing_protocol ripv1
;set ip network "ipnet-157.172.248.0" routing_protocol ripv2
;set ip network "ipnet-157.172.248.0" routing_protocol none
;set ip network "ipnet-157.172.248.0" rip_policies ripv1_rec ripv1_receive ripv1
;
;   ADDING STATIC IP ROUTES;
;add ip route 204.249.182.0 gateway 157.172.228.1 metric 1 mask 255.255.255.0
;
;   DNS ADD;
add dns host louvre address 157.172.248.54
add dns host wimpy address 157.172.248.40
;add dns server preference 1 address 157.172.248.40 name louvre
;
;   SYSLOG HOST ADD;
add syslog 157.172.248.54 loglevel verbose
;
;   LOCAL AUTHENTICATION;
enable authentication local
;
;   REMOTE AUTHENTICATION;
set authentication primary_server 2.3.4.5 primary_secret testing123
secondary_server 157.172.248.40 secondary_secret testing456
;
;   REMOTE AUTHENTICATION;
; enable authentication remote
;
;   ACCOUNTING;
set accounting primary_server 157.172.248.54 secondary_server 157.172.248.40
enable accounting
enable ip rip
enable ip routing
enable security_option remote_user_administration telnet
;
;   LINK TRAPS;
enable link_traps interface slot:4/mod:1
enable link_traps interface slot:4/mod:2
enable link_traps interface slot:4/mod:3
enable link_traps interface slot:4/mod:4
enable link_traps interface slot:4/mod:5
enable link_traps interface slot:4/mod:6
enable link_traps interface slot:4/mod:7
enable link_traps interface slot:4/mod:8

```

```

;
;   AUTHENTICATION TRAPS;
enable snmp authentication traps
set ppp receive_authentication pap
;set ppp receive_authentication chap
;
;   ADDING USERS;

; ROOT - ADMIN/MANAGER;
add user root password root type manage
;
;   NETWORK_SERVICE;
;enable network_service root
add user henry type network,dial_out
set network user henry ip_routing both
set network user henry send_password georgef
;
add user son type network
set network user son remote_ip_address 157.172.248.105/c
set network user son ip_routing both send_password gordo
set network user son address_selection negotiate
;
save all

```

Using Chat Scripts

Chat-style scripts can be used to support dial in users, including setting up a TELNET session, reporting IP and gateway addresses, and runtime errors, setting timeouts, and disconnecting calls. HiPer ARC supports chat scripts locally as well as remotely for RADIUS users. For detailed information about chat scripting including syntax, constructs and additional examples, see *Appendix E: RADIUS and TACACS+ Systems*.

See below for an example of a HiPer ARC-supported chat script. Use this script to TELNET to either of two fixed hostnames (*abc.com* or *def.com*) depending upon user's input.

```

TIMEOUT 60;

begin:
    SEND "Enter Remote Host Name:";
    EXPECT %login_host;
    IF ($login_host == "abc.com") GOTO telnet;
    IF ($login_host == "def.com") GOTO telnet;
    IF ($login_host == "logout") GOTO exit;
    SEND "Invalid choice";
    GOTO begin;

telnet:
    TELNET $login_host;

exit:
    HANGUP

```

Bootup Options

Using the Boot Configuration Menu

The Boot Configuration Menu is a handy tool to perform:

- firmware upgrades from FLASH memory or a network source

- reboots after system crashes
- diagnostic tests
- configuration deletions

The menu appears following power up (or a reboot) and after your screen has registered system initialization, kernel loading and several enabled processes. If you don't enter a choice in the open menu field within 15 seconds, the system will exit the menu and return to the HiPer ARC prompt.



As an alternative, you can use CLI boot commands such as `set bootrom config` and `set bootrom ip interface` to accomplish the same purpose as choosing the following menu options.

HiPer Access Router Boot Configuration		
1.	Boot mode	:FLASH
2.	IP Configuration Source	:STATIC
3.	Boot IP Interface	:eth:1
4.	Boot IP Address	:149.112.217.148
5.	Boot IP Default Gateway	:149.112.217.254
6.	Boot IP Network Mask	:255.255.255.0
7.	TFTP Image on Startup	:NEVER
8.	TFTP Boot Server IP Address	:149.112.213.1
9.	TFTP Boot Image File Name	:neo40001.dmf
10.	Crash upload	:DISABLED
11.	Crash Dump Upload Filename	:
12.	Manufacturing Diagnostics	:NONE
13.	Delete Router Configuration	:NO
14.	Delete Boot Configuration	:NO
15.	Command Line Parameters	:
E	Exit	
	Enter Choice	[E]

Boot Configuration Menu Options

Boot mode: FLASH or NETWORK. Option lets you automatically bootup from HiPer ARC's FLASH memory or from a network source you specify. If you opt to change the default *FLASH* setting to *NETWORK*, you'll need to enter more information to enable a TFTP server to supply the configuration files. To update your system image you must specify additional TFTP information in options 5 and 7 - 12.

IP Configuration Source: STATIC or BOOTP. The default *STATIC* option accepts the configuration stored in FLASH ROM. If you choose *STATIC* it uses the information entered in options 8 - 12 to configure the kernel's networking stack (but not the HiPer ARC router core). The *BOOTP* option accepts the configuration from a TFTP server you specify separately on your LAN.

Boot IP Interface: eth:1 or eth:2. The eth:1 LAN interface is the default. Eth:2 can be selected as a dedicated port for diagnostic purposes. The interface which is selected when you EXIT (E) will be used by the kernel to access the Ethernet prior to the router core being enabled.

Boot IP Address: ENTER VALUE. The kernel contains a networking stack allowing you to download files, upload a crash dump and perform other work. You should configure an IP address for the kernel to use. You can reuse the same address you assign to the HiPer ARC stack because the two stacks are never active at the same time. The address displayed is provided as a factory default. You must change it to specify the IP address of the LAN interface.

Boot IP Default Gateway: ENTER VALUE. The address displayed is provided as a factory default. You must change it to specify the HiPer ARC's IP address (default route).

Boot IP Network Mask: ENTER VALUE. The network mask displayed is provided as a factory default. You must change it to reflect the netmask of the LAN interface.

TFTP Image on Startup: ONCE, ALWAYS, NEVER. These choices specify how often you want to reboot the HiPer ARC from the image on the TFTP server. Choosing *ONCE* will update your software from the network via TFTP the *next* time you reboot and thereafter from FLASH, *ALWAYS* will continually update your software via TFTP, and *NEVER* (the default) will boot from your internal FLASH only.

TFTP Boot Server IP Address: ENTER VALUE. The IP address displayed is provided as a factory default. Change it to specify the IP address of the host from which the boot image will be downloaded and crash dump information will be uploaded. If you have enabled crash dumps you must fill in this field.

TFTP Boot Image File Name: The file and path displayed are provided as a factory default. Change it to specify the file and full path of the file to be downloaded. If you have enabled crash dumps you must fill in this field.

Crash Upload: DISABLED or ENABLED. Changing the default (DISABLED) to ENABLED will, following a board crash, automatically compress crash dump information and the entire memory and TFTP the crash dump to a server. The server's IP address must be configured via option 2.

Crash Dump Upload Filename: Crash dump information is written to the file you specify in the TFTP server if you have enabled the Crash upload in option 10. The crash dump filename should have 777 permissions if the server is a UNIX workstation.

Manufacturing Diagnostics: NONE, POST or INTERACTIVE. The default NONE runs the standard set of power-up diagnostics, POST runs a standard set of Power-on Self Test diagnostics and print a table of tests run and their results, and INTERACTIVE runs tests similar to HDM tests. This feature is designed for field debugging and is not meant for regular use.

Delete Router Configuration: NO or YES. Choose YES if your HiPer ARC configuration files were corrupted. All configuration files (*.cfg) stored in FLASH will be deleted without reformatting FLASH and operational code is kept intact. The *Quick Setup* program will be initiated to let you reconfigure HiPer ARC. See *Chapter 2: HiPer ARC Setup* for more information about Quick Setup. NO preserves your HiPer ARC router configuration.

Delete Boot Configuration: NO or YES. Switching from the default (NO) will cause your current boot configuration to be deleted and defaults restored.

Command Line Parameters: Indicates parameters being passed to the router-core application when the system boots. In general, this option is not user-configurable but some values may appear if HiPer ARC is configured from the CLI to reboot with a specific bulk configuration file. We recommend you do not explicitly use this option.

Exit - Use to leave this menu after using other options and boot the board. If the menu is left idle for more than a few moments, the system will return to the HiPer ARC prompt.

Software Downloads

You can download new code to HiPer ARC in several ways. The methods differ by offering: remote capability or requiring a local connection, a GUI or terminal emulation display, and easy or more complex set up. They are:

- *Total Control Manager* (TCM). This is the easiest, *recommended* method. The TCM offers a *GUI*, works on the fly and can be utilized *remotely*. See the TCM documentation for more information.
- The *TFTP startup*. This choice in the *Boot Configuration Menu* is described in the preceding section.
- *Zmodem* protocol using the Windows terminal emulator *HyperTerminal*. This method is easy but requires that you wait for the initial boot prompt pause - an interval lasting only 5 seconds - and download the file before the Boot Configuration Menu appears. This method requires a direct Console connection and reboots HiPer ARC. The steps are:
 - 1 At the boot prompt, click on your **right** mouse button.
 - 2 Click on **Send File...** and select **Send File**
 - 3 Specify a name in the **Filename:** field and click on **Send**.
 - *AT{Z}* command. Issuing the *AT{Z}* command at the initial boot prompt will also download files but is tricky considering the 5-second timeframe. This method requires a direct Console connection and automatically reboots HiPer ARC.
 - *AT{Z[F]}* command. Issuing the *AT{Z[F]}* command is similar to the *AT{Z}* command except for the additional function of formatting your FLASH memory. This method requires a direct Console connection and automatically reboots HiPer ARC.

TELNETd Access Port

The TELNETd Access Port identifies the specific TCP port number for incoming TELNET sessions. The default is **23**, TELNET's well-known port number.

You can change this access port number; the range is 1 to 65535. Note that 10000 through 10100 are reserved for an internal filter used for host device port security. Use the following command to change the *existing* TELNETd network service:

```
set network service telnetd server_type telnetd socket <number>
```




Some administrators consider using port 23 for remote administration a security risk since anybody can get a login prompt simply by telnetting to the system. This allows a potential vandal to seize control of HiPer ARC.

*Changing to a non-standard port adds protection by making a potential vandal guess which port the system is listening to. Alternatively, you can disable TELNET administration altogether by setting this parameter to **0** or issuing the **disable network service telnetd** command.*

Discarding and Renaming Files

There are several **delete** commands you can use to discard various files.

- **Delete configuration** discards all configuration files, reboots the system and restores system configuration to factory defaults
- **Delete file** removes a file from the FLASH file system
- **Delete filter** pulls a filter entry from the filter table and discards it from FLASH memory
- **Rename file** copies files within the FLASH file system. Use the command:

```
rename file <input_file> <output_file>
```

Using the CLI Editor

Edit Command

HiPer ARC's text editor (the **edit** command) works at the command line similar to UNIX Version 7's edit facility with some subtle differences. Its purpose is similar - to perform simple line editing of files, including filter files.



Edit is especially useful for editing filter files. It may not be as convenient when creating large filter files, though. An alternative to editing filter files internally uses TFTP to import files to HiPer ARC but this method requires that files be created and edited externally (see Chapter 8: Packet Filters).

Edit is available on the Console, through a dialed-in connection, or via TELNET. It works best when displayed on an ANSI terminal since it employs escape sequences defined for the ANSI terminal type to clear screens and display menus. Rules that apply to edit's use include:

- Edit opens *existing* files with the format: **edit** <file_name>.
- Two modes are available:
 - *Command*, in which a colon is displayed at the bottom of the screen to prompt for a command;
 - *Input*, in which all keyboard output is added to the file.
- While in command mode, Input mode is accessed by issuing either **i** or **a** commands.
- While in input mode, the command mode is restored by entering a line consisting of a single *period* (**.**). If you wish to write such a line, you can do so by entering two periods, then using the **s** command to change these to only one period.
- Commands consist of an optional line-range, a single character indicating the command, and other commands for an optional third argument.

- Line-range consists of either a single line number or a first-line number and last-line number separated by a comma (,).
- The carot character (^) refers to the first line of the file, the dollar sign (\$) refers to the last line.
- Filter files created with this command are *not* added to the Filter Table until you issue the **add filter** command; then use the **list filter** command to display them.

Refer to the table below for a list of edit commands. They can also be obtained from CLI help.

CLI Edit Commands	
<newline>	If a line is specified, it makes that line the new current line. Otherwise it advances the current-line-pointer by one line.
=	Equal sign prints the line number of the current line.
.	Period prints the current line.
-	Minus sign moves current-line-pointer back one or more, and prints new current line. Example: 5- moves line pointer back five lines.
+	Moves current-line-pointer forward one line, and prints new current line. Can also move cursor by multiples. Example: +++ moves cursor three lines forward.
^	Carot adds a line to the file.
\$	Dollar sign places cursor at end of last line of file.
/	Slash searches for text selection. Example: / <i>blah</i> finds first instance of "blah"
a, A	Enters <i>input</i> mode with a new line following current line. (Input mode is terminated by an input line containing a period in the first column.)
i, I	Enters <i>input</i> mode with a new line preceding current line. (Input mode is terminated by an input line containing only a period in the first column.)
c, C	<i>Copies</i> the specified range of lines to follow line number given. Example: 5,7c7 puts a copy of lines 5 - 7 after line 7.
d, D	<i>Deletes</i> specified range of lines (or current line). Leaves current-line-pointer at the following line.
f, F	<i>Prints</i> filename, or sets it to a new name if specified. <i>Finds</i> specified string selection and displays it. Example: f/ <i>alpha</i> / finds the "alpha" selection and displays whole string.
m, M	<i>Moves</i> specified range of lines to follow line number given. Example: 5,7m3 moves lines 5 - 7 "up", to follow line 3.
p, P	<i>Prints</i> specified lines.
q	<i>Quits</i> editor. This fails if edit buffer contains any changes. If so, use Q instead.
Q	Quits the editor. Any changes are discarded.
r	Replaces text on line. Using C f moves the cursor forward, C g moves the cursor backwards.
s, S	Substitutes text on current line. Example: s/ <i>alpha</i> / <i>beta</i> / finds the string "alpha" and replaces it with "beta".
v, V	Verifies filter. Considering this file as a filter, it verifies the file's contents via the Filter Manager.
w, W	Writes to file. If a filename is given, it is used and becomes the current filename. If a range of lines is specified, only those lines are written.
x, X	Saves and exits file.

Communicating with Remote and Local Sites

IGMP Forwarding

HiPer ARC's implementation of multicast forwarding employs the Internet Group Management Protocol (IGMP) to efficiently deliver IP traffic to a set of dial-in clients configured as members of a multicast group. Bandwidth is conserved by forcing the network to replicate packets from a single source to multiple clients only when necessary. This type of packet transfer is especially effective for applications which require large-scale dissemination such as network ticker tapes, live stock quotes, RealAudio, videoconferencing and shared whiteboards.

HiPer ARC's support of IGMP includes *proxy multicasting*, a method to allow the forwarding of packets all the way from the Internet Multicast Backbone (MBone) - a large virtual network of multicasting subnetworks and routers - through HiPer ARC out to its multicast member hosts.

How it Works

IGMP multicasting is initiated by routers seeking to learn the presence of group members configured on their directly attached subnetworks (standard group members are identified by IGMP addresses allocated in the Class D range from 224.0.0.0 - 239.255.255.255). HiPer ARC (or another router) sends queries out its modem (or Ethernet) ports, a host receives these queries and transmits report messages for each multicast group it seeks to join. HiPer ARC accepts these reports from the hosts and adds group members to its IGMP Multicast Table. See the illustration below.

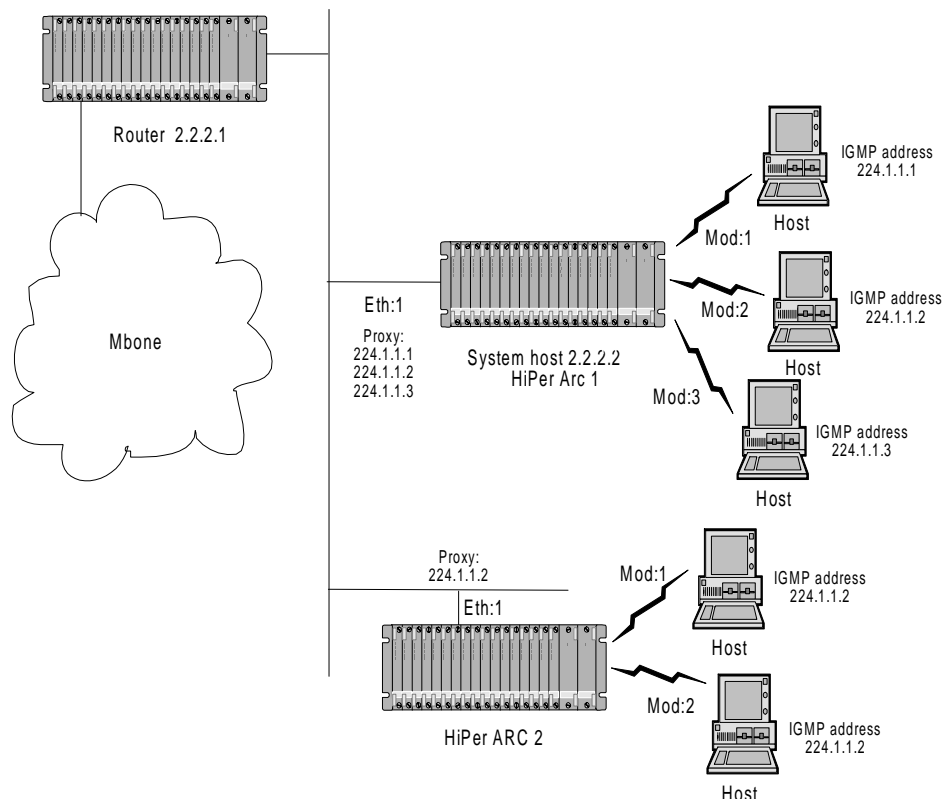


Figure 10-1 IGMP forwarding topology

In the example above, IGMP is run on each of the HiPer ARC interfaces on which an IP network has been configured. IGMP is run on the common Ethernet to which both the remote router and HiPer ARCs are attached. IGMP is also run on each WAN interface between a multicast host and HiPer ARC.

Since multicast group memberships are interface-specific, their existence is not shared between interfaces. So, multicast groups learned on HiPer ARC's WAN (modem) interfaces would not be advertised on HiPer ARC's Ethernet interface and the remote router shown above would not learn of any multicast groups learned on the HiPer ARC's modems. This problem is addressed by HiPer ARC proxying its WAN interface connections on the Ethernet interface so that when a multicast group is joined on a WAN interface, it is automatically joined on the Ethernet interface, allowing the remote router to learn of all HiPer ARC-connected multicast hosts.

Proxy multicasting completes the IGMP forwarding structure with one caveat: the administrator should ensure that there is only **one** connection to the Mbone so that no loops exist in the network. **No** WAN connection can be connected back to the Mbone other than through HiPer ARC. This prohibition is equally important for users configured on a RADIUS server.

Efficient discovery of all reporting multicast groups across the LAN-WAN is regulated by IGMP in such a way that the router with the lowest source IP address is designated a *querier*, while other routers become *non-queriers*. Multicast groups joined via the CLI by HiPer ARC are identified in the table as *self* entries and multicast groups learned on the network from other routers or hosts are identified as *learned* entries.

Table entries identified as *proxy* are groups that have been joined on a client interface and are being joined on the proxy interface for multicast forwarding. Also, entries can be identified by any combination of the three methods. If designated a non-querying router, HiPer ARC will function as a multicast client and report its associated multicast group members to the querier.

Step by Step Instructions

HiPer ARC's IGMP support is configured via *interfaces* and *users*. Interfaces are mapped to *multicast addresses* and enabled for *multicast forwarding*, *proxy* or other optional parameters. Local (or RADIUS) user profiles are configured as type *network* with the option of setting similar parameters. Default values render interface and user configuration simple. Follow the steps below.

- 1 Configure LAN settings of the HiPer ARC interface for IGMP. Creating an IP network automatically configures an IGMP interface, with all values taking default parameters except the *name* and *address*, unless you specify otherwise. Use the following command:

```
add ip network <name>
  address [IP_address]
  enabled [on | off]
  frame [snap | ethernet_ii]
  interface [eth:1 | eth:2 | slot:x/mod:y]
```

For example, configure an IGMP network named *hiperarc1*, with an IP address of 2.2.2.2, and these default values (not specified): *eth:1* interface, frame type *ethernet_ii* and enabled *on*.

```
add ip network hiperarc1 address 2.2.2.2 ENTER
```

- 2 If your IGMP clients are connected to HiPer ARC's modems, select a modem interface - slot:x/mod:y. If you want to configure HiPer ARC as a multicast client - regardless of its IP address in respect to other router addresses - make sure *routing* is *disabled*. *Routing*, *multicast forwarding* and *multicast proxy* are disabled by default. For more information on command values, see below. Use the command below:

```
set ip igmp [interface]
  query_interval <5-65,535 seconds>
  max_response_time <1-10 seconds>
  version <1-2>
  robustness <1-5>
  routing <enabled | disabled>
  multicast_forwarding [enabled | disabled]
  multicast_proxy [enabled | disabled]
```

<interface_name>	The interface on which IGMP is enabled: eth:1 , eth:2 or slot:x/mod:y
max_response_time	The interval a host has to respond to the IGMP query. Default: 10 . Range: 1-10 seconds
multicast_forwarding	Multicast packets are forwarded when enabled. Default: Disabled
multicast_proxy	Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with the set ip multicast proxy interface command. Default: Disabled
query_interval	The frequency at which IGMP Host-Query messages are sent on the specified interface. Default: 125 . Range: 5-65535
robustness	Tuning parameter for expected packet loss on a subnet. If packet loss on a subnet is expected to be high, robustness may be increased. Range: 1-5 . Default: 2
routing	Will attempt to become the IGMP querier on the specified interface. Default: Disabled
version	The version of IGMP running on this interface. This object can be used to configure a router capable of running either version. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. Default: 2

For example, to configure an IGMP interface on HiPer ARC with *multicast forwarding*, *routing* and *proxy* enabled, type:

```
set ip igmp slot:3/mod:1 routing enabled multicast_forwarding enabled multicast_proxy enabled
ENTER
```

- 3 Configure WAN settings for a network user employing IGMP. The following command includes values reflected in the preceding interface command. In the case where user and interface values differ, user values supercede those set on the interface. The following example assumes you've created a user *lynne*.

```
set network user <name> igmp
  query_interval <5-65,535 seconds>
  max_response_time <1-10 seconds>
  version <1-2>
  robustness <1-5>
  routing <enabled | disabled>
  multicast_forwarding [enabled | disabled]
  multicast_proxy [enabled | disabled]
```

For example, to configure an IGMP user with *routing*, *multicast_proxy* and *multicast_forwarding*, *version 1* and retain other defaults, type (abbr.):

```
set net user lynne igmp rout ena multicast_f ena multicast_p ena ver 1 ENTER
```

- 4 Configure the interface you want to *proxy* discovered multicast groups onto. You can set the HiPer ARC Mbone proxy as a LAN **interface** - *Eth: 1* or *Eth:2* - or a WAN interface with the name of a **user**. After a WAN proxy is specified, the *first* configured user who dials up HiPer ARC sets the modem it happens to be connected on as the proxy interface. After that user hangs up, all proxied groups are removed from the IGMP Multicast table. If that user dials in again, the proxy interface is set on a new modem interface. See graphic below.

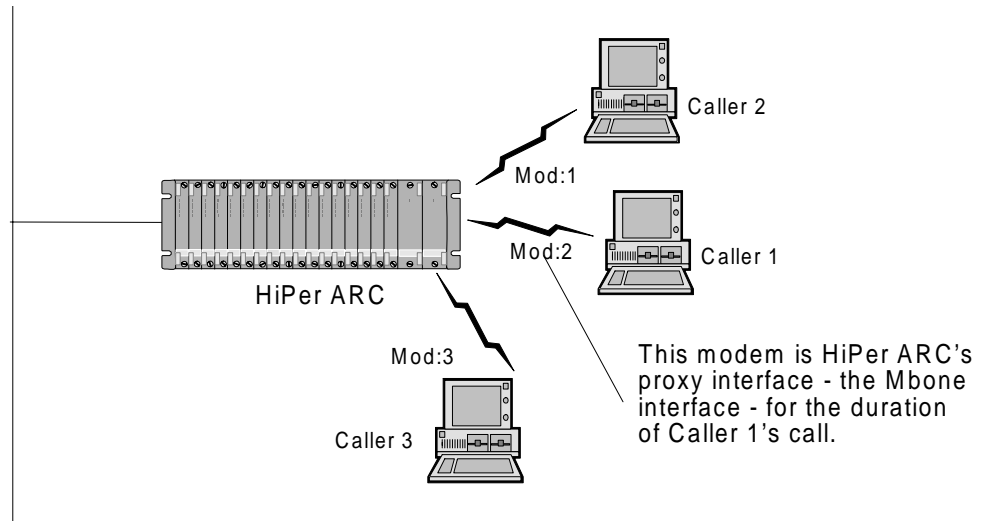


Figure 10-2 Proxy interface selection



*Important: Only **one** proxy interface can be set on HiPer ARC.*

Use the following command:

```
set ip multicast proxy interface <interface or user_name>
```

An example of an Ethernet proxy interface:

```
set ip multicast proxy interface eth:1 ENTER
```

or, an example of a WAN proxy interface:

```
set ip multicast proxy interface lynne ENTER
```

- 5 *Optionally*, configure the source address for all IGMP packets sent from HiPer ARC. With this value set, all IGMP packets will identify this address as their source address regardless of any other configured IP networks. If this value isn't set, all IGMP packets will take the IP host address (HiPer ARC's first enabled Ethernet address - *Eth:1* or *Eth:2*) as its source address. Use this command:

```
set ip application_source_address igmp <IP_address>
```

For example:

```
set ip application_source_address igmp 5.5.5.5 ENTER
```

- 6 *Optionally*, configure the *multicast heartbeat* function to monitor multicast traffic for a particular multicast group on a specified interface. This feature often is used to verify the connection to the Mbone. You can set a *window* which describes the number of times multicast traffic is received, a *time* which describes the interval to monitor multicast traffic, and a *threshold* which describes the number of intervals multicast traffic is received within the window before an SNMP trap is issued. Also, issue the command enabling the feature.

Use the following commands:

```
set ip multicast heartbeat
  interface <interface_name>
  group <ip_multicast_address>
  time <interval>
  threshold <number>
  window <number>

enable ip multicast_heartbeat
```

<interface_name>	The interface on which to monitor multicast traffic for the specified group: eth:1, eth:2, slot:x/mod:y
group	The IP address of the multicast group to monitor.
time	The interval, in seconds, to monitor multicast traffic. Range: 0 - 65535 . Default: 60
threshold	The interval during which multicast traffic is not received after which an SNMP trap is issued. Range: 0 - 65535 . Default: 3
window	The number of periods (in <i>time</i> values) to monitor multicast traffic. Range: 0-255 . Default: 5

For example:

```
set ip multicast heartbeat interface eth:1 group 239.1.1.3 time 60 threshold 2 window 8 ENTER

enable ip multicast_heartbeat ENTER
```

- 7 Display the IGMP multicast systems known to HiPer ARC and verify IGMP settings you've configured by issuing the following commands:

```
list ip igmp

show ip igmp <interface_name>

show ip settings
```

For example, use the following command to verify IP address/interface correlations and the discovered status of your multicast groups:

```
li ip igmp ENTER
```

The command displays:

Interface	Multicast Address	Status
slot:1/mod:1	224.1.1.1	SELF
slot:1/mod:2	224.1.1.2	SELF/LEARNED
slot:1/mod:3	224.1.1.3	SELF

For example, use the following command to verify *multicast forwarding*, *routing* and *proxy* settings for a particular interface (slot:1/mod:1):

```
show ip igmp slot:1/mod:1 ENTER
```

The command displays:

IGMP Interface	slot:1/mod:1
Query Interval	125 seconds
Max Response	10 seconds
Version	2
Querier	2.2.2.1
Joins	1
Groups	1
Robustness	2
Routing	ENABLED
Multicast Forwarding	DISABLED
Multicast Proxy:	ENABLED
IGMP Short Packets	0
IGMP Bad Checksum	0
Queries Received	1
Reports Received	2
Reports For Known Groups Received	0
Wrong Version Reports Received	0
Reports Sent	3

For example, use the following command to verify the *proxy interface* and HiPer ARC *source address*:

```
show ip settings ENTER
```

The command displays:

IP System Host address:	2.2.2.2
IP Forwarding:	ENABLED
IP Address Pool Filtering:	ENABLED
IP Address Pool Round Robin:	ENABLED
IP Multicast Proxy Interface:	Eth:1
IP Multicast Heartbeat Status:	ENABLED
IP Multicast Heartbeat Interface:	NONE
IP Multicast Heartbeat Group:	2.2.2.2
IP Multicast Heartbeat Time:	60 seconds
IP Multicast Heartbeat Window:	8
IP Multicast Heartbeat Threshold:	2
IP source address for RADIUS:	0.0.0.0
IP source address for SYSLOG:	0.0.0.0
IP local address for unnumbered links:	0.0.0.0
IP source address for IGMP:	0.0.0.0



If the Mbone proxy you set was a WAN interface, the command will display:

IP Multicast Proxy Interface:	lynne/slot:1/mod:2
--------------------------------------	--------------------

If the IP source address was set, the command will display:

IP source address for IGMP:	5.5.5.5
------------------------------------	---------

- 8 Save your configuration. Type:

```
save all ENTER
```


Scenario A: Mbone Connection Via Ethernet Interface

The sample configuration below shows how to set up HiPer ARC to allow multicast traffic to be forwarded from the Ethernet Mbone connection to any WAN interfaces wishing to receive this traffic. Also, multicast heartbeat is enabled to monitor multicast traffic and list and show commands are issued to verify the configuration. Refer to the graphic and commands below.

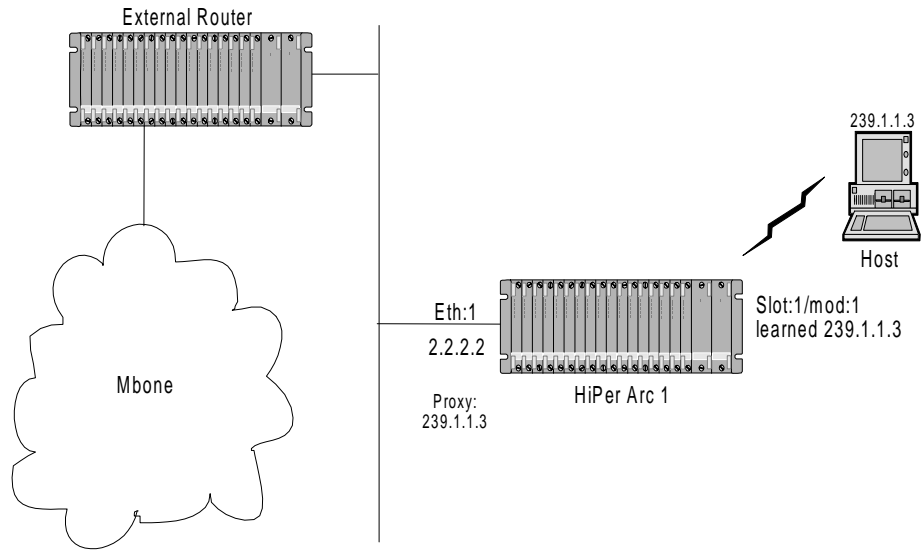


Figure 10-3 Scenario A: Mbone connection through Ethernet interface

Type the following:

```
add ip network hiperarc1 address 2.2.2.2 ENTER
set ip multicast proxy interface eth:1 ENTER
set ip igmp eth:1 multicast_forwarding enabled ENTER
add user lynne type network ENTER
set net user lynne igmp multicast_for ena multicast_routing ena multicast_proxy ena ENTER
set ip multicast heartbeat interface eth:1 group 239.1.1.3 time 60 threshold 2 window 8 ENTER
enable ip multicast_heartbeat ENTER
list ip igmp ENTER
show ip igmp eth:1 ENTER
show ip igmp slot:1/mod:1 ENTER
```

How it Works

Once user *lynne* dials in, any multicast groups learned or joined on interface *slot:1/mod:1* are proxied onto interface *eth:1*. HiPer ARC sends reports for these groups to the external router which is running a multicast routing protocol (PIM or DVMRP). Any multicast traffic destined for multicast groups joined by user *lynne* are routed through the external router to HiPer ARC. HiPer ARC receives these packets on its Ethernet interface and forwards them through *slot:1/mod:1* out to user *lynne*.

Since multicast heartbeat is enabled, the administrator can verify the connection status of multicast traffic to multicast group 239.1.1.3. If during the course of 8 intervals, less than 2 multicast hits are recorded, an SNMP trap will be issued.

Scenario B: Mbone Connection Via WAN Interface

The sample configuration below shows how to setup HiPer ARC to allow multicast traffic to be forwarded from the WAN Mbone connection to any other WAN or ethernet interfaces wishing to receive this multicast traffic. Refer to the graphic and commands below.

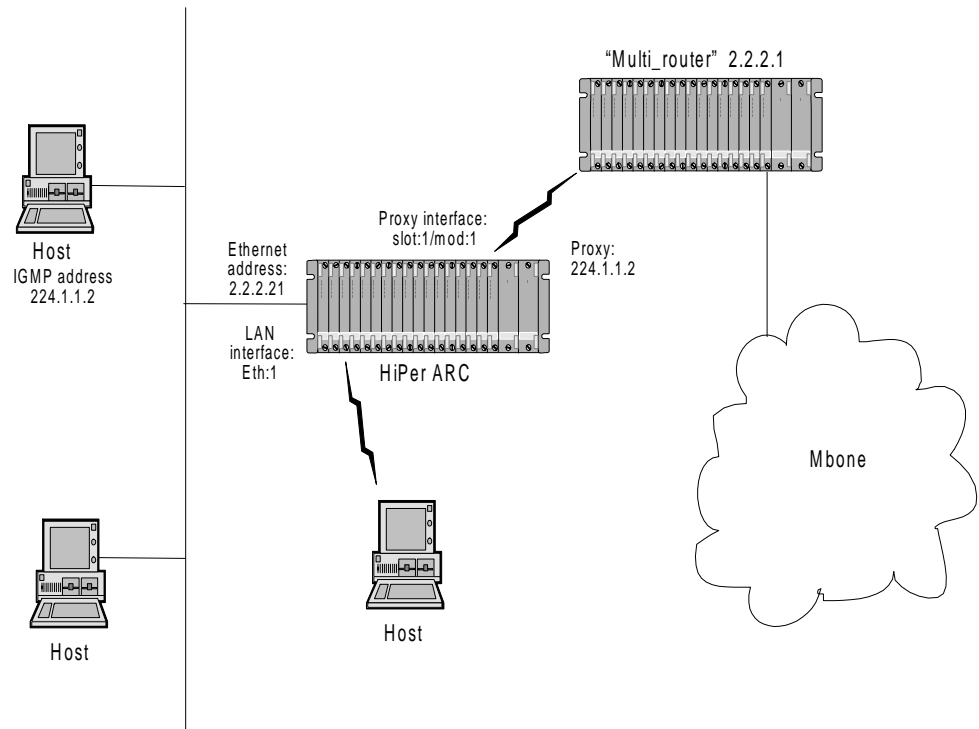


Figure 10-4 Scenario B - Mbone connection through WAN interface

Type the following:

```
add ip network hiperarc1 address 2.2.2.2 ENTER
set ip igmp eth:1 routing enabled multicast_forwarding enabled multicast_proxy ena ENTER
add user multi_router type network ENTER
set network user multi_router igmp multicast_forwarding enabled ENTER
set ip multicast proxy interface multi_router ENTER
list ip igmp ENTER
show ip igmp eth:1 ENTER
show ip igmp slot:1/mod:1 ENTER
```

How it Works

Once user *multi-router* dials in any multicast groups learned or joined on the Ethernet will be proxied onto *slot:1/mod:1*. HiPer ARC sends reports for these groups to the external router which is running a multicast routing protocol (PIM or DVMRP). Any multicast traffic joined by hosts on the Ethernet will be routed through the external router to HiPer ARC. HiPer ARC receives these packets on *slot:1/mod:1* and forwards them through the *eth:1* interface to hosts on the Ethernet.

Dial, Connect and Hangup Commands

You can dialup a remote or local user with the **dial** and **connect** commands and log in to hosts with the **rlogin** and **telnet** commands. You can use the **hangup** and **logout** commands to clear those lines.

Dial Command

The **dial** command makes an immediate connection for a manual dial-out user using the dial-out information in the user's profile. Use the following command:

```
dial <user_name>
```



To use this command, the user name must already exist in the system.

Hangup Command

To close an *interface* (hangup and leave the interface(s) in an ENABLED state), type:

```
hangup interface <interface_name>
```

To make a *modem group* unavailable for dial-in users, use the following command. It has the same effect as hanging up the phone.

```
hangup modem_group <name>
```

Reboot Command

Use the **reboot** command to recycle the system. But first, be sure to use the **save all** command to preserve any configuration changes.

See page Using the Boot Configuration Menu for more information on rebooting from the Boot Configuration Menu.

Dialin User Message

Use the **set switched interface** command to write a configurable message to all dial-in users when connections are made on that modem. This information is helpful for diagnostic purposes. Using the **show interface slot:x/mod:y** command displays the message as written. The options are:

- **\$date** - current date according to system uptime
- **\$callid** - user's call number according to system uptime
- **\$port** - port occupied by user (slot:x/mod:y)
- **\$hostname** - user's host name
- **\$sysname** - user's system name (same as hostname)
- **\$time** - time of call according to system uptime



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

For example:

```
set switched interface slot:3/mod:2 message "Welcome to the Hub, $hostname. You're Caller #
$callid connected on $port at $time on $date." ENTER
```

Upon dialup, HiPer ARC will display:

```
Welcome to the Hub, LCortese. You're Caller #2345 connected on slot:3/mod:1 at 5:39 pm on
September 5, 2001. ENTER
```



*You can also use the **set user** and **show user** commands to write and display specific dialin user messages.*

Exiting the CLI

Bye, Exit, Leave, Quit Commands

The **bye**, **exit**, **leave** and **quit** commands all serve to shut down the CLI but leave the connection open.

Logout Command

Logout exits the CLI and closes the connection, ending a dial-in user's or TELNET session.

Network Services

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



For more information about adding dial-out network service, including NCSI client setup, see Chapter 6: Network Dial-Out Access.

Adding Network Services

Use the **add network service** command shown below:

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

For example:

```
add network service DIALOUT close_active_connections true socket 99 data
auth=off,login_banner=\"Welcome to my Net\", service_type=dialout,drop_on_hangup=on
login_prompt=\"My Session\" ENTER
```



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



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

close_active_connections Indicates whether or not to *close* any active connections when a service is disabled.

data Ancillary *data*. Format one or more values with the following syntax.

auth=on/off	On indicates that login/ password authentication should be performed on incoming connections. Default: on
login_banner=string	ASCII string sent to a client when the connection is made. Enclose in quotes and backslashes only when spaces are included. Default: none
login_prompt=string	ASCII string specifying the login prompt to be sent during authentication. Enclose in quotes and backslashes only when spaces are included. <i>Auth</i> must be on. Default: login .
service_type=manage/dialout	Indicates whether the service is offering modem sharing service or manage service. Modem sharing service connects the client to a modem. Manage service connects the client to the command line, to manage the system. Applicable only to TELNET servers; you can't ClearTCP into the system to manage. Default: manage
modem_group=string	Used for modem sharing service, indicating the modem group the service will allocate a modem from. Enclose in quotes and backslashes only when spaces are included. Default: none .
drop_on_hangup=on/off	Used for modem sharing service. On causes the TCP session to be dropped when the modem hangs up. Off causes the connection to remain active. Default: off

Using the **list network services** command after typing the example above will display the following (e.g.):

CONFIGURED NETWORK SERVICES				
Name	Server Type	Socket	Close	Admin Status
calls	TELNETD	6001	FALSE	ENABLED
#### DATA: auth=off, login_banner= "Welcome to My Net", login_prompt="My Session,drop_on_hangup=on				
tftpd	TFTPD	69	FALSE	ENABLED
#### DATA:				
telnetd	TELNETD	23	FALSE	ENABLED
#### DATA:				
hdmconsole	TELNETD	23	FALSE	DISABLED
#### DATA:				
modem_group="slot:3/console"				

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

For example:

```
disable network service "telnet user" ENTER
set network service "telnet user" server_type telnetd data auth=off ENTER
enable network service "telnet user" ENTER
```

server_type Type of service being offered: *ClearTCPd*, *Dialout*, *SNMPd*, *TELNETd*, *TFTPd*.

socket Sets the port number the HiPer ARC listens on for network service requests.

Enabling and Disabling Network Service

By default, the network service is enabled when you add it. To edit the service, you must first disable it:

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

To enable network service:

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

Deleting a Network Service

To delete a network service:

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

Using TFTP

TFTP (Trivial File Transfer Protocol) can be used to transfer files to and from the system. Since this network service is enabled by default, set it up by first configuring your PC as a TFTP client of the hub by entering this command:

```
add TFTP client <hostname or IP address>
```



If you want to allow any system to TFTP into your system, set a TFTP client to 000.000.000.000.

Next, from a machine that has access to the same network, use the following TFTP commands to transfer the filter file to FLASH memory.

```
tftp <HiPer ARC IP address>
```

```
put <filename>
```

If you want to obtain a file from another network host, add that host as a TFTP client, and, from within the system, use TELNET to access that host and use the following command to obtain the file.

```
get <filename>
```



*Use **list files** to verify the file was sent to HiPer ARC.*



*Important: **Do not** transfer binary files. Transferring binary files of any type will cause unexpected results and may cause HiPer ARC to “hang”.*

Using Rlogin and TELNET

You can connect to a specific host on the network using the **rlogin** or **telnet** commands. You must first have used the **add dns host** or **add dns server** commands for HiPer ARC to recognize an IP host name.



Rlogin is not supported into HiPer ARC. You can only use rlogin to communicate out of HiPer ARC.

Rlogin and TELNET use the following syntax:

```
rlogin <IP name or address>
```

```
login_name <name>
```

```
tcp_port <number>
```

or:

```
telnet <IP name or address>
```

For example, to *TELNET* to a host with an IP address of 167.199.76.23, type:

```
telnet 167.199.76.23 ENTER
```

You can also create a TELNET client for access to HiPer ARC by using the following commands:

```
add telnet client <ip_address/subnet>
```

```
enable telnet client_access
```

For example:

```
add telnet client 132.146.34.56/43 ENTER
```

```
enable telnet client_access ENTER
```



When using TELNET or rlogin on a TCP connection via a global interface (HiPer ARC internal interface), you should run RIP. Without RIP running on the internal network, you won't learn of remote networks should the Ethernet interface be disabled. See Chapter 7 for more information.

TELNET Status

The **status** command displays the IP address of the remote host you (Console port user only) are Telnetted into and the value of the TELNET escape character. Typing status at the **telnet:** prompt will produce something like this:

```
Connected to 172.144.122.144.
Escape character is ^]
```

TELNET Control Characters

Console port users (service unavailable to login users) can use the **send** command to transmit a TELNET control character to a host.

After you've established a TELNET session (logged in and given your password), type the **TELNET escape** character: **C]** (Ctrl right bracket) followed by one of the ten other control characters, making sure that the characters are all uppercase. Your choices are:

Parameters	Description
AYT	Are you there
IP	Interrupt process
BRK	Break
AO	Abort output
EC	Erase character
EL	Erase link
GA	Go ahead
NOP	No operation
EOR	End of record
SYNC	Synchronize

For example, at the host prompt, type:

```
Ctrl ] send AYT ENTER
```

Use the **set_escape** command to change the TELNET escape character to a character of your choice. Use a *carat* (^) to precede another character. Type:

```
set_escape ^X ENTER
```

Closing a Connection

The **close** command shuts down an active TELNET connection.

Troubleshooting Commands

Viewing Facility Errors

The **set facility** command allows you to set and view log levels for the system's processes, ensuring that error messages reaching the threshold for that facility will be output to the console port.



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

Log levels range from the lowest state, *debug*, to the highest, *critical*. The default is *critical*. Type:

```
set facility <name>
loglevel [common | critical | debug | unusual | verbose]
```

For example:

```
set facility snmp loglevel unusual ENTER
```



*Use the **list facilities** command to view a log level change.*

Terminating an Active Process

The **kill** command terminates an ongoing process. You can kill a process only after it has started. For instance, if you want to kill a **ping** request that has run too long. Use the **list processes** command to view current active processes.

Resolving Addresses

The **arp** command performs IP address resolution. Type:

```
arp <ip address or host name>
```

The system will respond with an IP address (and MAC [Ethernet] address if found on a locally connected network) of the host. For example:

```
ARP: 172.122.120.118 -> 08:00:09:cc:58:bf
```

Resolving Host Names

The **host** command returns an IP address for a specified host name by sending it to a DNS server for resolution. But before you can resolve a host, you must have added a DNS local host and server entry for resolution. To do so, use the *add dns host <name> address <ip address>* and *add dns server <ip address>* commands.

For example:

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

A screen output example:

```
Network Name: hahvahd.college-hu.com
is resolved to Address: 133.114.121.015
```

Using Ping

The ping command

The **ping** command is very helpful in testing HiPer ARC connectivity with other network devices. Options let you set ping attempts (*count*), the period between ping attempts (*interval*), the time before quitting (*timeout*), a string value specifying data to be sent (*data*), the ping maximum packet dimension (*size*), the ping process off screen (*background*), the progressive ping output for each ping request (*verbose*) and the erasure of entries in the Remote Ping Table (*self_destroy_delay*).

The CLI can perform a ping with either *verbose* or *background* selected, but not both. *Verbose* causes the CLI to display information for each PING transmitted. *Background* causes the CLI to start the PING request and then ignores it. This diagnostic tool can also be initiated from an SNMP station. Type:

```
ping <IP address>
background [yes | no]
count [maximum packets]
data [string]
interval [seconds]
self_destroy_delay [minutes]
size [data size]
timeout [1-60]
verbose [yes | no]
```

For example:

```
ping 199.55.55.55 count 3 verbose yes ENTER
```

The command would display the following:

```
PING Request: 1      Time (ms):    10
PING Request: 2      Time (ms):     0
PING Request: 3      Time (ms):     0
PING Destination: 199.55.55.55 Status: ALIVE
Count:               3
Timeouts Occurred:   0
Minimum Round Trip (ms): 0
Maximum Round Trip (ms): 10
Average Round Trip (ms): 1
```

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

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

Listing Ping settings

You can use the **list ping systems** command to display ping results. For example:

PING						
Row	Destination	Status	Count	Int	Size	TTL
1	www.cnn.com	ACTIVE	25	1	64	20
2	knoll	ACTIVE	35	1	64	20
3	zapruder	COMPLETE	45	1	64	20

Showing ping statistics

The show **ping row** <number> command is an alternative to display ping statistics. For example:

PING SETTINGS for ROW: 1 DESTINATION: www.cnn.com	
Status:	COMPLETE
Resolved IP Address:	207.25.71.29
Count:	5
Interval:	1
Size:	64
Timeout:	20
Self Destroy Delay:	10

Use the **delete ping row** <number> command to erase a row in the Remote Ping Table.

Setting ping row ceiling

The **set ping maximum_rows** command sets the maximum number of rows permissible in the Remote Ping Table. Note that setting this parameter to a number smaller than the current number of rows will not cause any row deletions immediately but following any current ping. Default: **20**. Range: **1-1000**.

Configuring a ping user

You can configure a ping user to test the connectivity of a specified login host using the **add** and **set login user** commands. This user pings a login host, gets a successful/unsuccessful message and is disconnected. Use these commands:

```
add user <user name> type login
```

```
set login user <user name> login_host <name or IP_address> login_service pingJ
```

For example:

```
add user jack type login ENTER
```

```
set user jack login_host_name 3.3.3.3 login_service ping ENTER
```

Using ping to monitor system connectivity

The **add ping_service_loss_system** command creates a configurable ping that monitors connectivity across the Ethernet network to a specified server. If contact is lost to the server, HiPer ARC signals the NMC which can be configured to busy out all chassis modems so no more calls are answered and any hunt groups will answer to other systems.

Based on the ICMP ping protocol, this command checks the IP address for each time period specified. If no response is received before the timeout expires, HiPer ARC busies out all modems. Pings continue after modems busy out and when connectivity to all modems is restored, modem service is restored.

The configureable parameters are: *IP name or address* of the server to be pinged, *enable/disable* ping service to the specified server, *frequency* of ping requests, *misses_allowed* or number of ping failures to allow before busying out the modems, and *timeout* or the interval to wait before busying out the modems.

The command is written as follows:

```
add ping_service_loss_system <ip_name_or_address>
    enabled [yes | no]
    frequency [1-200 seconds]
    misses_allowed [1-1000]
    timeout [1-6000 seconds]
```

For example:

```
add ping_service_loss_system camel enabled yes frequency 30 misses_allowed 75 timeout 500 ENTER
```

Use can display all configured ping servers with the **show ping service_loss_system** command. For example:

PING SERVERS

Name	Freq	Time	Miss	Status
camel	30	10	1	ENABLED
2humps	40	20	1	ENABLED

The **set ping service_loss_system** command allows editing of the add command while the **enable service_loss_busyout** <ping> command turns the service on and the **disable service_loss_busyout** <ping> command turns it off. You can also use the **delete ping service_loss_system** command to remove the service altogether.

Using RADIUS to monitor system connectivity

The **set service_loss_busyout radius frequency** command configures the interval at which network connectivity will be checked by a RADIUS server. If service is lost to the RADIUS server after a specified period (*frequency*), HiPer ARC signals the NMC which can be configured to busy out the hub's modems. HiPer ARC will continuously poll the RADIUS server until connectivity is restored and, at that point, restore the hub's modem's to their normal state. The default value is 60 seconds and the range is 1-200 seconds. Use the command below:

```
set service_loss_busyout radius frequency <interval>
```

After setting the service, use the following command to enable it:

```
enable service_loss_busy_out radius ENTER
```

Viewing HiPer ARC System Information

You can use the **show system** command to see the firmware revision number, the date and the time that this revision was compiled as well as other system information that may be useful when consulting 3Com Technical Support. The system replies with the following display, for example:

```
SYSTEM DESCRIPTION
System Descriptor:
3Com Corporation HiPer Access Router Card Built on Feb 19 1998 at 06:59:26.
Object ID:                1.3.6.1.4.1.429.2.19
System UpTime:             2d 02:47:54
System Contact:            Larry Cortese
System Name:               HiPerLC
System Location:           Westboro
System Services:           Internet EndToEnd Applications
System Transmit Authentication Name: HiPer
System Version:            V4.1.0
```

Viewing Interface Status, Settings

Several commands are useful to display the active/inactive status and settings of specific interfaces (ports). They are: **list switched interfaces**, **list interfaces** and **show interface settings**, and **show switched interface** <slot:x/mod:[1-y]>.

Monitor PPP activity

The **monitor ppp** command lets you view the following realtime PPP activity:

- PPP call events
- Events on specific interfaces
- Events on the next session
- Events for specific users

Decode or hexadecimal output can be displayed. For a full description of this tool, see *Chapter 11: Command Reference*.

Tap all packets

Tap commands access data streams in order to diagnose connection problems or to log data to an off-line location. All data is captured bidirectionally in the stream (including protocol negotiation) on an *interface*, *user* or *next call* basis. Data can then be dumped to a SYSLOG host, the Console port, or a virtual console port (e.g. TELNET connection) in hexadecimal, ASCII or clear text..

Syslog option

When using the *syslog* option, for each tap, data can be prioritized and directed to one of eight priority locations, detailed below. Specifying *facility*, *priority* and an *IP address* for each tap is useful if the remote SYSLOG daemons are set up to direct different facility and priority levels to different destination files or terminals.

Screen option

When using the *screen* option, data from the tap is directed to the screen where the CLI command was issued. The CLI prompt will appear only when the tap is ended. A simple interface appears on screen with one option available: **Esc** followed by the **Enter** key to end the tap. Pressing these keys in sequence stops a tap.

Taps can degrade system performance considerably and are not saved to FLASH memory to guard against accidentally set, long-running taps. The configuration you choose to tap is flushed upon system reboot so tap commands must be re-issued on system startup. But, a permanent user tap can be set using vendor-specific RADIUS attributes.

Taps on RADIUS/TACACS+ users

Setting appropriate flags in a user's RADIUS or TACACS+ profile will turn on logging to a network file so that every time a user logs on, the log file is appended to it. This function facilitates auditing and tracking a blacklisted user, for which long-term monitoring may be desirable. Employing the *Port-Tap* attribute can monitor local users while vendor-specific RADIUS attributes can monitor remotely authenticated users.

How Tap works

A tap added for a user will begin tapping all currently active sessions as well as future sessions of that user until a delete command is issued for the added tap.

Taps are identified by an ID number. Adding a tap for the user adds a generic entry for the user and clones of the tap entry are added for each active session of the user. Deleting the generic entry (identified by its ID number) will delete all tap sessions as well. But, deleting a specific session will only delete that session.

Permanent taps for a user are installed automatically when a user logs in and if the user's profile has tapping enabled.

*The **monitor ppp** command performs some similar functions as the tap command but is limited to PPP data streams only. Use tap commands to capture network traffic to a remote SYSLOG host or your console.*

Also see the **list tap** command to view currently enabled taps.



Displaying System Information

List Commands

You can use **list** commands to view current configurations for all values stored in tables as well as facilities, files (FLASH memory configuration) and other data.

These commands are fully detailed in *Chapter 11: Command Reference*.

List Critical Events

The **list critical events** command displays the last *ten* critical status events, and the system time when each occurred. You can change which events are displayed on the console and syslogged over TELNET sessions, using the **set facility** command, which is useful for troubleshooting and debugging.

Show Commands

You can use **show** commands to view the current configuration and its routing activity. A few of the show commands used for troubleshooting are covered in this section, including **show memory**, **show connection settings**, **show connection counters** and **show accounting settings**. For a full explanation, see the CLI Command Reference section of this guide.

Show Memory

The **show memory** command displays the system's DRAM memory utilization.

For example:

SYSTEM MEMORY RESOURCES	
Total System Memory Resources:	22387 KB
Free Memory:	19698 KB
Code Size:	1965 KB
Initialized Data Size:	305 KB
Uninitialized Data Size:	4013 KB
Stack Size:	512 KB

Show Dial-in Connection Settings, Counters

The **show connection** command summarizes *settings* and the *number* of incoming calls for *dial-in* connections. You can reset default settings with the *set connection* command.

show connection [settings] [counters]

For example:

CONNECTION SETTINGS	
Host Selection Method:	ROUND-ROBIN
Global User Name:	default
Service Prompt:	Login/Network User
Message Prompt:	manage:

- *Host Selection Method* Means of choosing a host. Choices are *round-robin* or *random*.
- *Global User Name* *default* is the default
- *Command Prompt* Displayed when user dials in
- *Service Prompt* Prompt after dial-in user logs in (*LOGIN* or *NETWORK* service types available)
- *Message Prompt* Prompt following service prompt for login/network service administrative user. Choices: *CONNECT*, *EXIT*, *HELP*, *LOGOUT*, *MANAGE*, *RLOGIN*, *TELNET*

List Dialin Connections

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

- **IfName** - Modem slot and interface of current connections
- **User Name** - name of users currently connected
- **Type** - current type of connections established on modems. They include:
 - **On-demand** - user connection established for on-demand purposes
 - **Dial-back** - user connection established for callback purposes
 - **Continuous** - user connection established for continuous utilization

- **Manual** - user connection established on the fly
- **Timed** - user connection established for a particular interval
- **ShrMod (Shared-modem)** - dialout user connection to a modem utilizing a login service (TELNET or rlogin). LED does not light until call is unhooked (amber) and connected (green).
- **Dialin** - user connection established for dial-in purposes. LED lights *amber* when modem is unhooked, *green* when call is connected.
- **Bond** - user connection utilizing bandwidth allocation
- **Dedicated** - user connection established for a particular user
- **DLL** - data link layer that the specified dial-in session is connected to: **NONE, PPP, SLIP, RLG, TLNT, PING, ADMN, CLTCP**
- **Start Date** - start date of a connection established on the specified interface
- **Start Time** - start time of a connection established on the specified interface

An example is shown below.

CONNECTIONS

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

This chapter details all commands and related parameters used in the Command Line Interface (CLI). The following section describes some basic concepts of the CLI including the syntax and structure of the command language.

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 ip network <network_name>
        address [IP address]
        {enabled [no | yes] }
        {frame [ethernet_II, snap] }
        {interface [eth:1 or eth:2] }
```

add ip network is the command - *<network_name>* the required value
address is a required parameter - *[IP address]* the value for the IP address
{enabled} is the network "on" value - choices: *[no or yes]*
{frame} is the encapsulation type - choices: *[ethernet_II or snap]*
interface is the LAN connection - choices: *eth:1 or eth:2*

Parameters

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

Entering Commands

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

Using Control Characters

- While working in the CLI, system messages may scroll across your screen. You can recall the last thing you typed, using (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) to abort any currently executing and stacked commands.
- Commands can be retrieved by typing [Ctrl p] (for previous) and [Ctrl n] (for next). Command retrieval consults the history of previous fully entered commands, defaulting at the last ten commands. If an error occurs while a command is processing, any partial command (up to and including the field in error) is added to the history list.
- Command line editing allows these options: (Ctrl b) or left arrow brings you go back one character; (Ctrl c) deletes the running CLI process; (Ctrl f) or right arrow takes you forward one character; (ESC b) takes you back one word; (ESC f) takes you forward one word; (Ctrl a) takes you to the beginning of a command; (Ctrl e) takes you to the end of a command, and (Ctrl d) or (Ctrl k) deletes a selected character.

Abbreviation and Command Completion

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



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

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

Help

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

Additional Conventions

- The type of value you enter must match the type requested. Numbers are either decimal or hexadecimal. Text can be either a string that you create, or it may be a list of options you must choose from. When choosing an option, type the text of the option exactly.
- “Double quotation marks” set off user-defined *strings*. If you want white space or special characters in a string, it must be enclosed by “double quotation marks.”
- If a keyword is not *unique*, it will “ding”. Then, if you wish to list possible keywords, you may use positional help.
- Most commands are *not* case sensitive. As a rule, only *<name>* and *[password]* values require typing the correct case.
- Configuration changes are impermanent: they occur immediately but are lost on reboot unless you save them because the **save all** command places configuration changes in FLASH memory. These changes are lost by HiPer ARC if power fails before saving them.
- Some commands such as **add ip network** and **reconfigure** do *not* take effect immediately.
- Some *delete* commands require that you first *disable* the process or function. For example, commands to delete a network user, interface, and network service must first be disabled.
- In most cases, 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. IP and IPX network addresses shown in this document use the syntax described in the following table. IP netmasks can be configured three ways: using the CLI mask signifier (A,B,C or H), using the standard format (*nnn.nnn.nnn.nnn*) or counting the one bits in a range from 8-30 (32 for a host). For help setting bitmasks, see *Appendix B: Addressing Schemes* for a bitmask table.

Address Type	Format	Range
IP_ address	a.b.c.d	<ul style="list-style-type: none"> ■ 0.0.0.0 to 255.255.255.255 (decimal). ■ address 127.x.x.x is reserved for Loopback. ■ address 247.x.x.x or higher is not part of a valid IP Network Class (A, B, C) ■ address 0.0.0.0 is invalid in most contexts.
ip_net_ address	a.b.c.d/mask	255.255.255.255/A,B,C,H or <i>nnn.nnn.nnn.nnn</i> or 8-30 bits
ipx_net_ address	xxxxxxxx	hexadecimal
mac_ address	xx:xx:xx:xx:xx:xx	hexadecimal digit pairs
ipx_host address	xxxxxxxx.xx:xx:xx:xx:xx:xx	IPX network address.MAC (Ethernet) address

Interface Ranges

Interfaces can be expressed as variants of the **slot:x/mod:y** format where *x* is the slot number of the Total Control Hub and *y* is a modem number (port) from 1 - *y* depending on the type of modem card installed on the Hub. You can specify more than one interface or a range a couple ways. For example:

```
assign interface slot:4/mod:[1-3] ENTER
```

```
assign interface slot:4/mod:[1-3],slot:6/mod:15,slot:8/mod:[9-11] ENTER
```



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

Names

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

Desired name:	Entered as:
Larry's PC	" "Larry's PC" "
Server_number_3	Server_number_3

Users

A user entity is a table of parameters that are used when establishing a network connection. The **add user** and **set user** commands define the parameters of a user. The user commands are employed when making WAN network (dial-in) connections and for dial-out users. Local users (stored in the User Table) are limited to 450 entries.

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 ENTER
```

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:

- **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.

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

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

The order of items in a table is usually not relevant, nor is it inherent in the type of entity. Sometimes the order is relevant, though, 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.

CLI Commands

Add Commands

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

```

add aaa_server <domain_name>
    address [IP_address]
    enabled [yes | no]
    encryption [off | on]
    passthru [enabled | disabled]
    port [1-65,535]
    preference [1-10]
    secret [string]
    server_name [name]

```

Specifies a remote TACACS+ server to use by adding an AAA domain to the AAA Domain Table to support authentication, authorization and accounting (AAA). The AAA Domain Table lists all domains a user can log into. A preference number is assigned to AAA names in the DNS Table where IP address resolution is performed according to highest preference first.

Parameters	Description
<domain_name>	Domain designation of the AAA server. Example: joe@3.com.com . Limit: 64 ASCII characters
address	IP address of the AAA server. Default: 0.0.0.0
enabled	Switch to turn AAA server on or off. Default: Yes
encryption	Enables/disables encryption of entire data packet. Default: Off
passthru	When enabled, will discontinue authentication attempts after third AAA server refusal but still allow users access to a domain. This value is used in conjunction with <i>direct request</i> . Default: Disabled
port	Port number on the AAA server. TACACS+ standard port number: 49 . Range: 1-65,535
preference	Priority ranking of domains that specifies how servers are chosen. Highest preference - 1 , lowest: 10 . Range: 1-10
secret	Password shared by AAA server and HiPer ARC for encryption. Range: 0-15 ASCII characters. Field can be left blank or filled with null character: "" .
server_name	Familial name for the AAA server to be identified by DNS. Limit: 64 ASCII characters.

```

add address_pool user <user_name>
    pool_name <name>

```

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

Note: When creating an address pool user, be sure to verify that a valid address pool exists.

```

add atm1483 pvc <name>
    address <network_IP_address>
    interface <atmaal:1>
    network <network_name>
    peak <number>
    vci <number>
    vpi <number>

```

Creates a Permanent Virtual Circuit (PVC) for RFC-1483 compliant networks. To configure multiple subnets, you must issue the command repeatedly, specifying different network names and addresses.

An example for combining IP and IPX:

```
add atm1483 pvc testing vci 200 vpi 0 peak 100000 network atm interface atmaal:1
```

```
add atm1483 pvc ip_over_atm address 204.220.145.43 vci 220 vpi 1 peak 100000 network ip_over_atm interface atmaal:1
```

For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Parameters	Description
<name>	Designation for the PVC to allow easy recognition and configuration on HiPer ARC. Limit: 64 ASCII characters.
address	Network IP address for the far side of the PVC (router)
interface	This release supports only the <i>Span A</i> logical interface for independent configuration. Default: atmaal:1
network	Designation of the network for which the PVC is specified.
peak	The peak bandwidth for this PVC in kilobits/second. Default: 0 (bandwidth = 1/10 of interface speed). Range: 0-65535
vci	Number of the Virtual Channel Indicator. Range: 32-65535
vpi	Number of the Virtual Path Indicator. Default: 0 . Range: 0-255

```
add atm1577 pvc <name>
    interface <atmaal:1>
    network <network_name>
    peak <number>
    vci <number>
    vpi <number>
```

Creates a Permanent Virtual Circuit (PVC) for classical IP and ARP support on RFC-1577 compliant networks. To configure multiple subnets, you must issue the command repeatedly, specifying different network names and addresses. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Parameters	Description
<name>	Designation for the PVC to allow easy recognition and configuration on HiPer ARC. Limit: 64 ASCII characters.
interface	This release supports only the <i>Span A</i> logical interface for independent configuration. Default: atmaal:1
network	Designation of the network for which the PVC is specified.
peak	The peak bandwidth for this PVC in kilobits/second. Default: 0 (bandwidth = 1/10 of interface speed). Range: 0-65535
vci	Number of the Virtual Channel Indicator. Range: 32-65535
vpi	Number of the Virtual Path Indicator. Default: 0 . Range: 0-255

```
add atm_arp_server <name>
    atm_address [address]
    network [network_name]
```

Creates a remote ATM ARP (Address Resolution Protocol) server for RFC-1577 compliant networks. The ATM ARP server (not a HiPer ARC), which is queried to resolve IP mapping requests on the specified network, maps the IP addresses of connected servers to 20-byte ATM addresses. For example:

```
add atm_arp_server arp_server atm_address 11.22.33.44.55.66.77.88.99.00.11.22.33.44.55.66.77.88.99.00 network ip_atm1577
```

For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Parameters	Description
<name>	Designation of the ARP server to allow easy recognition and configuration on HiPer ARC. Limit: 64 ASCII characters.
atm_address	20-byte hexadecimal address of the NSAP (Network Service Access Point) ATM ARP server.
network	Designation of the network for which the ARP server is specified.

add chat_script <name>

Adds the specified file to HiPer ARC's Chat Script table. Chat scripts are helpful for general-purpose scripting by dialin users.

A chat script file must first be created using either the **edit** command or an off-line editor. Creating the file internally will store it in HiPer ARC's FLASH memory. If the file is created off-line, you must then create a TFTP client on HiPer ARC using the **add tftp client** command and TFTP the file to FLASH.

*Note: The **add chat_script** command must be issued before a chat script can run for a RADIUS user whose Vendor Specific Attribute refers to this file. Also, multiple users can reference the same chat file.*

For more information, see the **delete**, **verify**, **show** and **list chat_scripts** commands. Also, see *Appendix E: RADIUS and TACACS+ Systems* for information about chat script syntax, constructs, and its use with RADIUS.

add cross_connect <name>

peak <number>
vci1 <num_range, (32-65535)>
vci2 <num_range, (32-65535)>
vpi1 <number (0-255)>
vpi2 <num_range, (0-255)>

Creates ATM cross-connections for Virtual Path Indicators (VPI) and Virtual Channel Indicators (VCI) on a Hub or series of Hubs with multiple cascading ATM NICs installed. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Parameters	Description
<name>	Designation of the cross connection to allow easy recognition and configuration on HiPer ARC.
peak	The peak bandwidth for this PVC in kilobits/second. Default: 0 (bandwidth = 1/10 of interface speed)
vci1	Specified VCI for the PVC on Line A to be connected.
vci2	Specified VCI for the PVC on Line B to be connected.
vp1	Specified VPI for the PVC on Line A to be connected.
vpi2	Specified VPI for the PVC on Line B that the vci1 value will be connected to.

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.

Parameters	Description
<host_name>	Designation of the local host. Limit: 64 ASCII characters.
address	IP address of a named host in <i>nnn.nnn.nnn.nnn</i> 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, with 1 as the highest preference and 10 as the lowest. The first specified server is sent the IP Host Name to be resolved, first *with*, then *without* the default domain name (see *set dns domain_name* for more information about the default domain name). If that server cannot resolve the name, it is sent to the next specified server.

Note: HiPer ARC will try to reach each configured host three times in round-robin fashion before issuing an error message. For instance, in the case of three off-line servers - A, B and C - HiPer ARC will admit failure only after trying to reach them one after the other, three times.

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

add filter <filter_name>

Adds a filter file name to the Filter Table. The Filter Table is a managed list of filter names used by SNMP. A filter file is a text file stored in the FLASH file system that you load from an external source using TFTP (see *Chapter 8: Packet Filters* for more information) or create internally with the **edit** command (see *Chapter 9: Administrative Tools* for more information). **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. You can view the filters using the **show filter** command and verify whether the filter is correct by using the **show file** command.

Note: Filter files are stored as ASCII files in FLASH memory.

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

add framed_route user <name>

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

Adds a framed (static) network to the user profile for 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. For comparison, see **add ip route** command.

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

add init_script <script_name>

command <command_string>

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

Note: Do **not** use the default initialization script supplied with earlier firmware versions (NETServer releases 3.x). The `at&f1s0=1` script is invalid and may cause the HiPer ARC's modem interfaces to lock up.

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

add ip defaultroute gateway <IP_address or name>
metric [hop count] }

Allows a default route to be configured. The command adds a default route with a gateway on the IP network configured on the first HiPer ARC LAN interface (eth:1). This allows a default route to be configured.

A default route gateway specified with a lower metric acts as the *primary* default route gateway and a second default route gateway with a higher metric acts as the *secondary* default route gateway.

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

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. Range: 1-15 . Default: 1

add ip network <network_name>
address [IP_network_address]
frame [ethernet_ii | snap | atm1483 | atm1577]
interface [eth:1 | eth:2 | internal]
enabled [yes | no]

Adds an IP network to the list of IP networks available over the specified interface. When the system starts ups, the NMC can be configured to automatically create an IP network for default route and minimal SNMP settings (if you delete an IP network and it reappears following reboot, this is the reason why that occurs).

Note: Internal networks do not support SNAP encapsulation. Also, do not set the same internal IP address for more than one HiPer ARC on the same LAN. (see **set ip unnumbered_link local_address** for more.

Parameters	Description
<network_name>	Name of IP network, consisting of up to 64 unique ASCII characters; white space must be surrounded by double quotes.
address	IP address of the network, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The Mask Specifier can be 'A', 'B', 'C', or 'H', or a numeric value from 8 to 30 (32 for host) that describes the number of one bits in the mask. You can also specify the netmask in the xxx.xxx.xxx.xxx format. If you do not specify a mask, the system will generate it for you from the network address.
frame	Frame encapsulation to be used on this IP network. Choices: Ethernet_ii (Default) , snap , atm1483 , atm1577
interface	Name of the interface which this IP network will communicate over. Eth:1 and Eth:2 are the two LAN ports available while internal is a setting to define a global or "interfaceless" IP address for HiPer ARC when supporting an ondemand or manual user with RIP over an <i>unnumbered</i> LAN-to-LAN connection. The default is the first LAN interface (eth:1). See <i>Chapter 7</i> for more information.
enabled	Optional parameter indicates whether network is enabled (YES) or disabled (NO). Default: YES

```

add ip pool <pool_name>
    initial_pool_address <IP_network_address/subnet>
    route [aggregate | no_aggregate]
    size <1-4096>
    state [public | private]

```

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

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

HiPer ARC automatically derives subnet masks for *aggregate* users but a mask can be configured for *no_aggregate* users.

Note: Users assigned to more than one pool will receive an address from the last assigned pool in round robin fashion. Also, if the administrator reduces the size of the pool, users whose associated address pool was deleted won't be denied access until after their calls have terminated.

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

```

add ip route <host_name or IP_network_address>
    gateway [IP_name or gateway_address]
    { metric [hop_count]}

```

Adds an IP 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 all currently defined routes including the static route you create with this command but only if you have specified a *gateway*. Also see the **add ip defaultroute** command.

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

Parameters	Description
<network_address>	IP address or host name of the remote destination, in the format nnn.nnn.nnn.nnn, entered <i>with</i> or <i>without</i> a mask specifier. The mask specifier can be 'A', 'B', 'C', or 'H' (host), or a numeric value from 8 to 30 (32 if a host) that describes the number of one bits in the mask. You can also specify the netmask in the xxx.xxx.xxx.xxx format. If you do not specify a mask, the system will self-generate it (based on the network address) for all routes (<i>ip network address</i>) except <i>host</i> routes, for which you <i>must</i> specify a mask. For help counting bits, see <i>Appendix C: Address Schemes</i> for a bitmask table.
gateway	IP name or address of gateway used to reach this remote network.
metric	An integer for how distant the route is, in "hops", from the destination to HiPer ARC. Range: 1-15 . Default: 1

```
add ipx network <network_name>
    address [ipx_network_address]
    interface [eth:1 | eth:2]
    enabled [yes | no]
    frame [ethernet_ii | snap | dsap | novell_8023]
```

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

Parameters	Description
<network_name>	Name of IPX network. Unique ASCII string of up to 64 characters.
address	Address of the IPX network.
interface	Name of interface with which this IPX network 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. Choices: <ul style="list-style-type: none"> ▪ Ethernet_II - contain Type in place of length fields. Default ▪ SNAP (Ethernet_SNAP) - Sub-Network Access Protocol derived from 802.2 ▪ DSAP (802.2) - default frame type for NetWare v4.x ▪ Novell_8023 (802.3 raw) - default frame type for NetWare v2.x and v3.x networks

```
add ipx route <ipx_network_address>
    gateway [ipx_host_address]
    metric [1-15]
    ticks [tick_number]
```

Adds an IPX static route to the system'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 (network_address.mac_address).
metric	Number of hops through different routers to reach the remote IPX network. Range: 1-15
ticks	Estimated interval in ticks it takes to deliver a packet to the remote network. There are approximately 18 ticks per second.

add ipx service <service_name>
 address [internal network address]
 gateway [network_number.mac_address]
 metric [1-15]
 node [internal_node_number]
 socket [socket_number]
 type [service_type]

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

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

add l2tp lns <1-9> **address** <IP_address>

Adds a local L2TP network server (LNS) and its associated IP address on the LAC side of the L2TP tunnel. Additional security and a shared secret may also be specified using the **set l2tp lns** command.

The LNS is added to a list of default LNS systems that the LAC may seek to contact due to failure to receive an LNS tunnel endpoint (IP address) from the RADIUS server. A failure could be caused by an unconfigured RADIUS server, or a complete absence of the value in the user's RADIUS profile.

add login_host <host_name>

address [IP_address]
preference [number]
rlogin_port [TCP_port_number]
telnet_port [TCP_port_number]
clearTCP_port [TCP_port_number]

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

Parameters	Description
<host_name>	Name or IP address that specifies an IP host. Limit: 64 ASCII characters.
address	<i>Optional.</i> address of login host. 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. The first preference is 1 , the least preference, 10 . Range: 1-10 .
rlogin_port	<i>Optional.</i> Specifies the port number that will be used when a user executes the rlogin CLI command, specifying this host. Maximum: 65535 . Default: 513
telnet_port	<i>Optional.</i> Specifies the port number that will be used when a user executes the TELNET CLI command, specifying this host. Maximum: 65535 . Default: 23
clearTCP_port	<i>Optional.</i> Specifies the port number that will be used when a user's application requests a ClearTCP session with this host. Maximum: 65535 . Default: 6000

add modem_group <group_name>

interfaces [slot:x/mod:[1-y],slot:x/mod:[1-y]...]

Creates a group of interfaces. See also the **set modem_group** command, which configures all interfaces in the modem group. You can also add additional interfaces to this modem group using **assign interface**, and remove them with **unassign interfaces**. Modem groups *all* and *slot:1/mod:[1-y]*, *slot:2/mod:[1-y]*, etc... are provided as **default** modem groups with associated Hub modems as indicated. Use **list modem_groups** command to view entries.

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

Note: Default modem groups cannot be modified.

Parameters	Description
<group_name >	Name of the modem group. 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. Limit: 64 ASCII characters. Limit: 500 modem groups
interfaces	List of interfaces to be assigned to the modem group. The expected format is ssss,sss,sss... 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 slot:x/mod:[1-y],slot:x/mod:[1-y].

add mpip client <IP_address>
 sharedsecret <string>
 type <hiper | netserver>

Creates an entry for HiPer ARC configured as an MPIP client, in the MPIP server's Client Table with a password shared by the configured client and server, and the type of client specified.

Parameters	Description
<IP address>	Unique identifier of the MPIP client.
sharedsecret	Password shared by the MPIP client and server. Limit: 16 ASCII character
type	The product type of the MPIP client: HiPer ARC or NETServer . The distinction between these types is relevant only to a HiPer ARC configured as an MPIP server - NETServer-based MPIP clients must specify NETServer type. Default: HiPer ARC

add mpip server <IP_address>
 port <number>
 priority <1-32>
 sharedsecret <string>

Creates an entry for HiPer ARC configured as an MPIP server, in the MPIP client's Server Table with a password shared by the configured client and server.

Parameters	Description
<IP address>	Unique identifier of the MPIP server.
port	The UDP port all HiPer ARC MPIP servers use. Range: 0-65,535 . Default: 5912
priority	Rank specifying preference of MPIP server used. If two servers share the same priority, the server with the smaller IP address takes precedence. Default: 1 . Range: 1-32
sharedsecret	Password shared by MPIP server and client. Limit: 16 ASCII character

add network service <service_name>
 close_active_connections [true | false]
 data [ancillary data options]
 enabled [yes | no]
 server_type [server_type]
 socket [socket_number]

This configures a network listener process that provides a certain services, including modem sharing, TFTP file access, and SNMP, TELNET and ClearTCP support. For more information on configuring dialout service, see *Chapter 6: LAN to LAN Routing*. To view the available server types, use the **list available servers** command..

Parameters	Description
<service_name>	Name of this type of service. Limit: 64 ASCII characters.
close_active_connections	Indicates whether or not to close any active connections when a service is disabled by the disable network_service command. Default: False .
data	Ancillary Data. This field contains server-specific configuration data. See table below for configurable ancillary data parameters for TELNET. The <i>modem_group</i> value also applies to NCSI DialOut service.
enabled	<i>Optional</i> . Indicates whether the network is enabled (YES) or disabled (NO). When you add a network service, it is <i>enabled</i> by default.



Parameters	Description
server_type	Designates the type of service being offered. Services currently available are: <ul style="list-style-type: none"> ▪ ClearTCPD - daemon enables access to a modem group. Uses TCP. ▪ DialOut - supports dial-out connections to IP or IPX hosts. Uses TCP. Note: You can't create more than one DialOut service on a network with the <i>same name</i> without confusing the NCSI client. ▪ SNMPD - daemon supports SNMP. Uses UDP. ▪ TFTPD - daemon supports file transfer service. Uses UDP. ▪ TELNETD - daemon supports TELNET, either to the CLI or a modem group. Uses TCP.
socket	Port the server listens on. For TFTP, TELNET and CLEARTCP, it is the TCP or UDP port number. Socket numbers are the joined sender's (or receiver's) IP address and service type's port number. Maximum: 65535 . Range: 0-65535

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

Ancillary Data Parameters	Description
auth	On indicates that login/password authentication should be performed on incoming connections. Feature not supported for DialOut service. Format: auth= [on off] Default: on
drop_on_hangup	Value specifying whether the TCP session is dropped after modem hangs up. <i>Off</i> allows connection to remain active. Feature not supported for DialOut service. Default: off
login_banner	ASCII string sent to a client when connection is made. It must be quoted and offset by backslashes if spaces are included in the string. Specify carriage return after login banner with: login_banner=string\r\n\ . Feature not supported for DialOut service. Format: login_banner=string Default: none
login_prompt	ASCII string specifying the login prompt sent during authentication. It must be quoted and offset by backslashes if spaces are included in the string. Feature not supported for DialOut service. Specify carriage return after login banner with: login_banner=string\r\n\ Format: login_prompt=string Default: login:
modem_group	ASCII string specifying the name of a modem group for whose modems network service is supplied. This value must be specified when using DialOut service.
service_type	Indicates whether the service offered is modem sharing or manage. <ul style="list-style-type: none"> ▪ <i>Modem sharing</i> service connects a client to <i>multiple</i> modems. ▪ <i>Manage</i> service connects a client to the <i>command line</i>, to manage the system. Applicable only to TELNET servers; you can't use ClearTCP to access the system for management. Format: service_type=manage, dialout Default: manage

Add network service examples:

To configure a ClearTCP service to offer modem sharing on TCP port 6000, not doing authentication upon connect, using the modem slot:3/mod:1, type:

```
add network service modem_sharing server_type cleartcpd socket 6000
data auth=off,interface=slot:3/mod:1,service_type=dialout ENTER
```

*Note: Enclose DATA values including **spaces** with double quotes. E.g.: data modem_group="Hi Boston".*

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

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

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

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

```
add network service "Calling LA" server_type dialout data modem_group=LA
```

add ping service_loss_system <IP_name or IP_address>

```
enabled [yes | no]
frequency [1-200 seconds]
misses_allowed [1-1000]
timeout [1-6000 seconds]
```

Creates a configurable ping that monitors IP connectivity across the network to a specified server. If service is lost to the server, HiPer ARC notifies the NMC (which can be configured) to use auto-response to busy out all chassis modems so no more calls are answered and any hunt groups will answer to other systems. Based on the ICMP ping protocol, this command checks the IP address for each time period specified. If no response is received before the timeout expires, HiPer ARC busies out all modems. Pings continue after modems busy out and when connectivity to all modems is restored, modem service is restored.

Parameter	Description
<ip name or address>	IP name or address of the system to be pinged.
enabled	Ping service enabled/disabled to particular server.
frequency	Interval in seconds between ping requests. Default: 30 . Range: 1-200 .
misses_allowed	Number of ping failures allowed before busying out modems. Default: 1 . Range: 1-10 .
timeout	Interval in seconds to wait before busying out modems. Default: 10 . Range: 1-60 .

add pptp pns <1-9>

```
address <IP_address>
```

Adds a local PPTP network server (PNS) on the client side of the PPTP tunnel. The PNS is added to a list of default PNS systems that the client may seek to contact due to failure to receive an PNS tunnel endpoint (IP address) from the RADIUS server. A failure could be caused by an unconfigured RADIUS server, or a complete absence of the value in the user's RADIUS profile.

add snmp community <community_name>

```
address [IP_address]
access [ro | rw | adm]
community_pool [name]
validate_address [use_address | use_pool]
```

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

Parameter	Description
<community_name>	Group name that authorizes SNMP requests.
address	IP address of the remote SNMP manager, in the form <i>nnn.nnn.nnn.nnn</i>



Parameter	Description
access	Determines what type of access to SNMP MIBs the specified user has. Options: Read Only (RO) - user-level objects Read Write (RW) - user-level objects Administrator (ADM) - Administrator allows <i>read access to all objects</i> and <i>write access to all writeable objects</i> . RO is the default on public (0.0.0.0) networks and RW the default on private networks.
community_pool	Name of the SNMP community pool to use.
validate_address	When set to <i>use_address</i> the <i>address</i> of the SNMP community is used to validate the management station's IP address. When set to <i>use_pool</i> , the management station's IP address is validated against the list of IP address associated with the <i>community_pool</i> . Default: use_address

add snmp community_pool <pool_name>
address <IP_name or address>

Adds an entry to the SNMP Community address Pool table. This command is used in conjunction with the **add snmp community** command to allow multiple management station control of HiPer ARC through a pool of IP addresses.

Parameter	Description
<pool_name>	Pool name defining a group of SNMP management stations. Limit: 10
address	IP name or address of an SNMP management station in the pool. Limit: 10

add snmp trap_community <name>
address <IP_address>
trap_community_pool <name>
trap_validate_address <use_address | use_pool>

Adds to the list of community name/IP address pairs that are allowed to receive SNMP traps as well as allows multiple management stations to use the same SNMP trap community name. Entries are added to the SNMP Trap Community Address Pool table. You can display authorized users with the **list snmp trap_communities** command.

Parameter	Description
<name>	Group name defining who can receive SNMP traps.
address	IP address of the SNMP manager, in the form <i>nnn.nnn.nnn.nnn</i> .
trap_community_pool	Name of the trap community pool.
trap__validate_address	When set to <i>use_address</i> (default), the <i>address</i> of the SNMP trap community is used to validate the management station's IP address. When set to <i>use_pool</i> , the management station's IP address is validated against the list of IP addresses associated with the <i>trap_community_pool</i> . Employing <i>use_pool</i> selects IP addresses from the pool as destination addresses and does not use the specified <i>address</i> parameter although a token address must be entered for purposes of backward compatibility.

add snmp trap_community_pool <name>
addresses <IP address list>

Adds up to four or eight entries at a time (depending on the number of characters each IP address occupies) to the SNMP Trap Community Address Pool table. If IP addresses are in the single-digit form as *1.1.1.1*, eight entries can be added with the single CLI command; if addresses are in triple-digit form such as *146.115.112.111*, four IP addresses can be added with the single CLI command. The maximum size of the pool is 10 IP addresses. See **delete snmp trap_community_pool** and **list snmp trap_community_pools** commands for more information.

Parameter	Description
<name>	Pool name defining who can receive SNMP traps.

Parameter	Description
addresses	IP addresses of all SNMP managers associated with the pool , in the form <i>nnn.nnn.nnn.nnn</i> .

add syslog <IP_name or address>

allow_all_auth_levels [yes | no]

facility [log_auth | log_local0 | log_local1 | log_local2 | log_local3 | log_local4 | log_local5 | log_local6 | log_local7]

loglevel [critical | unusual | common | verbose]

Adds an IP host to the list of IP hosts that 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**.

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

Parameters	Description
<ip_name_or_address>	Host name or IP address of the UNIX host that will receive SYSLOG information.
allow_all_auth_levels	Permits or denies transmission of all loglevel syslog messages by the Auth facility. Default: Yes
facility	The SYSLOG node facility (site) where SYSLOG messages are sent. See choices above. Default: log_auth
loglevel	There are four levels of logging: <ul style="list-style-type: none"> ▪ CRITICAL - a serious system error, which may effect system integrity. Default ▪ UNUSUAL - an abnormal event, which the system should be able to recover from ▪ COMMON - a regularly occurring event ▪ VERBOSE - a regular periodic event, e.g. a routing update message

add tap interface <interface_name>

address <IP_address>

facility <log_auth | log_local0 | log_local1 | log_local2 | log_local3 | log_local4 | log_local5 | log_local6 | log_local7>

format <hex | ascii | clear>

loglevel <critical | unusual | common | verbose>

output <screen | syslog>

Creates a data stream tap on the specified interface to log data to an off-line location. All data is captured in the stream, including protocol negotiation, then dumped to a SYSLOG host, the Console or a virtual (TELNET or dialin) console port in *hexadecimal*, *ASCII* or *clear* text. HiPer ARC permits multiple taps on different ports simultaneously.

When using the *SYSLOG* option, for each tap, data can be directed to one of eight priority locations, detailed above. Specifying facility and priority for each tap is useful if the remote SYSLOG daemons are set up to direct different facility and priority levels to different destination files or terminals.

When using the *screen* option, data from the tap is directed to the screen where the CLI command was issued. The CLI prompt will appear only when the tap is ended. A simple interface appears on screen with one option available: pressing **ESC** and **ENTER** keys stop a tap.

The configuration you choose to tap is not saved to FLASH memory so tap commands must be re-issued on system startup, but, a permanent user tap can be set using vendor-specific RADIUS attributes.

Note: The **monitor ppp** command performs some similar functions as the **tap** command but is limited to PPP data streams only and provides PPP protocol decoding. Use tap commands to capture network traffic to a remote SYSLOG host or your console.

Issue the **delete tap** command to remove the tap from the table and **list tap** to view currently enabled taps.

Parameters	Description
<interface_name>	HiPer ARC designation for the specific interface to be tapped. Choices: modem interfaces (slot:x/mod:y).
address	Host name or IP address of the Unix host that will receive TAP information.
facility	The TAP node facility (site) where output is sent. See choices above. Default: log_auth
format	The text style tap output is displayed as. Choices: Hexadecimal, ASCII, Clear
loglevel	Priority levels of messages that can be logged: <ul style="list-style-type: none"> ▪ CRITICAL - a serious system error, which may effect system integrity. Default ▪ UNUSUAL - an abnormal event, which the system should be able to recover from ▪ COMMON - a regularly occurring event ▪ VERBOSE - a regular periodic event, e.g. a routing update message
output	Endpoint where tap information can be directed: SCREEN or SYSLOG

add tap next

```

address <IP_address>
facility <log_auth | log_local0 | log_local1 | log_local2 | log_local3 | log_local4 | log_local5 |
log_local6 | log_local7>
format <hex | ascii | clear>
loglevel <critical | unusual | common | verbose>
output <screen | syslog>

```

Creates a tap on the next dial in or network connection. Tap output begins immediately upon next session startup. Press **ESC** and **ENTER** keys to exit tapping. See the **add tap interface** command above for more information. Issue the **delete tap** command to remove the tap from the table and **list tap** to view currently enabled taps.

Parameters	Description
address	Host name or IP address of the Unix host that will receive TAP information.
facility	The TAP node facility (site) where output is sent. See choices above. Default: log_auth
format	The text style tap output is displayed as. Choices: Hexadecimal, ASCII, Clear
loglevel	Priority levels of messages that can be logged: <ul style="list-style-type: none"> ▪ 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 ▪ VERBOSE - a regular periodic event, e.g. a routing update message. Default
output	Endpoint where tap information can be directed: SCREEN or SYSLOG

add tap user <user_name>

```

address <IP_address>
facility <log_auth | log_local0 | log_local1 | log_local2 | log_local3 | log_local4 | log_local5 |

```

```

log_local6 | log_local7>
format <hex | ascii | clear>
loglevel <critical | unusual | common | verbose>
output <screen | syslog>

```

Creates a tap on all currently active sessions of a specified user. Tap output begins immediately upon entering the command. Press **ESC** and **ENTER** keys to exit tapping. See the **add tap interface** command above for more information. Issue the **delete tap** command to remove the tap from the table and **list tap** to view currently enabled taps.

Parameters	Description
<user_name>	HiPer ARC designation for the specific user to be tapped. Limit: 64 ASCII characters.
address	IP address of the UNIX host that will receive TAP information.
facility	The TAP node facility (site) where output is sent. See choices above. Default: log_auth
format	The teFxt style tap output is displayed as. Choices: Hexadecimal, ASCII, Clear
loglevel	Priority levels of messages that can be logged: <ul style="list-style-type: none"> ▫ 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 ▫ VERBOSE - a regular periodic event, e.g. a routing update message. Default
output	Endpoint where tap information can be directed: SCREEN or SYSLOG

add telnet client <IP address/mask>

Creates a TELNET client - after access is globally enabled with the **enable telnet client_access** command - capable of accessing HiPer ARC. By specifying a netmask, you can add network and subnetwork addresses. If no netmask is specified, the host netmasks value is assumed. An IP address of 0.0.0.0 allows universal entry to HiPer ARC by TELNET users. See the **delete telnet client** command for more information. Also, issue the **list telnet client** command for a list of configured users. Default: **Disabled**

add tftp client <IP_name_or_address>

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

Parameters	Description
<ip_name_or_address>	Host name or IP address of a host to be added. An address of 0.0.0.0 allows all clients TFTP access.

add tftp request <input_file_name>

```

action <get | put>
server <IP_name_or_IP_address>
mode <ascii | octet>
rexmt_timeout <1-60>
max_timeout <1-300>

```

Adds entries to the TFTP Client Request Table. Entries are the names of files either requested *from* or sent *to* the TFTP server. The command is useful for administrators at SNMP management stations seeking to access the TFTP client HiPer ARC.

Parameters	Description
<input_file_name>	Designation of file to be requested from or sent to the TFTP server. Limit: 32 ASCII characters.
action	Type of request sent to the TFTP server. Choices: put or get
server	Name or IP address of the TFTP server.
mode	The text format the file is transmitted as. Choices: ascii or octet (binary). Default: ascii



Parameters	Description
rexmt_timeout	Retransmission timeout - interval in seconds HiPer ARC waits for a reply from the TFTP server before retransmitting a TFTP request. Range: 1-60 . Default: 5 seconds
max_timeout	Interval in seconds HiPer ARC waits for a response from the TFTP server before the TFTP request is cancelled. Range: 1-300 . Default: 25 seconds

add user [name]

enabled [yes | no]
login_service [rlogin | telnet | cleartcp | ping]
network_service [ppp | slip]
password [password]
type [login,network,callback,dialout, 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. See the **show users** command for more information on individual users.

Note: Administrators creating RADIUS users should consult *Appendix E: Radius Authentication* for more information..

Parameters	Description
[name]	Name of user to be added, up to 64 ASCII characters. Limit: No more than 451 local users.
enabled	<i>Optional.</i> Indicates whether the user is enabled (YES) or disabled (NO) by this command.
login_service	<ul style="list-style-type: none"> ▫ Protocol to be used for a login user. Options are: ▫ RLOGIN ▫ TELNET (<i>default</i>) ▫ ClearTCP ▫ Ping - user pings a login host, receives a successful/unsuccessful message and is disconnected.
network_service	Framed protocol to be used by network user. Options: <ul style="list-style-type: none"> ▫ PPP - Point to Point Protocol (<i>default</i>) ▫ SLIP - Serial Line IP. SLIP is not supported currently for LAN-to-LAN users.
password	User password (optional). Limit: 127 ASCII characters. You can create a null password with: <i>password ""</i> .
type	Type of user - may be one or more types. <ul style="list-style-type: none"> ▫ Login uses the login_service specified. ▫ Network (<i>default</i>) uses network_service specified - a dial in user. ▫ Callback users are disconnected after authentication and called back. ▫ Dialout - modem sharing or WAN users. ▫ Manage users have administrative authority.

Arp Command

arp <ip_host_name_or_address>

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

For example, at the prompt, type:

```
HiPer>> arp houston
```

HiPer ARC will generate the following output:

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

Assign Command

assign interfaces <slot:x/mod:[1-y], slot:x/mod:[1-y],...>
modem_group <group_name>

Adds interfaces to an existing modem group or modem groups. To display interfaces assigned to the modem group, use the **show modem_group** command. Modem groups are added by the **add modem_group** command and displayed by the **list modem_groups** command.

Parameter	Description
interface name	Interfaces 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 slot:x/mod:[1-y]; for example: slot:3/mod [2-4], slot:5/mod:6. Limit: 64 ASCII characters.
modem_group	Name of the modem group.

Bye Command

bye

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

Clear Command

clear arp_cache

Deletes all data in the ARP cache without rebooting HiPer ARC. Issue the **list ip arp** command to display ARP statistics.

Copy Command

copy file <input_file> <output_file>

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

Delete Commands

Delete commands remove anything you previously added.

delete aaa_server <name>
preference <number>

Removes the TACACS+ server you created with the **add aaa_server** command. The preference value is the priority ranking of servers. Preference **1** is the highest and **10** is the lowest. Range: **1-10**

delete address_pool user <name>
pool_name <name>

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

delete atm1483 pvc <name>

Removes a Permanent Virtual Circuit (PVC) you created for RFC-1483 compliant networks with the **add atm1483 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

delete atm1577 pvc <name>

Removes a Permanent Virtual Circuit (PVC) you created for RFC-1577 compliant networks with the **add atm1577 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

delete atm_arp_server <name>

Removes a remote ATM ARP server for RFC 1577 compliant networks which you added via the **add atm_arp_server** command. The configured entry must be disabled with the **disable atm_arp_server** command before it may be deleted.

delete board crashdump

Removes the last crashdump saved on HiPer ARC.

delete chat_script <name>

Removes the specified file from the Chat Script table. For more information, see the **add**, **verify**, **show** and **list chat_scripts** commands. Also, see *Appendix E: RADIUS and TACACS+ Systems*.

delete configuration

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

delete cross_connect <name>

Removes ATM cross-connections for VPIs and VCIs on a Hub with multiple ATM NICs installed. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

delete dns cache <number>

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

delete dns host <host_name>

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

delete dns ncache <number>

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

delete dns server preference <preference_number>

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

delete file <file_name>

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

delete filter <filter_name>

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

delete framed_route user <user name>

ip_route <IP_name or address>

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

delete init_script <script_name>

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

delete ip defaultroute gateway <IP_address or name>

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

delete ip network <network_name>

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

delete ip pool <pool name>

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

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

delete ip route <network_name or IP_address/subnet_mask>

all_learned_routes

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

delete ipx network <network_name>

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

delete ipx route <ipx_network_address>
all

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

delete ipx service <service_name>
type [service_type]

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

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

delete ipx service_all

Deletes all IPX *learned* routes from the IPX Static Services Table. Refer to **delete ipx service** and **add ipx service** commands for more information.

delete l2tp lns <1-9>

Removes a local l2tp network server (LNS) from the LAC side of the l2tp tunnel created with the **add l2tp lns** command.

delete login_host preference <preference_number>

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

delete modem_group <group_name>

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

Note: Default modem groups such as al, slot:1/mod:[1-y] and others can't be modified or deleted.

delete mpip client <IP_address>

Deletes the Multilink PPP client you created with the **add mpip client** command.

delete mpip server <IP_address>

Deletes the Multilink PPP server you created with the **add mpip server** command.

delete network service <service_name>

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

delete ping row <number>

Deletes the specified ping row from the Remote Ping Table. See the **ping** command on page -260 for more information.

delete ping service_loss_system <IP_ name or address>

Deletes server connectivity pinging to specified IP name or address.

delete pptp pns <1-9>

Removes a local PPTP network server (PNS) from the client (PAC) side of the PPTP tunnel created with the **add pptp pns** command.

delete snmp community <name>

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

delete snmp community_pool <pool_name>

address <IP_address or name>

Removes an entry from the SNMP Community address Pool table. See the **add snmp community** command for more information.

Parameter	Description
<pool_name>	Pool name defining a group of SNMP management stations.
address	IP address or name of an SNMP management station in the pool.

delete snmp trap_community <name>

Removes 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 snmp trap_community_pool <name>

addresses <IP address list>

Removes entries from the SNMP Trap Community Address Pool table. See **add snmp trap_community_pool** and **list snmp trap_community_pools** commands for more information..

Parameter	Description
<name>	Pool name defining who can receive SNMP traps.
addresses	IP addresses of all SNMP managers associated with the pool , in the form <i>nnn.nnn.nnn.nnn</i> .

delete syslog <IP_name_or_address>

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

delete tap id [all | id]

Removes the particular tap entry (1-99) or *all* entries you added to the tap table with the **add tap** command.

delete telnet client <IP_address/mask>

Removes a TELNET client from a table of users permitted to access HiPer ARC. You may also disable TELNET access globally with the **disable telnet client_access** command. See the **add telnet client** command for more information. Also, issue the **list telnet client** command for a list of configured users. Default: **Disabled**

delete tftp client <IP_name or address>

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

delete tftp request <input_file_name>

Removes specified TFTP entries in the TFTP Client Request Table created with the **add tftp request** command.

delete traceroute row <number>

Removes a specified row from the main traceroute table when entered from an SNMP station or via a command file. The CLI deletes the row immediately upon completion of the traceroute. Range: **1-65535**. See **traceroute**, **list traceroute**, **set traceroute maximum_rows** and **show traceroute** commands for more information.

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/dialout Commands

dial <user_name>

Generates an outgoing call to the location specified by the user name. You can use the **list users** command to list the defined users, along with the services they are defined to work with, and their current status. Limit: **64 ASCII characters**

dialout

l2tp <user_name>

pptp <user_name>

Generates a dialout call to a specified remote user (similar to a manual dialup call) and brings an L2TP or PPTP tunnel up.

Disable Commands

Disable commands inactivate a host of processes previously enabled.

disable accounting

Disables remote accounting via RADIUS or TACACS+. You can use **show accounting** to see if it is currently running, and enable accounting to start accounting.

disable atm1483 pvc <name>

Disables a Permanent Virtual Circuit (PVC) you created for RFC-1483 compliant networks with the **add atm1483 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

disable atm1577 pvc <name>

Disables a Permanent Virtual Circuit (PVC) you created for RFC-1577 compliant networks with the **add atm1577 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

disable atmsig <name>

Disables the UNI (User-Network Interface) signalling configuration on the specified ATM network. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

disable atm_arp_server <name>

Disconnects from and disables a remote ATM ARP server for RFC 1577 compliant networks which you added via the **add atm_arp_server** command. The configured entry must be disabled with the **disable atm_arp_server** command before it may be deleted with the **delete atm_arp_server** command.

disable authentication [local | remote | hint_assigned]

Disallows the following types of authentication:

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

Note: Local authentication takes precedence over remote authentication.

- **Remote** - authentication based on a password stored in a *RADIUS or TACACS+* server.
- **Hint-Assigned** - remote authentication employing *optional IP address* assignment. HiPer ARC automatically assigns a temporary IP address to every dial-in user and reports it with the Framed-IP-Address in the RADIUS authentication request record. The RADIUS server may choose to accept this IP address with an Authentication-Ack message or choose to assign another IP address with an Authentication-Ack message containing no Frame-IP-Address field. Default: **Disabled** .

Issue the **show authentication** command to display settings.

disable authorization

Disallows TACACS+ authorization. If authorization is disabled, HiPer ARC attempts to authenticate based on the *"default"* user profile.

disable command global_terminal_settings_page_breaks

Disallows (for admin CLI users) page breaks (*more* processing) for *all* users. Alternatively, you can disable page breaks *locally* for a manage user's session with the **disable command local_terminal_settings_page_breaks** command. Issue the **set command global_terminal_settings_rows command** to vary the number of rows output to your PC screen. Also, see the **disable** and **show command settings** commands for this feature and the **set command local_terminal_settings_rows** command to edit the number of rows displayed on the system connected only locally to HiPer ARC.

disable command local_terminal_settings_page_breaks

Disallows (for admin CLI users) page breaks (*more* processing) for *locally* (the present session only) connected users. Alternatively, you can disable page breaks *globally* for a manage user's session with the **disable command global_terminal_settings_page_breaks** command. Issue the **set command local_terminal_settings_rows** command to vary the number of rows output to your PC screen. Also, see the **disable** and **show command settings** commands for this feature and the **set command global_terminal_settings_rows** command to edit the number of rows displayed on all HiPer ARC-connected systems.

disable critical_events_to_flash

Disables logging all critical errors to sinks and FLASH memory. This avoids the problem of too many critical errors generating a FLASH overload. Be aware that:

- the error log file is automatically renamed when HiPer ARC reboots,
- critical messages are still output to the Console, and
- issuing the **save all** command preserves this setting in the configuration file.

Use the **show critical_event settings** command to view logging configuration and event sinks and consult the **enable critical_events_to_flash** command for more information. Default: **Disabled**

disable cross_connect <name>

Disables ATM cross-connections for VPIs and VCIs on a Hub or series of Hubs with multiple ATM NICs installed. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

disable direct_request

Disables the TACACS+ direct request functionality you configured with the **set direct_request** command.

disable dns host_rotation

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

disable icmp logging

Disables display of the Internet Control Message Protocol to the SYSLOG server. Use the **show icmp** command to view edits.

disable icmp router_advertise

Disables HiPer ARC-generated router advertisements multicast on the same LAN segment as HiPer ARC. Use the **show icmp** command to view edits.

disable ilmi <atmaal:1 | atmaal:2>

Disables Interim Link Management Interface (ILMI) address registration supporting network management functions between users and the network. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

disable interface <interface name>

Disables any specified interface and if a call is up on the interface it will be disconnected. A disabled interface remains in the Interface Table, but will not transmit or receive any data. You can enter multiple interfaces as follows: slot:2/mod:5,slot:2/mod:7,slot:4/mod:3,slot:4/mod:8, or a range: slot:1/mod:[1-9]. Use the **list interfaces** command to see the currently defined interfaces, and their status.

disable ip address_pool_filtering

Disables packet filtering on all IP address pools (drops packets for IP addresses within IP pools *not in use*). See *Chapter 8: Packet Filters* for more information. Use the **show ip settings** command to view edits.

disable ip address_pool_round_robin

Turns off round robin allocation of IP addresses from IP address pools configured with the **add ip pool** command. Issue the **enable ip address_pool_round_robin** command to turn this feature on. Use the **show ip settings** command to view the current setting. Default: **ENABLED**

disable ip forwarding

Causes the system to stop forwarding any packets over IP networks but HiPer ARC will still operate as a client - under most circumstance, you would never disable forwarding. You may want to disable ip forwarding if you are using the system only as a terminal server since users who TELNET to the system can still connect to remote hosts. Use the **show ip settings** command to view edits.

disable ip multicast_heartbeat

Disables multicast monitoring for a specified multicast group or interface. See enable **ip multicast_heartbeat**, **set ip multicast_heartbeat**, and **show ip settings** commands for more information.

disable ip network <network_name>

Disables the specified IP network. Make sure there is no activity on this network before disabling it.

disable ip rip

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

disable ip routing

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

disable ip security_option drop_all_fragoffset1

disable ip security_option drop_tcp_fragoffset1

disable ip security_option disallow_all_header_options

disable ip security_option disallow_source_route_options

Each of the above commands disables the global filtering of all IP packets containing the specified datagram fields (see **enable ip security_option** command). This security feature also syslogs the event when the particular packet is dropped. Use the **show ip security** command to view edits.

disable ip static_remote_routes

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

disable ipx network <network_name>

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

disable ipx rip network <network_name>

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

disable ipx sap network <network_name>

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

disable l2tp lns <1-9>

Prevents the specified HiPer ARC from receiving tunnel requests as an L2TP network server (LNS). See the **enable l2tp lns** command for more information. Default: **Enabled**

disable link_traps interface

interface_name [eth:1, eth:2 or slot:x/mod:y]
modem_group [name]

Prevents SNMP from sending linkup and linkdown traps for the specified interface or modem group. We recommend you disable this feature on all *modem* interfaces to eliminate a barrage of perfunctory awareness messages forwarded from the NMC to the HiPer ARC alarm server whenever modem states change or HiPer ARC reboots. Although the default is **DISABLED** on modem interfaces, Hubs with *Quad Modems* installed must have the HiPer ARC setting disabled manually to effect the change. The command is **ENABLED** for Ethernet and WAN connections.

You can see if the interface is currently enabled for traps by using the **show interface settings** command.

disable modem_group <name>

Disables the modem group you enabled with the **enable modem_group** command. Modem groups *all* and others incorporating installed modem cards (e.g.: *slot:3*) are provided as default modem groups, making system-wide or slot-by-slot disabling possible. Use the **show modem_group** command to view INACTIVE status of disabled modem groups.

disable network service <service_name>

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

disable nmc chassis_awareness

Disables the dynamic configuration of the chassis modems. If chassis configuration updates from the Network Management Card (NMC) are received, they are ignored. All chassis slot configuration must be done through the CLI, CFM load or SNMP sets. Use the **show nmc settings** command to view edits.

disable nmc dsa_idle_rebalancing

Disallows idle modems to be periodically re-balanced by allowing slot ownership reassignment by the NMC. See **enable nmc dsa_idle_rebalancing** and **show nmc** commands for more information. Default: **Disabled**

disable nmc dynamic_slot_assignment

Turns off the identification of Chassis cards for dynamic slot assignment (DSA) in support of static load balancing and hot-standby fault tolerance. For more information, see **enable nmc dynamic_slot_assignment** and **show nmc settings** commands.

disable ntp

Disables the Simple Network Time Protocol which references clocks located on the Internet. See the **enable ntp** and **set ntp** commands for more information.

disable ping service_loss_system <IP_name or address>

Disables HiPer ARC ability to repeatedly ping the specified system to check for connectivity. Use the **list ping service_loss_system** command to view edits.

disable ppp offloading

Disables any PPP attempt to offload framing to modem cards.

disable pptp pns <1-9>

Disables the specified PPTP network server. See the **enable pptp pns** command.

disable primary_accounting_server

Disables the primary accounting server you configured with the **set accounting primary_server** command.

disable prompting single_level

Disables "first level" CLI prompting of Login/Network users by HiPer ARC. When enabled, this function bypasses the *Login/Network* prompt for those users, depositing them directly at the *HiPer>* prompt line, but still allows all first level accessed services such as TELNET, Rlogin, traceroute, etc. See **enable prompting single_level** and **show prompting single_level** commands for more information. Default: **Disabled**

disable radius fill_null_attributes

Disables the filling of *null* attributes in RADIUS accounting and authentication packets. Issue the **show radius** command to view settings. See the **enable radius fill_null_attributes** command for more information.

disable radius interim_accounting_interval

Disables interim accounting on the RADIUS server configured with the **set radius** command. Issue the **show radius** command to view settings. See the **enable radius interim_accounting_interval** command for more information. Default: **Disabled**

disable secondary_accounting_server

Disables the secondary accounting server you configured with the **set accounting secondary_server** command.

disable security_option remote_user_administration <dialin | telnet>

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

disable security_option snmp user_access

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

disable service_loss_busy_out [ping | radius]

Disallows busyout of modems if there is no connectivity to the RADIUS or PING servers. Use the **show service_loss_busyout** command to view edits. **Important:** *both* PING and RADIUS busy out features cannot be *enabled* at the same time. If the PING busy-out feature is enabled and you attempt to enable RADIUS busy-out, you'll receive an error message.

disable slip offloading

Disallows gateway card from trying to offload SLIP framing to modem cards. Use the **show slip** command to view edits.

disable snmp authentication traps

Instructs SNMP to stop recording trap information for user (either local or remote) authentication. Use the **show snmp** command to view edits.

disable system reset_eeprom

Disallows inclusion of earlier-saved EEPROM configuration when performing a bulk configuration download. See **enable system reset_eeprom**, **show system** and **reset configuration** commands for more information. Default: **DISABLED**

disable tacacsplus interim_accounting_interval

Disallows watchdog accounting on the TACACS+ server. See the **disable** and **set tacacsplus interim_accounting_interval** commands for more information.

disable tcp keepalives

Disallows TCP keep-alive support for all TCP sessions begun after this command is issued. See **enable tcp keepalives** and **set tcp keepalive_interval** commands for more information. Default: **Disabled**

disable tcp nagle_algorithm

Disallows use of the Nagle algorithm to allow transmission of small packets for TCP applications which require them. This algorithm withholds additional packet transmissions to an output buffer until there is sufficient data to fill a maximum-sized segment. See **enable tcp nagle_algorithm** and **show tcp** commands. Default: **Enabled**

disable telnet

client_access
escape
terminal_download_mode
trying_message

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

Parameter	Description
client_access	Disallows users from telnetting into HiPer ARC. Default: Disabled
escape	All TELNET clients are prevented from using the escape character during a session.
terminal_download_mode	Disables feature which <i>turns off</i> local and remote echo for TELNET on a TCP port other than 23 for a HiPer ARC TELNET client. Default: Disabled
trying_message	Turns off the trying status message for clients attempting to TELNET out of HiPer ARC. When escape is disabled, TELNET clients who issue the escape character during their session will not get a local TELNET command line (the character is sent as regular text).

disable tftp request <input_file_name>

Deactivates a request for service (get or put) from the TFTP server created with the **add tftp request** command. Use the **list tftp request** command to display TFTP request status.

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. Use **list users** and **show user** commands to view edits.

Disconnect Command

disconnect l2tp tunnel <number>

Disconnects the specified L2TP tunnel, bringing down all sessions running in the tunnel.

disconnect l2tp tunnel <number> **session** <number>

Brings down the specified call running in the L2TP tunnel. When the last session is brought down, the tunnel comes down with it. See the **list l2tp tunnels** command to view tunnel session information.

disconnect pptp tunnel <number>

Disconnects the specified PPTP tunnel, bringing down all sessions running in the tunnel.

disconnect pptp <number> **session** <number>

Brings down the specified call running in the PPTP tunnel. When the last session is brought down, the tunnel comes down with it. See the **list pptp tunnels** command to view tunnel session information.

disconnect user <name>

Brings down the specified user connection.

Do Command

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

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

Edit Command

edit or **edit** <input_file_name>

HiPer ARC's text editor, **edit** is similar to UNIX Version 7's edit facility with some subtle differences. Its purpose is similar - to perform simple line editing of files, including filter files.

Edit is available on the Console, through a dialed-in connection, or via TELNET. It works best when displayed on an ANSI terminal since it employs escape sequences defined for the ANSI terminal type to clear screens and display menus. To access Help for this command, type a question mark (?) at the colon prompt (:). For more information on edit commands, see *Chapter 9: Administrative Tools*.

Note: Edit is especially convenient when creating small or editing large filter files. An alternative method uses TFTP but this method is more suited to creating large filter filters.

Enable Commands

enable accounting

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

enable atm1483 pvc <name>

Enables a Permanent Virtual Circuit (PVC) you created for RFC-1483 compliant networks with the **add atm1483 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

enable atm1577 pvc <name>

Enables a Permanent Virtual Circuit (PVC) you created for RFC-1577 compliant networks with the **add atm1577 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

enable atm_arp_server <name>

Re-enables a previously disabled remote ATM ARP server for RFC 1577 compliant networks which you added with the **add atm_arp_server** command. See also **disable atm_arp_server** and **delete atm_arp_server** commands for more information.

enable atmsig <name>

Enables the UNI (User-Network Interface) signalling configuration on the specified ATM network. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

enable authentication <local | remote | hint_assigned>

Permits the following types of authentication:

- **Local** - user authentication based on a password specified in the User Table. When you issue the **add user** command, entering a password activates local authentication. If no password is specified (passwords are optional), and remote authentication is not enabled, the user will not be able to establish a connection. Local authentication is **enabled** globally by default.

Note: Local authentication takes precedence over remote authentication.

- **Remote** - authentication based on a password specified in a *RADIUS* or *TACACS+* server.
- **Hint-Assigned** - remote authentication employing *optional IP address* assignment. HiPer ARC automatically assigns a temporary IP address to every dial-in user and reports it with the Framed-IP-Address in the RADIUS authentication request record. The RADIUS server may choose to accept this IP address with an Authentication-Ack message or choose to assign another IP address with an Authentication-Ack message containing no Frame-IP-Address field. Default: **Disabled**

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

enable authorization

Allows TACACS+ authorization. If authorization is disabled, HiPer ARC attempts to authenticate based on the "default" user profile (username and password). Default: **Enabled**

enable command global_terminal_settings_page_breaks

Allows an administrative (*manage*) user to *globally* (for all HiPer ARC sessions) enable page breaks for commands which display text - list, show, et al - that would otherwise overflow the boundaries of the display screen. Alternatively, you can enable page breaks *locally* for a manage user's session with the **enable command local_terminal_settings_page_breaks** command. Issue the **set command global_terminal_settings_rows** command to vary the number of rows output to your PC screen. Also, see the **disable** and **show command settings** commands for this feature and the **set command local_terminal_settings_rows** command to edit the number of rows displayed on the system connected only locally to HiPer ARC.

enable command local_terminal_settings_page_breaks

Allows an administrative (*manage*) user to *locally* (for the present session only) enable page breaks for commands which display text - list, show, et al - that would otherwise overflow the boundaries of the display screen. Alternatively, you can enable page breaks *globally* for a manage user's session with the **enable command global_terminal_settings_page_breaks** command. Issue the **set command local_terminal_settings_rows** command to vary the number of rows output to your PC screen. Also, see

the **disable** and **show command settings** commands for this feature and the **set command global_terminal_settings_rows** command to edit the number of rows displayed on all HiPer ARC-connected systems.

enable critical_events_to_flash

Enables logging all critical errors into all sinks and FLASH memory. Issue this command when a FLASH overload due to many critical errors is *not* anticipated. Be aware that the error log file is *not* automatically renamed when HiPer ARC reboots. Issuing the **save all** command preserves this setting in the configuration file.

Use the **show critical_event settings** command to view logging configuration and event sinks and consult the **disable critical_events_to_flash** command for more information. Default: **Disabled**

enable cross_connect

Enables ATM cross-connections for VPIs and VCI on a Hub or series of Hubs with multiple ATM NICs installed. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

enable datalink ppp

interface <interface_name>

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

enable direct_request

Enables the TACACS+ directed request functionality you configured with the **set direct_request** command.

enable dns host_rotation

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

enable icmp logging

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

enable icmp router_advertise

Enables HiPer ARC-generated router advertisements multicast on the same LAN segment as HiPer ARC. Use the **show icmp settings** command to view the current setting.

enable ilmi <atmaal:1 | atmaal:2>

Enables Interim Link Management Interface (ILMI) address registration which supports network management functions between the user-side and network-side of the ATM UNI (User-Network Interface) interface. User-side configuration concerns customer premises equipment while network-side configuration concerns the network switch. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

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 (slot:3/mod:[1-9]). You can use **list interfaces** to see which interfaces are defined, and whether they are currently disabled. Use the **show icmp settings** command to view edits.

enable ip address_pool_filtering

Permits packet filtering on all IP address pools. See *Chapter 8: Packet Filters* for more information. Use the **show ip command** to view the current setting.

enable ip address_pool_round_robin

Turns on round robin allocation of IP addresses from IP address pools configured with the **add ip pool** command. Issue the **disable ip address_pool_round_robin** command to turn this feature off. Use the **show ip settings** command to view the current setting. Default: **Enabled**

enable ip forwarding

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

enable ip multicast_heartbeat

Enables multicast monitoring for a specified multicast group or interface. See **disable ip multicast_heartbeat**, **set ip multicast_heartbeat**, and **show ip settings** commands for more 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**. Use the **show ip routing** command to view the current setting.

enable ip routing

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

enable ip security_option drop_all_fragoffset1**enable ip security_option drop_tcp_fragoffset1****enable ip security_option disallow_all_header_options****enable ip security_option disallow_source_route_options**

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

*Note: Disallow and drop commands work in conjunction with each other. The **disallow_source_route_options** command is a subset of the **disallow_all_header_options** command so if you enable the **source route** command you must disable the all header command. But, enabling the more inclusive all header value renders the **source route** command unnecessary whether enabled or not. The same logic holds true for drop commands.*

The datagram fields shown below, when found, cause the packet to be dropped.

- **fragment offset=1** - packets with an offset equal to one are discarded in accordance with RFC 1858. Some routers that may be used on the same network with HiPer ARC may be configured to filter out specific traffic. In some cases these routers will not apply the filter correctly for IP packets with an offset of 1. To avoid this hole in the filtering mechanism, packets of this type can be discarded. Of the two drop commands, this is the highest level of security. Default: **enabled**
- **partial TCP headers** (offset=1) - Protocol field in the IP packet header (in this case, TCP). Packets of this type can be discarded. Lower level of security than All fragmented packets (Drop_all_fragoffset1). Default: **enabled**
- **all header options** - all choices in the IP Options field of the IP header. IP options may be generated as an attack to get past routing tables. To avoid this hole in security, packets of this type can be discarded. Of the two disallow commands, this is the highest level of security. Default: **disabled**
- **source route options** - another choice in the IP Options field of the IP header. Particular path the sender chooses to take through the network to reach its destination, as specified in the sender packet's IP header. Packets of this type can be discarded although this is a lower level of security than All Header Options. Default: **disabled**

enable ip static_remote_routes

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

enable ipx network <network_name>

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

enable ipx rip network <network_name>

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

enable ipx sap network <network_name>

Enables the 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** commands.

enable l2tp lns <1-9>

Enables the specified HiPer ARC to receive tunnel requests as an L2TP network server (LNS). See the **disable l2tp lns** command for more information. Default: **Enabled**

enable link_traps interface

interface_name [eth:1, eth:2 or slot:x/mod:y]
modem_group [name]

Informs SNMP to send linkup and linkdown traps for the specified interface or modem group. We recommend you disable this feature on all *modem* interfaces to eliminate a barrage of perfunctory awareness messages forwarded from the NMC to the HiPer ARC alarm server whenever modem states change or HiPer ARC reboots. Although the default is **Disabled** on modem interfaces, Hubs with *Quad Modems* installed must have the HiPer ARC setting disabled *manually* to effect the change. The command is **Enabled** for Ethernet and WAN connections.

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. Modem groups *all* and others incorporating installed modem cards (e.g.: *slot:3*) are provided as default modem groups, making system-wide or slot-by-slot enabling possible. 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 nmc chassis_awareness

Enables the dynamic configuration of chassis modems. When chassis configuration updates from the Network Management Card (NMC) are received, they are used to update slot configuration. This command can be used in conjunction with the **enable nmc dynamic_slot_assignment** command described below. Default: **Enabled**. Use the **show nmc settings** command to view edits.

enable nmc dsa_idle_rebalancing

Allows idle modems to be periodically re-balanced by allowing slot ownership reassignment by the NMC. Slots are monitored for idleness and if idle slots are discovered to have caused unbalanced modem allocation, modems will be re-assigned to another slot. See **disable nmc dsa_idle_rebalancing** and **show nmc** commands for more information. Default: **Disabled**

enable nmc dynamic_slot_assignment

Identifies cards in the Total Control Hub for dynamic slot assignment (DSA) to support static load balancing and hot-standby fault tolerance. Default: **Disabled**

DSA is an algorithm in the Network Management Card (NMC) which periodically polls chassis application cards for slots which support DSA. The NMC summarizes the information received and forwards that data to each HiPer ARC, and on the basis of that data computes statically load-balanced slot assignments. New assignments are made every time a modem or application card is removed from or inserted in the Hub. DSA performs automatic load balancing whenever two or more application (HiPer ARC) cards are present in the chassis, assigning all calls, in turn, to successive HiPer ARCs (Slot:1 - Hiper1, Slot:2 - HiPer2, Slot:3 - Hiper3, etc.). If a modem card reboots and is not statically assigned to a particular application card, then the modem slot is assigned to the application card with the least load.

*Note: By default, when HiPer ARC cards come up they are set to have ownership of all slots. So, it's very important that if you want to use DSA or have more than one HiPer ARC card that you properly configure slot ownership with the **set chassis slot** command. DSA will only reassign slots that have ownership of **no**.*

DSA is best suited for use as a "hot fail over" redundancy feature in the case where one HiPer ARC fails and a second HiPer ARC assumes ownership of all chassis cards. In this way, DSA can be employed in conjunction

with static chassis card configuration to provide protection against a single point of failure. This type of configuration is advantageous when all chassis cards are supported by one HiPer ARC with a second HiPer ARC used as an emergency backup.

In the example of a chassis containing 14 HDM cards and 2 HiPer ARCs, we recommend you:

- Enable chassis awareness with the **enable nmc chassis_awareness** command (ENABLED by default) and either:
- Enable DSA with the above command and set *slot ownership* of each slot to NO (**set chassis slot <x> owner no**), or,
- Statically configure each HiPer ARC to own 7 modem cards each. The command used on each HiPer ARC is: **set chassis slot <x> owner yes**

Note: In the case where a chassis slot is contested by the same HiPer ARC, DSA will assign ownership of that slot to the HiPer ARC occupying the lowest slot. Also, DSA never changes modem card ownerships unless a modem reboots or a HiPer ARC reboots unless Idle Rebalancing is enabled. Then the system will periodically reassign modems to HiPer ARC when not in use.

Note: Make sure that if your're using fail-over that you provide enough resources (IP addresses) on all HiPer ARC cards to support this feature.

enable ntp

Enables the Simple Network Time Protocol (NTP), which references a clock located on the Internet, allowing HiPer ARC to synchronize its clock setting with a server of your choice. See the **set ntp** and **disable ntp** commands for more information.

enable ping service_loss_system <IP_name or address>

Enables HiPer ARC to repeatedly ping the specified system to check for connectivity. Use the **show service_loss_system** settings command to view edits.

enable ppp offloading

Enables PPP attempts to offload PPP framing to modem cards. Default: **enabled**

enable pptp pns <1-9>

Enables the specified PPTP network server. See **disable pptp pns** command. Default: **Enabled**

enable primary_accounting_server

Enables the primary accounting server you configured with the **set accounting primary_server** command.

enable prompting single_level

Enables "first level" CLI prompting of Login/Network users by HiPer ARC. This function bypasses the standard *Login/Network* prompt for those users, depositing them directly at the *HiPer>* prompt line where the *Network* keyword can be issued. The command still permits all first level accessed services such as TELNET, Rlogin, traceroute, etc., and lets properly configured Login/Network users invoke a PPP session *after* completing any TELNET/Rlogin/ClearTCP sessions, if desired. After the PPP session ends, though, the connection is terminated. See **disable prompting single_level** and **show prompting single_level** commands for more information. Default: **Disabled**

enable radius fill_null_attributes

Permits the filling of null attributes in RADIUS accounting and authentication packets. If enabled, RADIUS accounting/authentication records will contain attributes with 'X' rather than a null string. The **show radius** command displays current settings.

enable radius interim_accounting_interval

Permits interim accounting on the RADIUS server configured with the **set radius** command. The **show radius** command displays current settings. Default: **Disabled**

enable secondary_accounting_server

Enables the secondary accounting server you configured with the **set accounting secondary_server** command.

enable security_option remote_user_administration <dialin | telnet>

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

enable security_option snmp user_access

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

enable service_loss_busy_out [ping | radius]

Allows HiPer ARC to busy out modems if there is no connectivity to the PING or RADIUS server. **Important:** you cannot enable *both* PING and RADIUS busy out features at the same time. If the PING busy-out feature is enabled and you attempt to enable RADIUS busy-out, you'll receive an error message. Use the **show service_loss_busyout** command to view edits. Default: **Disabled**

enable slip offloading

Allows gateway card to try offloading SLIP framing to modem cards. Use the **show slip** command to view edits. Default: **Enabled**

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. Use the **show snmp** command to view edits. Default: **Enabled**

enable system reset_eeprom

Applies earlier-saved EEPROM configuration when performing a bulk configuration download. EEPROM settings are saved in the *bspman.cfg* file when a **save all** is performed. This file and configured *filter files* are saved in the *bulk configuration file* when a **save configuration** command is issued. This command applies these saved EEPROM settings back into HiPer ARC when the bulk configuration file is downloaded and a **reset configuration** command issued.

See **disable system reset_eeprom**, **show system**, **reset configuration** and **save configuration** commands for more information. Default: **DISABLED**

Warning: We recommend you do not use this command unless you are an expert user.

enable tacacsplus interim_accounting_interval

Permits watchdog accounting on the TACACS+ server. See the **disable** and **set tacacsplus interim_accounting_interval** commands for more information.

enable tcp keepalives

Permits TCP keep-alive support for all TCP sessions begun after this command is issued. See **disable tcp keepalives** and **set tcp keepalive_interval** commands for more information. Default: **Disabled**

enable tcp nagle_algorithm

Allows use of the Nagle algorithm to limit small TCP packet transmissions and maintain high network throughput. This algorithm withholds additional packet transmissions to an output buffer until there is sufficient data to fill a maximum-sized segment. You may want to disable this feature if your TCP application must transmit small TCP packets; in that case, use the **disable tcp nagle_algorithm** command. Default: **Enabled**

enable telnet

client_access
escape
terminal_download_mode
trying_message

Allows various TELNET functions. Use the **show telnet** command to view settings.

Parameter	Description
client_access	Allows users to TELNET into HiPer ARC. This command is used in conjunction with the add telnet client command. See the list telnet client command for settings. Default: Disabled
escape	All TELNET clients are permitted to use the escape character during a session. By default the escape character is Ctrl] (right bracket). A user can change that value using <i>set_escape</i> in the TELNET program.
terminal_download_mode	Turns off local and remote echo for TELNET on a TCP port other than 23 for a HiPer ARC TELNET client. When enabled, this function forces TELNET clients to negotiate TELNET ECHO DISABLE for both local and remote sides of the connection. Default: Disabled
trying_message	Turns on the trying status message for clients attempting to TELNET out of HiPer ARC. When escape is enabled, TELNET clients who issue the escape character during their session will get a local TELNET command line. This function is not supported for login users.

enable tftp request <input_file_name>

Activates a request for service (get or put) from the TFTP server created with the **add tftp request** command. Use the **list tftp request** command to display TFTP request status.

enable user <name>

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

Exit Command

exit

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

Hangup Commands

Cuts interface or modem group connections.

hangup interface <interface_name>

Disconnects any calls (causes the connection on the specified interface to hangup and leave the interface(s) in an *Enabled* state. You can enter multiple interfaces (e.g.): slot:1/mod:4,slot:2/mod:3 or a range: slot:1/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. See **add modem_group**, **list modem_groups** and **show modem_group** commands for more information.

Help Command

help <command>

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

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

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

Hide Command

hide events

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

History Command

history

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

For example:

```
arp
arm camus
arp camus
arp carrot
li chas
```



```
li int
hosT cassatt
host carrot
hisTORY
```

Host Command

host <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 (add DNS host) or a DNS server entry (add DNS server) to resolve the name. This command is identical to the **resolve name** command.

Network Name: cassatt.mass-usr.com
is resolved to address: 153.234.24.145

Join Command

join ip igmp <IP_multicast_address>

interface <eth:1 | eth:2 | slot:x/mod:y>

Adds a member to this multicast address group. Entries are added to the IGMP Cache Table. Issue a **list interfaces** command to view assigned interface names and the **leave ip igmp**.

Kill Command

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.

*Note: You must type upper case letters and type the full process name when issuing the **kill** command.*

Leave Command

leave

Exits a *manage* user from the CLI, but keeps the link up. This command returns you to Dial-In user or TELNET commands. For example:

```
manage: leave
HiPer:
```

leave ip igmp <IP multicast address>

interface <interface name>

Removes a member from this multicast address group configured with the **join ip igmp** command. Entries are deleted from the IGMP Cache Table.

List Commands

Displays information saved as entries in HiPer ARC tables.

list aaa_server

Displays configuration information of TACACS+ servers. For example:

AAA Server Table			
AAA Name	Preference	IP Address	State
aaa	1	149.112.189.180	ENABLED
3com.com	2	149.112.189.183	ENABLED
mindspring.com	3	149.112.189.196	ENABLED
toast.com	4	192.147.72.18	ENABLED
gov.net	5	149.112.189.199	ENABLED

list all sessions vpn <domain_name>

Displays all active tunnel sessions for the specified domain name. While not displayed by this command, the domain name appears in the **list all tunnels** output, shown below.

Sessions				
TunID	SessID	UserName	PeerIPAddress	Type
2	2	ppp1	149.112.214.146	L2TP

list all tunnels

Displays settings and statistics for all active tunnels on the system. Information for both LAC and LNS devices is displayed. This command is useful for Internet Service Providers offering domain-based tunnel services.

TUNNELS						
TunID	Domain	PeerIPAddress	Type	Sessions	StartDate	StartTime
2	Unspecified	149.112.214.146	L2TP	1	25-JUN-1998	00:28:29

list active interfaces

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

Interface Name	Oper Status	Admin Status
loopback	Up	Up
internal	Up	Up
eth:1	Up	Up
eth:2	Down	Up
slot:3/mod:1	Up	Up
slot:3/mod:2	Up	Up
slot:3/mod:3	Up	Up
slot:3/mod:4	Up	Up

list atm1483 pvcs

Displays Permanent Virtual Circuits (PVC) you created for RFC-1483 compliant networks with the **add atm1483 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*. The command lists:

PVC Name	VPI	VCI	Protocol	address	Status
ip_over_atm	1	220	IP	204.249.183.47	ENABLED
pvc_0_44	0	44	IPX	204.249.183.45	ENABLED

list atm1577 pvcs

Displays Permanent Virtual Circuits (PVC) you created for RFC-1577 compliant networks with the **add atm1577 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

PVC Name	VPI	VCI	Network Name	Status
atm1577	0	110	ip_atm1577	ENA
pvc_0_44	0	44	ip2_atm1577	ENA

list atm_arp_server

Displays settings for the ATM ARP server you configured with the **add atm_arp_server** command. The ATM ARP server maps IP addresses of connected servers to 20-byte ATM addresses. It lists:

ARP Server Name	ATM address	Subnet	State	Interface
arp_server	11.22.33.44.55.6 6.77.88.99.00.11 22.33.44.55.66.7 7.88.99.00	204.249.180.4	ENA	atmnet:1

list available servers

Displays the available network servers and supported network services. The choices are: Dialout service, SNMP service, TELNET service, TFTP service, or ClearTCP. The services listed by this command are used in the *server_type* field of the **add network service** command.

Server Type	Type	Protocol	Module	Description
ClearTCPD	NETWORK	TCP	Telnet	ClearTCPD, enabling access to a modem group.
DialOut	NETWORK	NCSI	DialOut	An IP Dial-out server.
SNMPD	NETWORK	UDP	SNMPAgent	SNMP agent.
TELNETD	NETWORK	TCP	Telnet	TELNET server. Either to the CLI or a modem group.
TFTPD	NETWORK	UDP	TFTP	Server side of TFTP, for accessing files.

list chassis

Displays chassis settings for all slots. The following example illustrates a chassis configuration where dynamic information is received from the NMC.

Note: No NMC slot information is available.

Slot	Owner	Description	Ports	Type
1	YES	High Density Modem 24 Channels	23	Dynamic
2	YES	High Density Modem 30 Channels	29	Dynamic
3	YES	Quad Analog V.32 Terbo Modem	4	Dynamic
4	YES	Quad Anal-Digi V.34 Modem	4	Dynamic

Slot	Owner	Description	Ports	Type
5	YES	EMPTY--	0	Static
6	YES	EMPTY--	0	Static
7	NO	EMPTY--	0	Static
8	NO	Windows NT Server NAC	0	Dynamic
9	NO	Quad Analog V.32 Terbo Modem	4	Dynamic
10	NO	Quad Analog V.32 Terbo Modem	4	Dynamic
11	NO	Quad Analog V.32 Terbo Modem	4	Dynamic
12	NO	Quad Analog V.32 Terbo Modem	4	Dynamic
13	NO	Quad Analog V.32 Terbo Modem	4	Dynamic
14	NO	EMPTY--	0	Static
15	NO	EMPTY--	0	Static
16	YES	HiPer Access Router NAC	0	Dynamic

The example below illustrates a chassis configuration where no NMC exists and only statically configured cards are shown:.

Slot	Owner	Description	Ports	Type
1	YES	High Density Modem 24 Channels	23	Static
2	YES	High Density Modem 30 Channels	29	Static
3	YES	Quad Modem	4	Static
4	YES	RISCC HiPer ARC NAC	0	Static
5	YES		0	Static
6	YES		0	Static
7	NO		0	Static
8	NO		0	Static
9	NO		0	Static
10	NO		0	Static
11	NO		0	Static
12	NO		0	Static
13	NO		0	Static
14	NO		0	Static
15	NO		0	Static
16	NO		0	Static

list chat_scripts

Displays the chat script files you added to the Chat Script table. For more information, see the **add**, **delete**, **verify** and **show chat_script** commands. Also, see *Appendix E: RADIUS and TACACS+ Systems*. It lists:

CHAT SCRIPTS

Name	Status
hiper1	CHAT_SCRIPT_NORMAL

list connections

Displays all connections established on switched interfaces. It lists:

- **IfName** - Modem slot and interface of current connections
- **User Name** - name of users currently connected
- **Type** - current type of connections established on modems. They include:
 - **On-demand** - user connection established for on-demand purposes

- **Dial-back** - user connection established for callback purposes
- **Continuous** - user connection established for continuous utilization
- **Manual** - user connection established on the fly
- **Timed** - user connection established for a particular interval
- **ShrMod (Shared-modem)** - dialout user connection to a modem utilizing a login service (TELNET or rlogin) or NCSI. LED does not light until call is unhooked (amber) and connected (green). NCSI sessions using the port redirector display *None* as the DLL type.
- **Dialin** - user connection established for dialin purposes. LED lights *amber* when modem is unhooked, *green* when call is connected.
- **Bond** - user connection utilizing bandwidth allocation
- **Dedicated** - user connection established for a particular user
- **DLL** - data link layer that the specified dial-in session is connected to: **NONE, PPP, SLIP, SHELL, RL(O)G(I)N, TLNT, PING, ADMN, CL(EAR)TCP, L2TP, PPTP, TAP, PRMT**
- **Start Date** - start date of a connection established on the specified interface
- **Start Time** - start time of a connection established on the specified interface

IfName	User Name	Type	DLL	Start Date	Start Time
slot:3/mod:1	larry	DIALIN	SLIP	05-AUG-1997	13:56:1
slot:3/mod:2	ginger	SHRMOD	SHELL	05-AUG-1997	13:57:2
slot:3/mod:1	larry	DIALIN	PPP	21-SEP-1997	00:34:25

list critical events

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

CRITICAL EVENTS

Event

At 22:01:39, Facility "GWC PBUS Modem Driver", Level "CRITICAL": GWCMDM_AL, slot:3/mod:1 TAPI_OPEN failed, retrying

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

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

list cross_connect

Displays ATM cross-connections for Virtual Path Indicators (VPI) and Virtual Channel Indicators (VCI) configured with the **add cross_connect** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*. The command lists:

Cross Connect Name	Port	VPI	VCI	Port	VPI	VCI	PCR	State
connect_0_100	1	0	700	2	0	900	100000	ENA

list dialout

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

- **Index** - table list
- **General (Modem Group) Name** - modem group name for the interface enabling network users access to the communication server interfaces without requiring the user to know the specific name or location of an interface.
- **Specific (Interface) Name** - particular name associated with this interface enabling a network user to find a particular port for access to a specified service associated with that interface.
- **State** - condition of the interface regarding dialout use: **InUse**, **Available**, and **Unavailable**.
- **Type** - the type of network connection: **None** (if no client attached), **IP** or **IPX**.
- **Address** - Ethernet address of the remote station: IP address for IP, MAC address for IPX. If an IP, IPX or no client is attached to HiPer ARC port, this value is all zeros..

DIALOUT CONNTECTIONS

Index	General (Modem Group) Name	Specific (Interface) Name	State	Type	Address
1	All	slot:3/mod:3	Available	None	0.0.0.0

list dns cache

Displays entries in the DNS Cache table.

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

DNS CACHE TABLE

Number	Pretty Name	Class	Type	Source
1	cassatt.mass-usr.com	1	1	153.234.24.145
2	mass-usr.com	1	2	153.234.24.145
3	cassatt.mass-usr.com	1	1	153.234.24.145
4	uswb1rd1.mass-usr.com	1	1	153.234.24.145
5	ns1.ma.ultra.net	1	1	153.234.24.145
6	sinbad.mass-usr.com	1	1	153.234.24.145

list dns hosts

Displays the DNS local host and its IP address, which you configured using **add dns host** command. For example:

DNS LOCAL HOSTS

Name	address
scylla	123.34.234.145
charybdis	123.45.234.87

list dns ncache

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

- **Number** - Row number in DNS Negative Cache Table.

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

DNS NEGATIVE CACHE TABLE

Preference	Pretty Name	Class	Type	Source
1	cassatt.mass-usr.com	1	1	153.234.24.145
2	mass-usr.com	1	2	153.234.24.145
3	cassatt.mass-usr.com	1	1	153.234.24.145

list dns servers

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

- **Preference** - server priority for DNS service
- **Name** - your name for the server
- **address** - IP address of server
- **Status** - current status (ACTIVE, INACTIVE)

DNS NAME SERVERS

Preference	Name	address	Status
1	scylla	134.134.140.145	ACTIVE
2	charybdis	123.145.166.187	ACTIVE

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. For example

Facilities	
Event Facility	Log Level
ATM Network Driver	Critical
Attach Process	Critical
Auth Facility	Critical
Board Support Management Process	Critical
Call Initiation Process	Critical
Command Line Interpreter	Critical
Configuration File Manager	Critical
Configurator	Critical
Console Driver	Critical
DNS	Critical
Discovery	Critical
Driver	Critical
Ethernet Driver	Critical
Event Handler	Critical
Filter Manager Process	Critical
GWC PBUS Modem Driver	Unusual

IP	Critical
IP Dial-out Process	Critical
IP Routing Process	Critical
IP Spoofing Process	Critical
L2TP	Critical
MIB Registrar	Critical
NMIF	Critical
NTP - Network Time Protocol	Critical
Network Management Bus Agent	Critical
Network Management Bus Driver	Critical
Network Management Configuration	Critical
Network Management Interface	Critical
PPP	Critical
PPP Trace	Critical
Polling Process	Critical
Remote Ping Process	Critical
RoboExec	Critical
Sbus	Critical
SLIP Process	Critical
SNMP	Critical
TCP	Critical
TFTP Process	Critical
Telnet	Critical
Traceroute	Critical
UDP	Critical
URP	Critical

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. For example:

Atmarp.cfg	0	FILE_READ_WRITE
CLI.cfg	41	FILE_READ_WRITE
CallInitProcess.cfg	11490	FILE_READ_WRITE
Chassis.cfg	467	FILE_READ_WRITE
ConfigProcess.cfg	4916	FILE_READ_WRITE
DNS.cfg	125	FILE_READ_WRITE
DialOutProcess.cfg	29	FILE_READ_WRITE
EventHandler.cfg	0	FILE_READ_WRITE
FilterMgr.cfg	24	FILE_READ_WRITE
IPForwarder.cfg	340	FILE_READ_WRITE
IpRterProcess.cfg	24	FILE_READ_WRITE
IpxProcess.cfg	547	FILE_READ_WRITE
L2tpProcess.cfg	162	FILE_READ_WRITE
MPIPPProcess.cfg	35	FILE_READ_WRITE
Ntp.cfg	49	FILE_READ_WRITE
PilgrimStrings.ind	165396	FILE_READ_ONLY
PilgrimStrings.str	204007	FILE_READ_ONLY
PingProcess.cfg	19	FILE_READ_WRITE
PppProcess.cfg	6	FILE_READ_WRITE



Atmarp.cfg	0	FILE_READ_WRITE
CLI.cfg	41	FILE_READ_WRITE
PptpProcess.cfg	77	FILE_READ_WRITE
QuickSetup.cfg	846	FILE_READ_WRITE
RemotePingProcess.cfg	21	FILE_READ_WRITE
Robo.stats	422	FILE_READ_WRITE
RoboExecNMProcess.cfg	1368	FILE_READ_WRITE
RoboString.ind	10612	FILE_READ_ONLY
RoboString.str	8621	FILE_READ_ONLY
SlipProcess.cfg	20	FILE_READ_WRITE
SnmpProcess.cfg	16	FILE_READ_WRITE
TcpProcess.cfg	20	FILE_READ_WRITE
TermProt.cfg	44	FILE_READ_WRITE
TftpProcess.cfg	26	FILE_READ_WRITE
TracerouteProcess.cfg	20	FILE_READ_WRITE
app.ld	1030860	FILE_READ_ONLY
log-file.local	3924	FILE_READ_WRITE
old-log-file.local	3924	FILE_READ_WRITE
user_settings.cfg	1971	FILE_READ_WRITE
Total Sectors	Allocated sectors	Deleted Sectors
7168	1649	128
		Free Sectors
		5391
		MinimumFree Sectors
		1075

list filters

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

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

FILTERS		
Filter Name	Status	Protocols
easyfilter.fil	NORMAL	IP IP-RIP
testfilter.fil	VERIFY FAILED	

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 ATSO=0. You can modify existing initialization scripts using the **set init_script** command.

list interfaces

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

- **Interface Name** - LAN interface name: **eth:1**, **eth:2**, or ATM interfaces such as **ds3:1**, **atmaal:1** and **atmcell:1**
- **Oper Status** - current operating status of the interface; **Up** or **Down**. For modem interfaces, Oper Status will be Down only if the modem is disabled.
- **Admin Status** - permanently configured status of the interface, **Up** or **Down**.

Interface Name	Oper Status	Admin Status
eth:1	Up	Up
eth:2	Down	Up
slot:3/mod:1	Up	Up
slot:3/mod:2	Up	Up
slot:3/mod:3	Up	Up
slot:3/mod:4	Up	Up
internal	Up	Up
loopback	Up	Up
ds3:1	Up	UP
ds3:2	Down	UP
atmaal:1	Up	Up
atmaal:2	Down	Up
atmcell:1	Up	Up
atmcell:2	Down	Up

list ip addresses

Displays the IP address for each active IP network. It lists:

- **address** - IP address of the interface
- **Bcast Algo** - Algorithm used to determine which address to broadcast representing the entire network. Choices are:
 - **1** - the IETF standard: *nnn.nnn.nnn.255* (**default**)
 - **0** - the BSD standard: *nnn.nnn.nnn.000*
- **Reassembly Max Size** - maximum allowable size of packet that can be reassembled from a fragmented packet
- **Interface** - interface this IP address uses to connect to the system. Choices: **internal**, **loopback**, **eth:1**, **eth:2**

IP addressES	Bcast Algo	Reassembly Max Size	Interface
address			
2.2.2.2/A	1	3464	internal
127.0.0.1/A	1	3464	loopback
123.145.134.140/22	1	3464	eth:1

list ip arp

Displays the contents of the ARP cache. It lists:

- **IP address** - network address for this entry

- **Phys address** - MAC address the IP address maps to
- **Type** - Ethernet interface type: **Dynamic**
- **IfName** - LAN interface name: **eth:1** or **eth:2**

IP address	Phys address	Type	IfName
134.134.155.156	02:e0:48:00:e3:eb	Dynamic	eth:1
134.134.155.254	00:c0:13:45:ac:e7	Dynamic	eth:1
134.122.135.119	08:00:20:77:8b:e4	Dynamic	eth:1
134.122.145.143	00:21:ae:f5:05:10	Dynamic	eth:1

list ip defaultroute

Displays default gateway IP routers, which act as default routes for IP packets destined for remote hosts unknown to the HiPer ARC. All unspecified routes are automatically sent to this gateway. A default route gateway specified with a higher metric acts as the *primary* default route gateway and a second default route gateway with a lower metric acts as the *secondary* default route gateway. It lists:

- **address** - IP address of the default route
- **Mask** - subnet mask of the default route
- **Gateway** - IP address of the gateway router
- **Metric** - hop count to the gateway
- **State** - status of the default route

Configured default routes

Address	Mask	Gateway	Metric	State
112.23.44.34	255.255.255.252	112.23.45.34	3	State
112.23.44.34	255.255.255.252	112.23.45.32	4	State

list ip igmp

Displays configured IGMP *interfaces*, their associated *multicast addresses* and IGMP *status*. The command lists:

- **Interface** - The Ethernet (**eth:1**, **eth:2**) or modem interface (**slot:x/mod:y**) the IGMP multicast address is mapped to.
- **Multicast address** - An IP address assigned from the standard range of recognized addresses identifying an IGMP group. Range: **224.0.0.0 -239.255.255.255**
- **Status** - Description of how the specified multicast address joined the group. Status types may be single or combined. The types:
 - **Self** - Multicast address group joined by HiPer ARC
 - **Learned** - Multicast address group discovered by HiPer ARC (non-HiPer ARC join)
 - **Proxy** - Multicast address group connected to another interface on HiPer ARC

Interface	Multicast address	Status
eth:1	224.0.0.1	SELF
eth:2	224.0.0.2	LEARNED/PROXY
eth:1	224.0.0.3	SELF/PROXY
slot:3/mod:1	224.0.0.4	LEARNED/SELF/PROXY
eth:1	224.0.0.5	SELF/LEARNED

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 HiPer ARC interface
- **Neighbor** - IP address of the remote system
- **Status** - status of the connection: **Enabled** or **Disabled**
- **Interface** - *any valid interface*

address	Neighbor	Status	Interface
0.0.0.0/H	192.112.226.200	Enabled	slot:1/mod:3
134.134.155.156/22	0.0.0.000	Enabled	eth:1
192.112.226.201/C	0.0.0.0	Disabled	NONE
143.134.225.3	143.134.226.23	Enabled	internal

list ip networks

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

- **Name** - network designation
- **Prot** - IP protocol only
- **Int** - name of the LAN interface this network runs on: **atmnet:1**, **eth:1**, **eth:2**, **loopback**, **internal**, **slot:x/mod:y**
- **State** - state of the network; **Ena(bled)** Or **Dis(abled)**
- **Type** - *Static* (user-specified), *Auto* (default) or *Dynamic* network
- **Network address** - address of the IP network

Name	Prot	Int	State	Type	Network address
atm1483	IP	atmnet:1	ENA	STAT	204.249.180.46/C
ipnet	IP	eth:1	ENA	STAT	134.134.144.156/22
internal	IP	internal	ENA	STAT	2.2.2.2/A
n1-ip-l7	IP	slot:1/mod:3	ENA	DYN	192.112.226.200/H
IP-loopback	IP	loopback	ENA	AUTO	127.0.0.1/A

list ip pools

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

- **Name** - Pool designation
- **address** - Initial IP address and subnet mask of specified pool
- **Size** - Number of IP addresses you made available in the pool
- **InUse** - Number of IP addresses currently in use within the pool
- **State** - Conditional status of the IP pool: **Public** or **private**
- **Route** - Indicates whether pool is being broadcast as a single network (**aggregate**) or separate networks (**no_aggregate**).default: **no_aggregate**
- **Status** - Indicates current condition of pool. Choices:
 - **Active** - pool is available to assign user IP addresses from.

- **Remove** - pool size is being modified or the base address of the pool is being modified. No users can be assigned from the pool until operation is completed.
- **Remove_pending** - pool size is being modified and an active user is currently using a pool entry that needs to be removed. Users can be assigned from the pool in this state.
- **Delete_pending** - pool is being deleted but an active user has been assigned out of this pool and must wait until user hangs up to delete the pool. Users are not assigned from the pool in this state.

Name	Address	Size	InUse	State	Route	Status
ippool	166.165.165.155 /H	20	15	PUBLIC	NO_AGGREGATE	ACTIVE
ippool 2	166.165.165.135 /28	2	1	PUBLIC	AGGREGATE	ACTIVE

list ip routes

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

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

The command lists:

- **Destination** - IP address that the route resolves to
- **Prot** - *LOCAL*, *RIP* or *NetMgr* (routes you added)
- **NextHop** - address of the gateway used to reach this route
- **Metric** - number of router hops away this route is from the system
- **Interface** - interface that the route uses: **Loopback**, **eth:1**, **eth:2**, **slot:x/mod:y**

Destination	Prot	NextHop	Metric	Interface
0.0.0.0/0	NetMgr	146.165.166.254	1	eth:1
127.0.0.0/A	LOCAL	127.0.0.1	1	loopback
127.0.0.1/H	LOCAL	127.0.0.1	1	loopback
127.255.255.255/H	LOCAL	127.255.255.255	1	loopback
166.165.166.160/27	NetMgr	166.166.166.181	1	eth:1
166.166.166.180/H	LOCAL	166.166.166.180	1	eth:1
255.255.255.255/H	LOCAL	255.255.255.255	1	eth:1
140.179.0.0/B	RIP	192.112.226.254	6	eth:1
154.020.0.0/B	RIP	192.112.226.253	2	eth:2
145.033.234.232//28	LOCAL	145.033.235.057	1	slot:3/mod:4

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 address** - network address of this route
- **Prot(ocol)** - protocol used to find this route. Choices: **LOCAL, RIP, STATIC, NLSP, OTHER**
- **NextHopNIC** - network address of the next router (the next hop to the destination), the MAC address for the local IPX nodes (on the LAN), or the **ATM PVC**
- **Gateway** - address of the gateway to this network
- **Metric** - number 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.

IPX ROUTES

Network address	Prot	NextHopNIC	Gateway	Metric	Ticks
010000	RIP	ATM PVC	000011	2	2
000010	STATIC	00:08:00:2b:14:95	000010	1	1
000011	STATIC	ATM PVC	000011	1	1
000013	STATIC	ATM PVC	000011	1	2
001005	STATIC	11:11:11:11:11:11	000010	1	1

IPX STATIC ROUTES

Network address	NextHopNIC	Gateway	Metric	Ticks
000010	00:08:00:2b:14:95	000011	1	1
000011	ATM PVC	000010	1	1
000013	ATM PVC	000011	1	2
001005	11:11:11:11:11:11	000011	1	1

list ipx services

Displays IPX pool addresses previously defined with the **add ipx services** command. 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. Choices: **SAP, LOCAL, NLSP, STATIC, OTHER**
- **Metric** - number of hops through routers to reach this service

IPX SERVICES

Name	NetNum	Node	Socket	Type	Prot	Metric
0060B078F32F83CRNPI78F32F	161	00:60:b0:78:f3:2f	400c	30c	SAP	2
hiawatha	165	00:c0:4f:f5:bd:b6	4010	640	SAP	2

list ipx static routes

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

- **Network address(ess)** - network address requiring this route
- **NextHopNIC** - network address of the next router in the routing path
- **Gateway** - address of the host you defined as the gateway
- **Metric** - number of routers a packet must pass through to get to gateway
- **Ticks** - delay, in hops, to reach the route's destination

IPX STATIC ROUTE

Network address	NextHopNIC	Gateway	Metric	Ticks
161	00:00:00:01:00:23	161	1	1
01010101	00:00:00:01:00:23	01010101	1	1

list l2tp lns

Displays settings of all L2TP network servers (LNS) configured with the **add l2tp lns** command. It lists:

- **Index** - Number corresponding to particular L2TP network server in the Local L2TP LNS table.
- **Address** - address of particular L2TP network server in the table.

L2TP LOCAL LNS LIST

Index	address
1	134.234.123.43
2	134.234.123.45

list l2tp tunnels

Displays settings on the L2TP network server (LNS) for all configured L2TP tunnels. See the **list connections** command for DLL settings on the L2TP area concentrator (LAC).

- **Tun(nel) ID** - designation of the L2TP tunnel
- **Status** - state of the tunnel. Types: *NO STATE, ALLOCATED, CONNECTING, STARTING SESSION, ESTABLISHED, STOPPING SESSION, DISCONNECTING, LOST, IDLE TIMEOUT*
- **IP address** - IP address of the remote tunnel endpoint to which it is connected. Depending on the RAS executing the command, if looking at the LNS, this value is the LAC address.

L2TP TUNNELS

TunID	Status	IP address
1	ESTABLISHED	149.112.214.102

list l2tp session tunnel <number>

Displays information on all configured L2TP tunnel sessions.

- **Tun(nel) ID** - designation of the L2TP pipe
- **Ses(sion) ID** - designation of the L2TP session
- **Status** - status of the tunnel session. Types: *NO STATE, ALLOCATED, WAITING, CALLING, OFFERING, ANSWERING, CONNECTED, DISCONNECTING LOCAL, DISCONNECTING REMOTE, LOST CONTROL TUNNEL*
- **User Name** - Designation of user active on this tunnel session .

L2TP SESSIONS

TunID	SesID	Status	UserName
-------	-------	--------	----------

L2TP SESSIONS

1	1	CONNECTED	larry
---	---	-----------	-------

list lan interfaces

Displays installed interfaces - Ethernet (eth:1, eth:2), 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:

- **Name** - LAN interface name: **eth:1** or **eth:2**
- **Oper Status** - current operating status of the interface; **Up** or **Down**
- **Admin Status** - permanently configured status of the interface, **Up** or **Down**

Interface Name	Oper Status	Admin Status
eth:1	Up	Up
eth:2	Down	Up

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 *ClearTCP* TCP port numbers assigned to that login host

Preference	Name	Rlogin Port	Telnet Port	ClearTcp Port	Host address
1	camel	513	23	0	153.21.234.18
2	castle	513	23	0	153.21.234.236
3	zephyr	513	23	0	153.21.234.155
5	dromedary	513	23	0	153.21.234.89
6	styx	513	23	0	153.21.234.142

list modem_groups

Displays modem groups that you previously defined using the **add modem_group** command, along with the number of ports in each group. This command also lists default modem groups for each slot and all ports (all). For example:

GROUP	Number of Interfaces
all	86
slot:10	4
slot:11	4
slot:12	24
slot:13	24
slot:2	4
slot:3	4
slot:4	4
slot:5	4
slot:6	4
slot:7	4
slot:8	4



GROUP	Number of Interfaces
slot:9	4
dialout	4
wan	4
callback	4

list mpip bundles

Displays bundle owners and users for the Multilink PPP links registered by MPIP clients. This command displays data only when HiPer ARC is acting as an MPIP server and when MPIP calls are up for a machine acting as a client. For example:

MPIP Bundles				
Bundle Owner	EndPoint Value	Discriminator Type	No. Links	User Name
149.112.214.140	61626364656600000000	1	3	john
149.112.214.142	78787879797900000000	1	2	larry
149.112.214.142	73616E696C6B00000000	1	1	jack

list mpip clients

Displays IP addresses and client types (HiPer ARC or NETServer) of all Multilink PPP clients you configured using the **add mpip client** command. For example:

Client	Type
149.112.214.140	NETSERVER
149.112.214.142	HIPER
149.112.221.169	HIPER
149.112.222.130	HIPER

list mpip links

Displays all Multilink PPP links registered by MPIP clients. The command displays the following:

- **Bundle Owner** - IP address of the first client receiving any bundle on this link (where the link terminates)
- **Link Owner** - IP address of the virtual client receiving a bundle on this link
- **Link ID** - entry in the table for each configured link
- **User Name** - name of the user transmitting the bundle

For example:

MPIP Links			
Bundle Owner	Link Owner	Link ID	User Name
149.112.214.140	149.112.214.140	11	john
149.112.214.140	149.112.214.140	12	john
149.112.214.140	149.112.214.142	13	john
149.112.214.142	149.112.214.142	14	larry
149.112.214.142	149.112.214.140	13	larry
149.112.214.142	149.112.214.142	15	jack

list mpip locallinks

Displays MPIP client information, including all MPIP users and their respective bundle owners - the remote access server where MPIP links are terminated. The command displays an *index* entry in the table for each

configured MPIP link, that link's *bundle owner* (first client receiving any bundle on this link), and *user* (name of the user sending the bundle). For example:

Local MPIP Links		
Index	Bundle Owner	User
1	149.112.223.150	abc1
2	149.112.223.150	abc1
3	149.112.223.150	abc1
4	149.112.223.151	pqr1
5	149.112.223.151	pqr1

list mpip servers

Displays all Multilink PPP servers you configured using the **add mpip server** command. For example:

MPIP Servers		
IP address	UDP Port	Priority
149.112.214.140	5912	1

list network services

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

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

Name	Server Type	Socket	Close	Admin Status
1	TELNETD	6000	FALSE	Enabled
DATA: service_type=dialout,modem_group="all"				
2	TELNETD	61	FALSE	Enabled
DATA: modem_group="all",auth=off,service_type=dialout				
tftpd	TFTPD	69	FALSE	Enabled
DATA:				
telnetd	TELNETD	23	FALSE	Enabled
DATA:				
cleartcp	ClearTCPD	6688	FALSE	Enabled
DATA:				

list networks

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

- **Name** - designation of the network that you defined with the **add network** command
- **Prot** - protocol of the network: **IP** or **IPX**
- **Int** - Ethernet interface the network is running on: **eth:1**, **eth:2**, **loopback**, **internal**, **slot:x/mod:y**

- **State** - Condition of network: **ENA** (enabled), **ENA*** (enabling), **DIS** (disabled), **DIS*** (disabling), **INIT** (initialized), **INV** (invalid)
- **Type** - *STAT* (static), *DYN* (dynamic) or *AUTO* (default) network
- **Network address** - address of the IP network

Name	Prot	Int	State	Type	Network address
ipnet	IP	eth:1	ENA	STAT	132.122.57.1240/22
IP-loopback	IP	loopback	ENA	AUTO	127.0.0.1/A
internal	IP	internal	ENA	STAT	2.2.2.2/A
n1-ip-l7	IP	slot:1/mod:3	ENA	DYN	192.112.226.200/H

list pbus datagrams

Displays statistics associated with packet bus datagrams (currently zero since the datalink driver doesn't support UI frames). It also shows the hardware setting for the pbus clock. When the Clock Statistic is *master*, HiPer ARC provides clocking. When the Clock Statistic is *slave*, another card provides the clock. When the Error Statistic displays *1*, the pbus is operating normally.



In systems with clock backplanes, no master is designated. All new backplanes are clocked.

SentPkt	RcvPkt	TimOut	ErrStat	ClockStat
0	0	0	1	Master

list pbus sessions

Displays active pbus sessions based on interface name (one per modem connection) and includes the number of packets sent (*Spkts*) or received (*Rpkts*) and *packet size*. Session is the modem driver identifier.

Interface	Slot	Channel	Session	Rpkts	Spkts	PktSize
slot:1/mod:1	1	1	512	0	0	4096
slot:1/mod:2	1	2	513	0	0	4096
slot:1/mod:3	1	3	514	0	0	4096
slot:1/mod:4	1	4	515	0	0	4096

list pbus traps

Displays trap status results of each active pbus connection (transmitted to the Network Management Card). Traps are: *Session Active*, *Session Inactive*, *Pbus Congestion*, *Pbus Session Lost*, and *Pbus Session Error*. When a parameter is enabled and these conditions occur, traps are sent to the NMC, when disabled, they are not sent to the NMC. See the **set pbus trap** command for more information.

Interface	SessAct	BusCong	SessLst	SessIna	SessErr
slot:1/mod:1	Enabled	Enabled	Enabled	Enabled	Enabled
slot:1/mod:2	Enabled	Enabled	Enabled	Enabled	Enabled
slot:1/mod:3	Enabled	Enabled	Enabled	Enabled	Enabled
slot:1/mod:4	Enabled	Enabled	Enabled	Enabled	Enabled

list ping service_loss_systems

Displays information from systems pinged as specified by the **add ping service_loss_system** command. It lists:

- **Name** - IP address or name of the system to ping.
- **Freq(ency)** - number of seconds between ping requests

- **Time(out)** - Number of seconds a ping request can be open before it fails (is labeled a miss).
- **Miss(es)** - number of allowable misses before this system is unreachable.
- **Status** - whether the particular server is pinged or not. **Enabled** or **Disabled**

Name	Freq	Time	Miss	Status
244.245.143.143	30	2	1	Enabled
ds.internic.net	30	2	1	Enabled
news.ultranet.com	30	2	1	Enabled

list ping systems

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

- **Row** - Row number within the Remote Ping Table.
- **Destination** - Host name or IP address of the target node being tested.
- **Status** - Present state of this row. Possible states include:
 - **Complete** - Requested number of pings resolved
 - **Active** - Ping requests in progress
 - **Bad address** - Resolved IP address is illegal
 - **Waiting DNS** - Awaiting DNS resolution
 - **Not Active** - Specified ping row not active
 - **DNS Failed** - Destination address could not be resolved
 - **Alloc Failed** - System failed to allocate resources
- **Count** - Number of pings to be transmitted.
- **Interval** - Number of seconds between ping requests. Default: **1 second**.
- **Size** - Size of data to be transmitted, in bytes. Default: **64 bytes**.
- **TTL** - Ping message time-to-live period. Default: **20 seconds**.

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

list ppp

Displays PPP bundles and links. When multiple physical links are combined to run multilink PPP (RFC1717), the group of physical links is called a bundle. 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 the **set network user ppp** command.

- **Bundle Index** - index number of the physical interface in the bundle
- **Link Index** - index number in the list of links
- **Oper Status** - current operational status of the link. **Opened** or **Not Opened**

- **Interface Name** - slot and modem designation of interface belonging to this bundle/link

Bundle Index	Link Index	Oper Status	Interface Name
4		Opened	
	5	Opened	slot:3/mod:1

list ptp pnss

Displays settings of all PPTP network servers configured with the **add ptp pns** command. It lists:

- **Index** - Number corresponding to particular PPTP Network Server in the LOCAL PPTP PNS Table.
- **address** - address of particular PPTP Network Server in the table.

PPTP LOCAL PNS LIST	
Index	Address
1	134.234.123.43
2	134.234.123.45

list ptp tunnel <number> sessions

Displays information on all current PPTP tunnel sessions.

- **Tun(nel) ID** - designation of the PPTP pipe
- **Ses(sion) ID** - designation of the PPTP session
- **Status** - status of the tunnel session. Types: *NO STATE, ALLOCATED, WAITING, CALLING, OFFERING, ANSWERING, CONNECTED, DISCONNECTING LOCAL, DISCONNECTING REMOTE, LOST CONTROL TUNNEL*
- **User Name** - Designation of user active on this tunnel session .

PPTP SESSIONS			
TunID	SesID	Status	UserName
1	1	CONNECTED	larry

list ptp tunnels

Displays settings for all current PPTP tunnels.

- **Tun(nel) ID** - designation of the PPTP tunnel
- **Status** - state of the tunnel. Types: *NO STATE, ALLOCATED, CONNECTING, STARTING SESSION, ESTABLISHED, STOPPING SESSION, DISCONNECTING, LOST, IDLE TIMEOUT*
- **IP address** - IP address of the remote tunnel endpoint to which it is connected. Depending on the RAS executing the command, if looking at the PNS, this value is the LAC address.

PPTP TUNNELS		
TunID	Status	IP address
1	ESTABLISHED	149.112.214.102

list processes

Displays all processes running on the system. It lists:

- **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*

See example below. Note that some processes are not supported in this version of HiPer ARC.

PROCESSES

Index	Name	Type	Status
2001	NameManager	System	Inactive
12001	Console	System	Inactive
22001	FileManager	System	Inactive
32001	Configurator	Application	Inactive
42001	Main	Application	Active
52001	MIB Registrar	Application	Inactive
62001	Config File Manager	Application	Inactive
72001	RoboExec NetManagement	Application	Active
82001	Event Handler	Application	Inactive
92001	System Bus	Driver	Inactive
a2001	NMB Driver	Driver	Inactive
b2001	Device Discovery	Application	Inactive
c2001	Console	Driver	Inactive
d2001	Loopback Driver	Driver	Inactive
e2001	Ethernet	Driver	Inactive
f2001	IP Forwarder	Forwarder	Inactive
102001	UDP Process	Application	Inactive
112001	TCP Process	Application	Inactive
122001	Telnet	Application	Inactive
132001	SLIP Process	Application	Inactive
142001	TFTP Process 1421	Application	Inactive
152001	IP Spoofing	Application	Inactive
162001	Ping Service Checker	Application	Inactive
172001	User Manager	Application	Inactive
172001	RADIUS User Manager	Application	Inactive
182001	SNMP Agent	Application	Inactive
192001	Point to Point Protocol	Application	Inactive
1a2001	Domain Name System	Application	Inactive
1b2001	Filter Manager Process	Application	Inactive
1c2001	NTP-Network Time Protocol	Application	Inactive
1d2001	NMB Agent	Application	Inactive
1e2001	BSP Management Process	Application	Inactive
1f2001	Remote Ping Process	Application	Inactive
202001	File System Compaction Process	Application	Inactive
21200	IPX/IP Dial-out Process	Application	Inactive
22200	Traceroute Process	Application	Inactive
232001	Tunnel Dispatcher	Application	Inactive
242001	NPPTP	Application	Inactive
252001	L2TP Process	Forwarder	Inactive
262001	VTP Process	Application	Inactive
272001	MPIP Process	Application	Inactive
282001	Port Tapping Process	Application	Inactive
292001	Call InitProcess	Application	Inactive
2a2001	IPX	Forwarder	Inactive
2b2001	IPX RIP	Application	Inactive
2c2001	SAP	Application	Inactive

PROCESSES

Index	Name	Type	Status
2d2001	IPX DIAG	Application	Inactive
2e2001	IPX NETBIOS	Application	Inactive
2f2001	IPX SPOOF	Application	Inactive
302001	IPX WAN	Application	Inactive
312001	IP Routing Instance	Application	Inactive
322001	CLI	Application	Inactive
332001	GWC Modem Driver	Driver	Inactive
342001	PPP Monitor 2822	Application	Inactive
35200a	CLI 34200a	Application	Inactive

list rtab preferred

Displays Routing Table information. It lists:

- **Destination** - IP network destination address
- **Protocol** - The routing mechanism through which the specified route was discovered. Choices:
 - **RIP** - any route discovered by RIP
 - **REMOTE** - user-specified remote or IP Pool aggregated remote static route
 - **LOCAL** - user-specified local route
- **Age** - Time since route was created in seconds
- **NextHop** - IP address of the next hop of the specified route
- **Metric** - Number of hops between HiPer ARC and its destination
- **Interface** -HiPer ARC Ethernet and modem interfaces the specified routes are mapped to

ROUTING TABLE PREFERRED ROUTES

Destination	Prot	Age	NextHop	Metric	Interface
0.0.0.0/0	REMOTE	147806	151.117.120.123	1	eth:1
151.117.120.74/H	LOCAL	147806	151.117.120.74	0	eth:1
151.117.120.6/H	LOCAL	147806	151.117.120.65	0	eth:1
151.117.110.4/H	LOCAL	147806	151.117.110.4	0	eth:1
151.117.110.24/H	LOCAL	147806	151.117.110.24	0	eth:1
151.117.110.23/H	IP	147806	151.117.110.23	0	eth:1

list sessions

Displays information regarding current HiPer ARC connections. It lists:

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

SESSIONS

Name	Conn_Typ	Prot_Typ
new	LAN	UNKNOWN
local	WAN	PPP
bottom	WAN	PPP
larry	LAN	TELNET

list snmp communities

Displays the SNMP communities defined using the **add snmp community** command.

- **Community Name** - community designation for the IP address
- **IP Address** - IP address of a member of the community
- **Access** - The allowed access for this community. Choices:
 - **Read/Only** - read-only access to user-level objects allowed
 - **Read/Write** - read and write access to user-level objects and write access to writeable user-level objects allowed.
 - **Administrator** - read access to all objects and write access to all writeable objects allowed
- **Community Pool** - Name for a pool of IP addresses comprising this SNMP community
- **Validate address** - Method selected to determine access to this community: *use_address* uses the specified IP address to validate access, *use_pool* uses the list of IP addresses specified in the *community_pool* value to validate access.

SNMP COMMUNITIES

Community Name	IP Address	Access	Community Pool	Validate address
larry	149.122.145.23	Administrator		use_address
nancy	149.122.145.24	Read/Write	Boston	use_pool
gina	149.122.145.26	Read/Only		use_address

list snmp community_pools

Displays all entries in the SNMP Community address Pool table. See **add snmp community_pool** command for more information. It lists:

COMMUNITY POOLS

Name	Number of addresses
westboro	54
shrewsbury	43
worcester	149

list snmp trap_communities

Displays SNMP trap communities defined using the **add snmp trap_community** command. It lists:

- **Community Name IP Address** - trap community designation for the associated system
- **Community Pool** - name of the trap community pool. If the trap community pool does not exist and the *validate_address* parameter is configured to use the trap community pool, the name of the trap community pool displayed is preceded by an asterisk.
- **Validate Address** - Method selected to determine access to this trap community: *use_address* uses a specified IP address to validate access, *use_pool* uses a list of IP addresses to validate access.

SNMP TRAP COMMUNITIES

Community Name		
IP Address	Community Pool	Validate Address
Kensington		useAddress
Kerby		usePool
Kenwood		useAddress
1.1.1.3		

list snmp trap_community_pools

Displays all SNMP trap community pools in the SNMP Trap Community Address Pool defined using the **add snmp trap_community_pool** command. It lists:

- **Name** - designation of the trap community pool
- **Number of Addresses** - Sum of IP addresses associated with the specified trap community pool

TRAP COMMUNITY POOLS	
Name	Number of Addresses
Joisy	5

list switched interfaces

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

- **Interface Name** - interface name: (e.g.) *slot:3/mod:1*
- **Oper(ating) Status** - current operating state of the interface; **Up** or **Down**. Oper Status is Up only if modem is connected.
- **Admin(istrative) Status** - state of the interface configured by the administrator: **Up** or **Down**.

INTERFACES		
Interface Name	Oper Status	Admin Status
slot:3/mod:1	Up	Up
slot:3/mod:2	Up	Up
slot:3/mod:3	Up	Up
slot:3/mod:4	Up	Up

list syslogs

Displays IP addresses which get SYSLOG entries from the Syslog Table. 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: (e.g.) *UNUSUAL*
- **M(e)s(sa)g(e)** - current number of messages sent since system bootup
- **Count** - number of event messages sent to this SYSLOG sink
- **Facility** - SYSLOG sink node facility to which the SYSLOG message is sent. Choices are: **LOG_AUTH**, **LOG_LOCAL0**, **LOG_LOCAL1**, **LOG_LOCAL2**, **LOG_LOCAL3**, **LOG_LOCAL4**, **LOG_LOCAL5**, **LOG_LOCAL6**, AND **LOG_LOCAL7**

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

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

list tap

Displays all current tap settings specified with the **add tap interface**, **next** or **user** commands. The command parameters are:

- **Id** - Tab entry in the table
- **Type** - Tap type: **USER**, **SESSION**, **INT(ER)F(ACE)**
- **Perm(anent)** - Whether tap is on continuously or not: **Yes** or **No**
- **Interface** - Modem where tap is being conducted
- **User** - Name of user whose output is being tapped
- **Out(put)** - Location where output is being directed: **SCR(EE)N** or **SYSL(OG)**
- **F(or)m(a)t** - Text style of output: **HEX(ADECIMAL)**, **ASC(II)**, or **CL(EA)R**
- **Facility** - Site where tap output is stored. Default: **LOG_AUTH**
- **Lev(e)l** - Syslog level of tap output: **CRIT(ICAL)**, **UNUS(UAL)**, **COMM(ON)**, **VERB(OSE)** - *Default*
- **Address** - SYSLOG host IP address

The command lists:

Id	Type	Perm	Interface	User	Out	Fmt	Facility	Levl	Address
1	USER	No		larry	SCRN	ASC	LOG_AUTH	VERB	
2	USER	Yes	slot:3/mod:1	larry	SYSL	HEX	LOG_AUTH	CLR	
3	INTF	No	slot:3/mod:1		SCRN	CLR	LOG-LOCAL1	CRIT	
4	NEXT	No			SCRN	ASC	LOG-LOCAL2	UNUS	

list tcp connections

Displays information about all TCP (TELNET, RLOGIN, etc.) connections including those set by the user.

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

TCP CONNECTIONS				
Local address	Local Port	Remote Address	Remote Port	Status
0.0.0.000	23	0.0.0.000	o	Listen
0.0.0.000	5000	0.0.0.000	o	Listen
0.0.0.000	6000	0.0.0.000	o	Listen
0.0.0.000	6668	0.0.0.000	o	Listen
157.132.148.180	23	157.132.148.183	1047	TimeWait

**TCP CONNECTIONS**

157.132.148.180	23	157.132.148.183	1047	Established
145.134.121.199	23	143.134.122.189	3220	SynReceived

list telnet client

Displays a list of TELNET client you configured using the **add telnet client** command. when access is globally enabled with the **enable telnet client_access** command - capable of accessing HiPer ARC. By specifying a netmask, you can add network and subnetwork addresses. If no netmask is specified, the host netmasks value is assumed. An IP address of 0.0.0.0 allows universal entry to HiPer ARC by TELNET users. See the **delete telnet client** command for more information. Also, issue the **list telnet client** command for a list of configured users. Default: **Disabled**

TELNET CLIENT ADDRESSES

IP Address	Netmask
148.132.112.23	255.255.255.0
148.132.112.45	255.255.255.255

list tftp clients

Displays IP addresses of all users allowed to use the Trivial File Transfer Protocol (TFTP) to connect to the system. Use the **add network service** command to add TFTP support to the system, the **add tftp client** to authorize users to connect and the **add tftp request** command to initiate TFTP service. For example:

TFTP CLIENT addressES

```
0.0.0.0
157.122.138.134
234.122.156.134
```

list tftp requests

Displays statistics of all current requests for servic in the TFTP Client Request Table. It lists:

- **Filename** - Name of file to be requested from or sent to the TFTP server.
- **Server** - Name or IP address of the TFTP server
- **Action** - Type of request send to the TFTP server. **Put** or **Get**
- **Status** - State of each current TFTP request in the table:
 - **Normal** - Request is in the table or has been successfully completed
 - **Getting** - Initial state: TFTP server is receiving a file
 - **Putting** - Initial state: TFTP server is sending a file
 - **Error** - Request has finished unsuccessfully and will generate an error message

TFTP REQUEST TABLE

Filename	Server	Action	Status
filter.in	Scylla	PUT	NORMAL
hiper	Styx	GET	GETTING

list traceroute

Displays the current rows in the main traceroute table when entered from an SNMP station or via a command file. Rows entered from the CLI are automatically *deleted* upon traceroute completion but rows entered from

an SNMP station will persist for 30 minutes. See **traceroute**, **delete traceroute**, **set traceroute maximum_rows** and **show traceroute** commands for more information.

- **Row** - Rows currently active in Traceroute Table
- **Destination** - host name or IP address of traceroute target
- **Hop Count** - Number of hops traceroute has traveled to reach destination
- **State** - Status of traceroute process associated with this row

When using SNMP or a command file only to perform a traceroute list, the following states may be reported.



Traceroute-generated packets received by HiPer ARC will not increment the ICMP error counters Time Exceeded and Destination Unreachable. See attributes below.

- **Active** - specified IP address (host) is resolve
- **Not Active** - before this row is activated
- **Waiting DNS** - awaiting DNS resolution
- **DNS Failed** - destination address could not be resolved due to timeout or other reason
- **Bad address** - resolved IP address is illegal
- **Hop Timeout** - timeout occurred
- **Hops Exceeded** - maximum number of hops exceeded
- **Dest Unreachable** - a route to the host could not be found
- **Tracing** - performing traceroute
- **Completed** - traceroute completed successfully
- **Resource Failure** - not enough resources to complete the command

Row	Destination	Hop Count	State
1	132.143.24.70	12	Active
3	mayflower	30	HOPS EXCEEDED
4	moth	30	HOPS EXCEEDED

list traceroute row <number> hops

Displays counters for specified traceroutes. It lists:

- **Row** - entry number in the Traceroute Table. Range: **1-255**
- **Hop** - number of hops taken to reach destination
- **IP address** - IP address of destination
- **Round Trip Time** - period to reach destination and return to HiPer ARC

ROW	HOP	IP address	ROUND TRIP TIME
1	1	11.0.0.20	100
1	2	10.0.0.2	100

list tunnel connections

Displays tunnel information for all tunnels configured with the **add tunnel user** command.

IfName	User Name	Type	Start Date	Start Time
--------	-----------	------	------------	------------

tun:1	larry	L2TP	19-SEP-2041	03:39:58
tun:10	nancy	L2TP	19-SEP-2041	03:39:59
tun:100	gina	L2TP	19-SEP-2041	03:40:07
tun:101	tom	L2TP	19-SEP-2041	03:40:07
tun:102	craig	L2TP	19-SEP-2041	03:40:08

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.

UDP LISTENERS

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

list users

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

- **User Name** - user designation you specified using **add user** command
- **Login Service** - *TELNET*, *RLOGIN*, or *ClearTCP*
- **Network Service** - type of network service: **PPP** or **SLIP**. SLIP service not supported for LAN-to-LAN users.
- **Status** - link status: **ACTIVE** (in use), **INACTIVE** (not in use) or **DISABLED** (inactivated)
- **Type** - type of configured user: see the **add user** command for more information

USERS

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

Logout Command

logout

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

Monitor Commands

monitor ppp

Allows monitoring of realtime PPP activity. For best results, we recommend you use this program via TELNET. HiPer ARC offers three methods to evaluate PPP events:

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

If you want to monitor PPP events using this command, you must first issue a **show events** command as a managed user dialing in. **Monitor ppp** is limited to checking PPP data streams. It cannot monitor network traffic nor capture data and direct it to a SYSLOG host or your console as with the **tap** commands. The command performs the following types of monitoring:

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

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

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

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

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

When you issue the command, the menu displays the screen below.

```
HiPer>> monitor ppp
```

HiPer PPP Monitor

Select a letter for one of the following options:

- C) Monitor PPP Call Events.
- I) Monitor a specific interface.
- N) Monitor the next session that starts up.
- U) Monitor a specific user

**HiPer PPP Monitor****X) Exit the monitor.**

For each choice (shown in descending order), you'll see the following screens. Follow the prompts as directed.

Monitoring PPP Call events.**About to begin Tracing of PPP Call Events****Hit return/enter to start the trace.****Hit escape to go back to the monitor.****Monitor a specific interface****Enter the interface to monitor below:****Press Escape to return to the previous screen.****Press Enter/Return to enter the name.****Interface: []****Monitoring the next session to start up.****About to begin PPP Tracing of next session started.****Hit return/enter to start the trace.****Hit escape to go back to the monitor.****Monitor a specific user****Enter the user name to monitor below:****Press Escape to return to the previous screen.****Press Enter/Return to enter the name.****User Name: []****Monitoring Stop/Start**

When monitoring begins, a variety of information is displayed with some options available to you. When I is selected, as soon as data entry is validated the program will display the following message:

Interface: [slot:3/mod:1]**Monitoring interface slot:3/mod:1****About to begin PPP Tracing of interface slot:3/mod:1****Hit return/enter to start the trace.****Hit escape to go back to the monitor.**

See below for tracing output.

All output is paused until **ENTER** is pressed. If **ESC** is pressed, monitoring stops and the main menu is displayed again. When **ENTER** is pressed, the program will display:

Decode tracing started, press ESCAPE to stop; press X for hex tracing.

After a slight delay, the monitor will display output and the following message until **ESC** is pressed.

...Tracing the current/next session; ESCAPE to stop...

Once you press **ESC**, you have the option of pressing **ENTER** again to continue monitoring or **ESC** once again to terminate monitoring and return to the main menu.

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

Idle Timer

While monitoring is active (after **U** is pressed), and as long as no data is displayed, the program will show an idle message to verify it's active. Every minute the program will display the following:

....Tracing for user "larry"; Escape to stop...

When monitoring data is displayed, this message will not appear.

Decode and Hexadecimal Display

Interface, User and Next Session monitoring display two types of data: *decode and hexadecimal*. *Decode* - the default - displays packets without decompression in a textual, decoded output. *Hexadecimal* displays packets with decompression in hexadecimal and any ASCII equivalent as soon as they are received or just before transmission. Both modes can be switched on the fly.

An example of Decode mode output:

Decode tracing started, press ESCAPE to stop; press X for hex tracing.

Incoming PPP Data on interface: slot:3/mod:1

449d 45 00 00 28 1b 13 40 00 20 06 25 6a 92 73 7a b8 92 73 7a b4 ..

Incoming PPP Data on interface: slot:3/mod:1

9d53 45 00 00 28 1c 13 40 00 20 06 24 6a 92 73 7a b8 92 73 7a b4 ..

Incoming PPP Data on interface: slot:3/mod:1

9d53 45 00 00 28 1d 13 40 00 20 06 23 6a 92 73 7a b8 92 73 7a b4 ...

Incoming PPP Data on interface: slot:3/mod:1

9d53 45 00 00 28 1e 13 40 00 20 06 22 6a 92 73 7a b8 92 73 7a b4 ...

To switch from decode mode to hexadecimal mode, type: **H** or **X** (case is immaterial). See example below.

Outgoing PPP Data on interface: slot:1/mod:2

```
LCP      CFG_REQ  MRU          05 ea
          ASYNC_MAP 00 00 00 00
          AUTH_TYPE c2 23 05
          MAGIC_NUM df 0f 9a 55
          PROTO_COMP
          AC_COMP
          MPP_MRRU   05 ea
          MPP_ENDPTID 00
```

Incoming PPP Data on interface: slot:1/mod:2

```
LCP      CFG_REJ  MPP_MRRU   05 ea
          MPP_ENDPTID 00
          SEC DNS    00 00 00 00
```

Outgoing PPP Data on interface: slot:1/mod:2

```
IPCP     CFG_NAK  COMPR_TYPE  00 2d 0f 00
          NEW_ADDRS 95 70 d6 d0
          PRIM DNS   95 70 14 03
          SEC DNS    95 70 d5 01
```

Incoming PPP Data on interface: slot:1/mod:2

```
IPCP     CFG_REQ  COMPR_TYPE  00 2d 0f 00
          NEW_ADDRS 95 70 d6 d0
          PRIM DNS   95 70 14 03
          SEC DNS    95 70 d5 01
```

Outgoing PPP Data on interface: slot:1/mod:2

```
IPCP     CFG_ACK  COMPR_TYPE  00 2d 0f 00
          NEW_ADDRS 95 70 d6 d0
          PRIM DNS   95 70 14 03
          SEC DNS    95 70 d5 01
```

Outgoing PPP Data on interface: slot:1/mod:2

```
IPCP     CFG_REQ  COMPR_TYPE  00 2d 0f 00
          NEW_ADDRS 80 01 02 01
```

Incoming PPP Data on interface: slot:1/mod:2

```
IPCP     CFG_ACK  COMPR_TYPE  00 2d 0f 00
          NEW_ADDRS 80 01 02 01
```

Incoming PPP Data on interface: slot:1/mod:2

```
IP_DATA  45 00 00 60 34 02 00 00 20 11 64 da 95 70 d6 d0 95 70 ff ff ...
```

Incoming PPP Data on interface: slot:1/mod:2

```
IP_DATA  45 00 00 60 35 02 00 00 20 11 63 da 95 70 d6 d0 95 70 ff ff ...
```

To switch back to decode mode, type: **D**

Note: There may be a lag due to delayed output to the screen.

monitor radius

Allows monitoring of realtime RADIUS activity. This feature provides:

- **Monitoring all RADIUS packets** - Displays all RADIUS packets transmitted or received by HiPer ARC.
- **Monitoring all RADIUS authentication packets** - Displays all RADIUS authentication packets transmitted or received by HiPer ARC.
- **Monitoring all RADIUS accounting packets** - Displays all RADIUS accounting packets transmitted or received by HiPer ARC.
- **Monitoring a specific RADIUS user** - Displays any RADIUS sessions currently active for the specified user. As any new session begins for the user, monitoring will also begin.
- **Monitoring the next session that starts up** - Displays results for next RADIUS session created. This option is useful if a user is having difficulty connecting and it's unclear which interface the user will connect on because of his inclusion in a hunt group. As soon as the next incoming or outgoing RADIUS connection is established, monitoring will begin. There is no differentiation on the next session - the user selects to monitor the next session and will see the next session displayed regardless of interface or user name employed.
- **Monitoring all RADIUS packets sent to or received from a specific server** - Displays all traffic to and from a specified server.
- **Exiting the monitor** - Exits the program.
- **Decode and Hexadecimal Display** - All monitoring displays two types of data: *decode* or *hexadecimal*. *Decode*, (the default), displays packets without decompression in a textual, decoded output. *Hexadecimal* displays packets with decompression in hexadecimal and any ASCII equivalent as soon as they are received or just before transmission. Both modes can be switched on the fly.

When you issue the **monitor radius** command, the menu displays the screen shown below.

HiPer>> monitor radius

HiPer RADIUS Monitor

Select a letter for one of the following options:

- A) Monitor all RADIUS packets
- B) Monitor all RADIUS authentication packets
- C) Monitor all RADIUS accounting packets
- D) Monitor a specific user
- E) Monitor next session
- F) Monitor all packets to a specific server
- X) Exit the monitor.

For each menu choice (shown in descending order), you'll see the following screens. Options can be selected by typing the letters A, B, C, etc. Both lower case and upper case letters are accepted - all selection keys are case insensitive. Follow the prompts as directed:

Option A

Option A monitors all RADIUS packets transmitted and received by HiPer ARC. After selecting this option the following menu will display:

Tracing all RADIUS packets

Decode tracing started, press H and D to toggle between hex and decode mode

Press Escape to return to the previous screen.

Pressing the letters **H** or **D** toggles the *Decode* and *Hex Dump* modes. By default, RADIUS monitor starts in decode mode. At any time during tracing, pressing **H** will toggle it to Hex Dump mode; pressing **D** will toggle it back to Decode mode.

While in decode mode, pressing the **H** will display the following message:

```
Tracing changed to hex dumps; press D for decode tracing.
```

While in Hex dump mode, pressing the letter **D** will display the following message:

```
Tracing changed to decode; press H for hex tracing.
```

Pressing the **ESC** key at any time during tracing will place the monitor back in Main Menu.

Option B

Option B traces all *authentication* packets. It will not display the accounting packets. After selecting this option the following menu will display:

```
Tracing all RADIUS authentication packets
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

Option C

Option C traces all *accounting* packets can be traced. It will not display authentication packets. After selecting this option the following message will display:

```
Tracing all RADIUS accounting packets
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

Option D

Option D traces all packets of a specific *user*. After selecting this option the following menu will display:

```
Monitor a specific user
Enter the user name to monitor below:
Press Esc to return to the previous screen.
Press Enter/Return to enter the name.
User Name: [      ]
```

Enter the *user name* and press **ENTER**. The following message will display:

```
Monitoring a specific user
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

Option E

Option E monitors the *next session* only. After selecting this option the following message will display:

```
Tracing next RADIUS session
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

Option F

Option F monitors RADIUS packets to a specific RADIUS server. After selecting this option the following menu will display:

```
Monitor a specific server
Enter the server name to monitor below:
Press Escape to return to the previous screen.
Press Enter/Return to enter the name.
Server Name: [      ]
```

Now type the IP Address of the RADIUS server. Note that you need to enter the IP address of the RADIUS server and host name or any other alias or the host name will not suffice.

After typing the IP address of the RADIUS server, press the **ENTER** key. The following message will be display:

```
Monitoring all packets to a specific server
Decode tracing started, press H and D to toggle between hex and decode mode
Press Escape to return to the previous screen.
```

A sample Decode tracing output will look like this:

```
Source-IP  Src-Port  Destination-IP  Dest-Port Id  Packet-Type
124.32.45.65  2345      149.112.213.34  1645          1 Access-Accept

User-Name :                admin1
NAS-IP-Address :            149.112.223.137
NAS-Port :                  0
Interface-Index :           0
Chasis-Call-Slot :          1
Chasis-Call-Span :          1
Chasis-Call-Channel :       1
Service-Type :              6
Login-IP-Host :             149.112.223.3
Login-Service :             0
Login-TCP-Port :            23
Session-Timeout :           2000
Idle-Timeout :              699
State :                     GroupOne
Class :                     AccountOne
```

A sample Hex dump output will look like this:

```
Source-IP  Src-Port  Destination-IP  Dest-Port Id  Packet-Type
0.0.0.0     1646      149.112.213.34  2346          Accounting-Request

Outgoing PPP Data on interface: slot:3/mod:1  | p@ !  K n|
2d 10 17 19 48 65 78 20 74 72 61 63 69 6e 67 20 | joseph  a|
73 74 61 72 74 65 64 2c 20 70 72 65 73 73 20 45 | dmin1  p ( |
```


.....

```

53 43 41 50 45 20 74 6f 20 73 74 6f 70 3b 20 70      | , admin11)  |
72 65 73 73 20 44 20 66 6f 72 20 64 65 63 6f 64     |-          =  |
65 20 74 72 61 63 69 6e 67 2e 0d 0a                  |             |
                                                    | p .  z1    |

Source-IP   Src-Port   Destination-IP   Dest-Port Id   Packet-Type
149.112.213.34 2346    149.112.213.137 1646          Accounting-Request

2f 45 00 03 01 34 5d 00 00 ff 03 6a 46 92 73 7a      | /E  4]  jF sz|

```

Paused Commands

s or ENTER	Continues printing
q	Cancels rest of output
Ctrl c	Quits output

PING

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

Sends a ping (ICMP echo request) to a remote IP host. This tool to test connectivity can also be initiated from an SNMP station. The CLI can perform a ping with either verbose or background selected, but not both. *Verbose* causes the CLI to display information for each PING transmitted. *Background* causes the CLI to start the PING request and returns you to the prompt until results are ready.

Parameters	Description
<IP_name or address>	IP address in dotted notation, or host name of remote system.
background	When selected, pings are run in a background process on your screen. Can choose either background or verbose, not both. Default: NO
count	Number of pings requests to send. Default: 1 . Range: 1-1000
data	String value specifying data to be sent. Note: If data length is bigger than ping size, only the first ping size octets are used. If data length is zero, the server uses random data. If data length is smaller than ping size, the data pattern will be repeated as many times as necessary to fill up the transmission buffer. Range: 0-255 ASCII characters
interval	Period in seconds between successive ping requests. Note that the actual interval might be different for any given transmission, because the server will not send a new request before a previous request is completed (replied to or timed-out). Default: 1 second . Range: 1-65535 .

self_destroy_delay	<p>Period, with <i>background</i> selected, indicating the number of minutes a row in the Remote Ping Table is allowed to be inactive before it is erased by the server. A row is considered inactive any time the ping state is one of the following:</p> <ul style="list-style-type: none"> ▪ Not Active - row is not active ▪ DNS Failed - destination address could not be resolved ▪ Bad address - resolved IP address is illegal ▪ Completed - requested number of iterations is completed ▪ Alloc Failed - failed to allocate resources <p>Range: 0-65535 minutes. Default: 10 minutes.</p>
size	<p>Size of pinged packet. Note that the actual datagram is larger than this value by 42 octets because it includes:</p> <ul style="list-style-type: none"> ▪ MAC header (14 octets on Ethernet) ▪ IP header (20 octets) ▪ ICMP header (8 octets) <p>Default: 64 bytes. Range: 1-1400.</p>
timeout	<p>Period in seconds before determining that a transmission has not been replied to. Range: 1-60. Default: 20 seconds.</p>
verbose	<p>When set to <i>yes</i>, data is displayed progressively for each ping (if the count is more than one) Output includes each ping <i>request</i> and the elapsed <i>round trip time</i> in milliseconds, the ping <i>destination</i> and its <i>status</i>, the ping <i>count</i> you specified, any <i>timeouts</i> that may have occurred, and <i>maximum</i>, <i>minimum</i> and <i>average round trip times</i>. Can choose either <i>background</i> or <i>verbose</i>, not both. A round trip time of -1 indicates ping resolution failed. Default: NO</p>

A ping with the verbose parameter selected will display the following:

```

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

```

Quit Command

quit

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

Reboot Command

reboot

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

IMPORTANT: Switching between RADIUS and TACACS+ requires a reboot.

Reconfigure Command

reconfigure ip network <network name>
 address <IP_address>
 interface <eth:1 | eth:2>
 frame <ethernet_ii | snap | atm1483>

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

Rename Command

rename file <input_file> <output_file>

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

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

Reset Commands

Restores the following HiPer ARC settings to their default configuration.

reset

accounting counters
authentication counters
configuration
modem_group <name>
modems <slot:x/mod:[1-y;slot:x/mod:[1-y] ..

Parameters	Description
accounting counters	Restores accounting statistics to default values.
authentication counters	Restores authentication counters to default values.

configuration	Restores individual HiPer ARC configuration files (.CFG) from a bulk configuration file. The bulk configuration function reads all configuration files generated by HiPer ARC processes and concatenates them into a single compressed file which can then be uploaded by Total Control Manager. A bulk configuration file can be named using the set bulk_file command.
modem_group	Resets the specified modem group following changes to its configuration. This “hard” reset issues an ATZ! command, closing any active connections on that port.
modems	Resets the specified modems 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 modems slot:1/mod:[2-5],slot:2/mod:[7-9]

Resolve Command

resolve name <IP_host_name>

Returns an IP address for the specified host name by sending it to DNS for resolution. If the Domain Name 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 (add DNS host) or a DNS server entry (add DNS server) to resolve the name. This command is identical to the **host** command.

Network Name: cassatt.mass-usr.com
is resolved to address: 153.234.24.145

RLOGIN Command

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. Limit: 64 ASCII characters.
login_name	User name needed to login to the remote system.
TCP_port	TCP port number to create the connection to. Default: 513 . Maximum: 65535

Save Commands

Preserves changes you made to HiPer ARC configuration files.

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. When a save all is *in process*, the following message will display:

Saving ... SAVE ALL

When the save is *finished*, the following message will display:

Saving.....
SAVE ALL Complete.

save configuration

Saves individual configuration files (.CFG) to a bulk configuration file for uploading to HiPer ARC. You can name the bulk configuration file with the **set bulk_file** command. The **reset configuration** command breaks out individual configuration files from the bulk configuration file.

set Commands

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

set aaa_server <name>

address [IP_address]
enabled [yes | no]
encryption [off | on]
passthru [enabled | disabled]
port [1-65,535]
preference [1-10]
secret [string]
server_name [name]

Edits a TACACS+ server you created with the **add aaa_server** command.

Parameters	Description
<domain_name>	Domain designation of the AAA server. Example: joe@3com.com . Limit: 64 ASCII characters
address	IP address of the AAA server. Default: 0.0.0.0
enabled	Switch to turn AAA server on or off. Default: Yes
encryption	Enables/disables encryption of entire data packet. Default: On
passthru	When enabled, discontinues authentication attempts after third AAA server refusal but still allows users access to a domain. This value is used in conjunction with <i>direct request</i> . Default: DISABLED
port	Port number on the AAA server. TACACS+ standard port number: 49 . Range: 1-65,535
preference	Priority ranking of domains that specifies how servers are chosen. Highest preference - 1 , lowest - 10 . Range: 1-10
secret	Password shared by AAA server and HiPer ARC for encryption. Range: 0-15 ASCII characters. Field can be left blank or filled with null character: "" .
server_name	Familial name for the AAA server to be identified by DNS. Limit: 64 ASCII characters.

set accounting

attribute_style [netserver | standard]
log_unauthenticated_calls [true | false]
primary_destination_port <port_number>
primary_retransmissions <number>
primary_secret <"secret_string">
primary_server [IP_address or host_name]
secondary_destination_port <port_number>
secondary_retransmissions <number>
secondary_secret <"secret string">
secondary_server [IP_address or host_name]
source_port <port_number>
start_time [authentication | connection]
timeout [number_seconds]
vsa <enabled | disabled>]

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

IMPORTANT: The IP address/port number pair for accounting and backup servers must be unique or conflicts will occur. In other words, one accounting server designated as both first and second server must have unique port numbers designated for both servers. The same port number can be designated on servers with different IP addresses, though.

Parameters	Description
attribute_style	Sets Unauthenticated Time (RADIUS attribute #9012) value. If set to <i>netserver</i> , unauthenticated time is the interval from when the call arrived to when the Access-Accept message is received; to set to <i>standard</i> , unauthenticated time is the interval from when the call was connected to when the Access-Accept message is received.
log_unauthenticated_calls	Sets HiPer ARC to log calls which fail prior to authentication. Default: True
primary_destination_port	Destination port number of the primary RADIUS server. To ensure correct identification of server response packets, configure a unique IP address/port combination. Range: 0-65,535 . Default: 1813
primary_retransmissions	The interval HiPer ARC waits for a response from the primary server before retransmitting. Range: 0 - 2147483647 . Value of 0 causes infinite retransmissions. We recommend you <i>do not</i> set to 0.
primary_secret	Password of the Primary RADIUS server. Limit: 16 ASCII characters . Null string: ""
primary_server	Initial server to send the accounting information to. To ensure correct identification of server response packets, configure a unique IP address/port combination.
secondary_port	Port number of the Secondary RADIUS server. To ensure correct identification of server response packets, configure a unique IP address/port combination. Range: 0-65,535 . Default: 1813
secondary_retransmissions	The interval HiPer ARC waits for a response from the secondary server before retransmitting. Range: 0-2147483647 . Value of 0 causes infinite retransmissions.
secondary_secret	Password of the Secondary RADIUS server. Limit: 16 ASCII characters . Null string: ""
secondary_server	Second server to send the accounting information to. To ensure correct identification of server response packets, configure a unique IP address/port combination.
source_port	Port number of the source port of the primary accounting server. Default: 1813
start_time	When accounting begins. You may choose either: <ul style="list-style-type: none"> ▪ Authentication - session time in number of seconds after user name and password are entered. ▪ Connection - session time in number of seconds from modem pickup.
timeout	Interval between retransmissions. Default: 5 seconds. Range: 1-60 .
vsa	Enables/disables transmission of Vendor Specific Attributes to specified RADIUS servers.

set accounting_backup primary

```

first_destination_port <port>
first_secret <string>
first_server <IP_name or address>
second_destination_port <port>
second_secret <string>
second_server <IP_name or address>

```

Configures first and second backup servers for the primary accounting server group. HiPer ARC delivers accounting packets to primary *and* secondary server groups independently so that if all servers in one server group are not responsive, packets will be received successfully by the other group. Further redundancy is insured by having a first and second backup server per server group. If a server within a server group does not respond when a packet is transmitted to it, the packet is retransmitted to the next backup server in *round-robin* fashion.

IMPORTANT: The IP address/port number pair for accounting and backup servers must be unique or conflicts will occur. In other words, one accounting server designated as both first and second server must have unique

port numbers designated for both servers. The same port number can be designated on servers with different IP addresses, though.

Use the **enable** and **disable primary_accounting_server** and **secondary_accounting_server** commands to control this feature.

Parameters	Description
first_destination_port	RADIUS destination port number of the first backup server for the primary server group. Range: 0-65,535 . To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination. Default: 1813
first_secret	Password of the first backup server for the primary accounting server group. Limit: 16 ASCII characters . Null string: ""
first_server	Unique designation for initial backup server in the primary accounting server group. To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination.
second_destination_port	RADIUS destination port number of the second backup server for the primary accounting server group. Range: 0-65,535 . To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination. Default: 1813
second_secret	Password of the secondary RADIUS server for the primary accounting server group. Limit: 16 ASCII characters . Null string: ""
second_server	Unique designation for second backup server in the primary accounting server group. To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination.

set accounting_backup secondary

first_destination_port <port>
first_secret <string>
first_server <IP_name or address>
second_destination_port <port>
second_secret <string>
second_server <IP_name or address>

Configures first and second backup servers for the secondary accounting server group. HiPer ARC delivers accounting packets to primary *and* secondary server groups independently so that if all servers in one server group are not responsive, packets will be received successfully by the other group. Further redundancy is insured by having a first and second backup server per server group. If a server within a server group does not respond when a packet is transmitted to it, the packet is retransmitted to the next backup server in *round-robin* fashion.

IMPORTANT: The IP address/port number pair for accounting and backup servers must be unique or conflicts will occur. In other words, one accounting server designated as both first and second server must have unique port numbers designated for both servers. The same port number can be designated on servers with different IP addresses, though.

Use the **enable** and **disable primary_accounting_server** and **secondary_accounting_server** commands to control this feature.

Parameters	Description
first_destination_port	RADIUS destination port number of the first backup server for the secondary accounting server group. To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination. Range: 0-65,535 . Default: 1813
first_secret	Password of the first backup server for the secondary accounting server group. Limit: 16 ASCII characters . Null string: ""
first_server	Unique designation for initial backup server in the secondary accounting server group. To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination.

second_destination_port	RADIUS destination port number of the second backup server for the secondary accounting server group. To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination. Range: 0-65,535 . Default: 1813
second_secret	Password of the secondary RADIUS server for the secondary accounting server group. Limit: 16 ASCII characters . Null string: ""
second_server	Unique designation for second backup server in the secondary accounting server group. To ensure correct identification of server response packets, configure a <i>unique</i> IP address/port combination.

set acct_format <all | simple | sprint>

Configures different attribute formats for accounting. See *Appendix E: RADIUS and TACACS+ Systems* for detailed attributes information. The command lists:

- **all** - accounting attributes that HiPer ARC can provide
- **simple** - attributes format based on the Sprint CRD and CP Version 1.2 in conformance with TACACS+.
Default
- **sprint** - vendor-specific attributes format based on Sprint specifications.

set atm options <interface_name>

cable_length <short_haul | long_haul>

clock_source <network | internal>

frame_type <adm | plcp>

line_type <m23 | cbit | cchan | g832 | g751>

payload_scrambling <on | off>

Configures the ATM NIC's physical DS3 interfaces. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Parameters	Description
<interface_name>	Designation of the physical DS3 interface name. Span A corresponds to ds3:1 , Span B to ds3:2 ; e3:x , atmcell:x
cable_length	Allows the ATM NIC to be configured for long-haul (cable length between NIC and switch is between 0 and 450 feet) or short-haul (DSX-3, the cable length between the NIC and the switch is between 0 and 225 feet).
clock_source	Sets the timing source for the DS3 port. If the port is used as an independent port, the timing source should be configured for network (the source is the ATM switch). If the port is used to cascade additional NICs, the source should be configured for internal .
frame_type	Sets the method ATM cells are formatted: via ADM or the Physical Layer Convergence Protocol (PLCP). Default: ADM
line_type	Sets the DS3 line implementing this circuit.
payload_scrambling	Minimizes the number of zero gaps in the packet stream, improving bandwidth efficiency.

set atm_address network <network_name>

address [NSAP address]

Configures an NSAP ATM address to establish an RFC-1577 SVC when the ATM switch being connected is a public switch or a private switch not supporting Interim Link Interface Management (ILMI) address registration. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

Parameters	Description
<network_name>	Designation of the network for which the address is specified.



address	20-byte NSAP hexadecimal address (for the local network as configured on your switch) for use by SVCs on this network. E.g.: <i>ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff</i>
---------	--

set authentication

primary_destination_port <port number>
primary_secret <string>
primary_server <IP_address or name>
retransmissions <count>
secondary_destination_port <port number>
secondary_secret <string>
secondary_server <IP_address or name>
source_port <port number>
tertiary_destination_port <port number>
tertiary_secret <string>
tertiary_server <IP_address or name>
timeout <period>
vsa <enabled | disabled>

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

Parameters	Description
primary_destination_port	RADIUS destination port for the primary authentication server. Default: 1812 . Range: 0 - 65,535
primary_secret	Password of the Primary RADIUS server. Limit: 16 ASCII characters. Null string: ""
primary_server	IP address or name of the initial server to exchange authentication data with.
retransmissions	Maximum number of times to retransmit packets to one or both servers if transmissions fail. Default: 10 . Range: 0-100 . Value of 0 infinite infinite retries. We recommend you <i>do not</i> set to 0.
secondary_destination_port	RADIUS destination port for the secondary authentication server. Default: 1812 . Range: 0 - 65,535
secondary_secret	Password of the Secondary RADIUS server. Limit: 16 ASCII characters. Null string: ""
secondary_server	IP address or name of the second server to exchange authentication data with.
source_port	RADIUS source port for the primary authentication server. Default: 1812 . Range: 0 - 65,535
tertiary_destination_port	RADIUS destination port for the tertiary authentication server. Default: 1812 . Range: 0 - 65,535
tertiary_secret	Password of the Tertiary RADIUS server. Limit: 16 ASCII characters. Null string: ""
tertiary_server	IP address or name of the third server to exchange authentication data with.
timeout	Interval in seconds between retransmissions. Default: 3 seconds. Range: 1-60 .
vsa	Enables/disables transmission of Vendor Specific Attributes to specified RADIUS servers.

set board command_line_parameters <string>

Specifies CLI arguments used prior to HiPer ARC boot up. You can issue a command at the CLI to begin configuration using the bulk configuration file you earlier TFTP'd into HiPer ARC's FLASH memory. This command is useful when performing similar configurations on multiple HiPer ARCs. For example:

```
set board command_line_parameters -config anyone.cfg
```

Use the **show board command_line_parameters** command to display CLI arguments used at boot time.

set bootrom boot interface <eth:x>

Selects the Ethernet interface (LAN interface number) to be used for booting over the LAN. Use the **list lan interfaces** command to display available Ethernet interfaces. This parameter is used only at system boot up and is directly written into EEPROM, so the **save all** command is not required to save it.

set bootrom config

bootmode [flash | network]
ip_config_source [bootp | static]
upload_crashdump [disable | enable]

Sets bootrom parameters (used only at system boot up). The bootmode refers to a boot image taken from system FLASH memory or an image taken from a host on the network. The IP configuration source is where the network configuration is derived from during *network* booting, either *statically* (from HiPer ARC) or from a network host via the *bootp* method. These parameters are written to EEPROM directly, so the **save all** command is not required to save them.

Parameters	Description
bootmode	Sets booting method from <i>FLASH</i> memory or the <i>network</i> . Default: Flash
ip_config_source	If booting over the LAN, IP parameters will be taken either from <i>static</i> configuration in the board or will use <i>bootp</i> . Default: Static
upload_crashdump	If the system crashes, it will upload the crash dump file to the configured tftp server. Default Disable

set bootrom ip interface <eth:x>

address <IP_address>
crashdump_file <filename>
gateway <IP_address>
loadfile <filename>
netmask <ip_netmask>
tftpserver <IP_address>
tftp_boot [always | never | once]

Sets IP parameters for each LAN interface (used only when the system boots up). These IP parameters are used for network downloading of the image during booting and uploading crash dump information to a network host. The parameters are written to EEPROM directly, so the **save all** command is not required to save them.

Parameters	Description
<eth:x>	LAN interface address
address	IP address of the interface
crashdump_file	Crashdump information is written in to this file in the TFTP server. Limit: 127 ASCII characters
Gateway	IP address of the HiPer ARC.
Loadfile	File name of system boot image kept in the TFTP server. Limit: 127 ASCII characters
Netmask	Netmask of the LAN interface.
tftpserver	IP address of the host from which the boot image will be downloaded and crash dump information will be uploaded.
tftp_boot	How often boot image will be downloaded from tftp server. This parameter is valid only if bootmode is set to NETWORK. The choices are: <ul style="list-style-type: none"> ▫ NEVER - NETWORK boot will <i>not</i> be attempted. Default ▫ ONCE - will boot from NETWORK <i>once</i>; after that bootmode will change to FLASH. ▫ ALWAYS - each time the system boots the image will be taken from the network.

set bulk_file <file_name>

Specifies the name of a HiPer ARC bulk configuration file, which is the compressed concatenation of individual HiPer ARC configuration files (.CFG) used for uploading to HiPer ARC. You can name one of *two* bulk configuration file with the **set bulk_file** command and break out individual configuration files from the bulk configuration file with the **reset configuration** command.

```

set chassis slot <number>
    card_type <card_type>
    owner <yes | no>
    type <static>
    ports <1-31>

```

Configures a specific type of NAC modem card, the ownership of the slot, the number of ports to be enabled on a card in a slot, and the type of entry for that slot. The default **card_type** parameter is EMPTY.

Parameters	Description
slot number	Slot number in chassis from 1-16. Slot numbers can be specified in a range, such as: <i>4, 7, 8-14</i>
card_type	Type of quad modem hardware in the slot. They include: <ul style="list-style-type: none"> ■ QUAD_MODEM - V.34-type modem card (1-4 ports) ■ QUAD_I_MODEM - ISDN-type modem card (1-4 ports) ■ HDM_24 - 24-channel HiPer DSP card (1-24 ports) ■ HDM_30 - 30-channel HiPer DSP card (1-30 ports) ■ EMPTY - No card in slot. Number of ports set to zero.
owner	Specifies the ownership of a particular slot. Ownership means HiPer ARC communicates with modem interfaces resident on a card in this slot. Ownership is required because there may be more than one HiPer ARC card within the same chassis. Modem cards in the chassis must be partitioned among the various HiPer ARC cards within the chassis so that packet bus sessions from each modem can be established with the corresponding HiPer ARC. Default: yes
type	Changes the row type to <i>static</i> so chassis configuration data learned from the NMC chassis message may be saved to the configuration file. When chassis configuration entries are created after receiving a chassis awareness message from the NMC, the row type is set to <i>dynamic</i> . Any entries created through a CFM load, SNMP set, or CLI command render the row type <i>static</i> . Only static entries are saved to the configuration file via CFM.
ports	Sets the number of active ports for the card in the specified slot. Range: 1-31 .

```
set clearTCP connect_message <message string>
```

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

If the string is surrounded by double quotes, you can insert an escape character 'I' inside the quoted string. If the string is followed by the characters **b, f, n, r, t or v**, HiPer ARC will place special characters in the string, as follows:

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

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

- x0A = 0x0a

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

Other rules state:

- a double quote (") will place the double quote in the token
- a forward slash '/' will place one forward slash in the token

set command

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

Configures command line parameters. It lists:

Parameters	Description
global_terminal_settings_rows	Configures the page size (number of rows) output by CLI commands to subsequent HiPer ARC-connected sessions of administrative (manage) users. This command is not effective for currently connected users. Range: 1-256 . Default: 23
history	Sets depth of the buffer holding command history. Use history command to see current depth and list of your last CLI commands. Default: 10 commands . Range: 1-500 .
idle_timeout	Sets Console login connection to close after being idle for the specified interval, if that user is required to log in (login_required value must be set to YES. Range: 0-60 minutes. Default: 5 min.. Zero (0) value produces no timeout. Value can be changed only by a manage user.
local_prompt	Sets a separate (temporary) prompt for a command file session. Limit: 64 ASCII characters.
local_terminal_settings_rows	Configures the page size (number of rows) output by CLI commands to locally connected PC screens of administrative (manage) users. This command is effective only for the session when the command is issued. Range: 1-256. Default: 23
login_required	Sets whether a user on the Console port is required to log in. Value can be changed only by a manage user. Default: No.
prompt	Sets the global (permanent) command prompt for the CLI. Use show command to see the currently defined prompt. Limit: 64 ASCII characters

set connection

host_select [round_robin | random]
manage [manage prompt]
service [dialin user prompt]
user_name [user name]

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

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

set dialout

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

Sets global parameters for all NCSI dialout connections over modems.

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

set direct_request

delimiter <string>
timeout <interval>

A TACACS+ related command useful for tunneling and global realmng, allowing administrators to maintain separate AAA servers for different groups of users. The command enables HiPer ARC to direct authentication requests to a specified AAA server. The user name and password a user normally enters when connecting to HiPer ARC is expressed in the following way when employing directed request: *user@domain*. In this syntax, user is the *user name* and host the *host name* to which authentication is directed. HiPer ARC sends only the portion of the user name preceding the @ sign to the host specified following the @ sign. In other words, directed request lets you transmit a request to a configured server with only the user name sent to that specified server.

When deactivated using the **disable direct_request** command, AAA server rotation connects to the first available entry in the AAA Server Table via a round-robin method. Default: **enabled**.

Parameters	Description
<string>	Delimiter string consists of up to 6 delimiters (any printable character) used to determine the user name. Default: @#%
timeout	The interval in seconds before HiPer ARC selects the next-preferred server. Default: 5 seconds. Range: 0-30 seconds.

set dns

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

Sets the global parameters for DNS; both local DNS hosts (**list DNS host**) and remote DNS servers (**list DNS servers**), and DNS caching and negative caching parameters, in support of DNS host rotation for load balancing. See associated commands: **set login user** <name> **login_host_name**, **enable dns host_rotation** and **disable dns host_rotation** and *Chapter 9: Administrative Tools* for more information.

Parameters	Description
------------	-------------

cache	Enables or disables DNS caching. Setting to CLEAR flushes the DNS cache. Default: disabled
cache_maxttl	Maximum time in seconds DNS cache entries remain in the DNS cache before they're flushed. Range: 0 - 2147483
domain_name	Default domain designation to be used if no domain is specified (by add dns server command) in the name to be resolved. For example: usr.com. Limit: 64 ASCII characters.
ncache	Enables or disables negative DNS caching. Setting to CLEAR flushes the DNS negative cache. The negative DNS cache contains entries the DNS server found to be in error. For example, if the host name abc.xyz.com doesn't exist, the DNS server will return a non-existent name error.
ncache_maxttl	Maximum time in seconds DNS negative cache entries remain in the DNS negative cache before they're flushed. Range: 0 - 2147483
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: 1 . Range: 1-5 .
timeout	Interval in seconds to wait before deciding a request to a Name Server has timed out. Minimum interval and default is 5 seconds, maximum interval is 245 seconds.

set dns server preference <number>
name <server_name and domain_name>
address [IP_address]

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

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

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

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

*Note: Do not confuse **set facility** and **set syslog** commands. The **set facility** command determines which messages are generated on the console or to a telnetted PC - depending on the loglevel specified for each facility. The **set syslog** command, on the other hand, determines which messages are saved - depending on the global loglevel you've set for the particular SYSLOG host. The **show event** command displays event messages on the console if telnetted into HiPer ARC.*

The log 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
- **Verbose** - a regular periodic event, e.g. a routing update message
- **Debug** - for debugging purposes only

set global_call_type <pptp | l2tp | none>

Configures all calls as PPTP or L2TP calls, for use in systems where only PPTP or L2TP calls are made. This default can be disabled with the *none* value. This command effects immediate VPN tunnelling without authentication to limit network overhead.

```
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**.

*Note: Do **not** use the default initialization script supplied with earlier firmware versions (NETServer 3.x). The at&f1s0=1 script is invalid and may cause HiPer ARC's modems to lock up.*

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.

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

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

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

Parameters	Description
<interface_name>	Designation of interface you are setting parameters for. Limit: 64 ASCII characters.
filter_access	Off causes filters specified for an interface with a set interface command to override filters specified with a set user command when the filters are of the same type. Default: Off
input_filter	Name of the filter file you wish to be applied to the input stream coming in on the specified interface. Limit: 20 ASCII characters.
output_filter	Name of the filter file you wish to be applied to the output stream leaving the specified interface. Limit: 20 ASCII characters.

```
set ip application_source_address [radius | syslog | igmp]
    IP_address <IP_address>
```

Specifies the source IP address (where packets exit) of a HiPer ARC which has more than one Ethernet interface for IP routing or multi-home logical networks configured on the Ethernet and which needs to communicate that source address to an associated RADIUS or SYSLOG server. When configured (eth:1 or eth:2), the source address (of UDP packets) *overrides* both the internal IP address and *autoconfigured* IP system hosts address. HiPer ARC Ethernet addresses range in importance thusly: source IP address (highest priority), internal IP address, and default IP address (lowest priority). When the IP address is configured at **0.0.0.0**, this option is not set.

The **show ip settings** command will display this configuration.

See the **set ip unnumbered_link local_address command** for configuration of Ethernet IP addresses supplied to remote PPP or SLIP users when they dialup HiPer ARC.

```
set ip defaultroute gateway <IP_address or name>
    metric [hop count] }
```

Reconfigures a backup default route. The command changes the address or metric of a *primary* default route with a gateway on the IP network configured on the first HiPer ARC LAN interface (eth:1), and values for a *backup* default route with a gateway on the IP network configured on the second HiPer ARC LAN interface (eth:2).

A default route gateway specified with a higher metric acts as the *primary* default route gateway and a second default route gateway with a lower metric acts as the *secondary* default route gateway.

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

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. Range: 1-15 . Default: 1

```
set ip igmp <eth:1 | eth:2 | slot:x/mod:y>
    max_response_time <1-10 seconds>
    multicast_forwarding [enabled | disabled]
    multicast_proxy [enabled | disabled]
    query_interval <5-65,535 seconds>
    robustness <1-5>
    routing <enabled | disabled>
    version <1-2>
```

Specifies Internet Group Management Protocol (IGMP) settings to configure IP multicast groups. HiPer ARC performs IGMP forwarding; the present release does not support IGMP routing protocols such as PIM and DVMRP.

Parameters	Description
<interface_name>	The interface on which IGMP is enabled: eth:1 , eth:2 or slot:x/mod:y
max_response_time	The interval a host has to respond to the IGMP query. Default: 10 . Range: 1-10 seconds
multicast_forwarding	Multicast packets are forwarded when enabled. Default: Disabled
multicast_proxy	Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with the set ip multicast proxy interface command. Default: Disabled
query_interval	The frequency at which IGMP Host-Query messages are sent on the specified interface. Default: 125
robustness	Tuning parameter for expected packet loss on a subnet. If packet loss on a subnet is expected to be high, robustness may be increased. Range: 1-5 . Default: 2
routing	Will attempt to become the IGMP querier on this interface. Default: Disabled
version	The version of IGMP running on this interface. This object can be used to configure a router capable of running either version. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. Default: 2

```
set ip multicast heartbeat
    interface <interface_name>
    group <ip_multicast_address>
    time <interval>
    threshold <number>
    window <number>
```


Configures multicast monitoring for a specified multicast *group* or *interface*. See **enable** and **disable ip multicast_heartbeat**, and **show ip settings** commands for more information. It lists:

Parameters	Description
<interface_name>	The interface on which to monitor multicast traffic for the specified group: eth:1 , eth:2 , slot:x/mod:y
group	The IP address of the multicast group to monitor.
time	The interval, in seconds, to monitor multicast traffic. Range: 0 - 65535 . Default: 60
threshold	The interval during which multicast traffic is not received after which an SNMP trap is issued. Range: 0 - 65535 . Default: 3
window	The number of periods (in <i>time</i> values) to monitor multicast traffic. Range: 0-255 . Default: 5

set ip multicast proxy interface <interface_name>

Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with this command. See **set ip igmp** command above for more information.

set ip network <name>

```

broadcast_algorithm [bsd | ietf]
reassembly_maximum_size [number]
rip_authentication_key [string]
rip_export_metric <0-15>
rip_policies_update <rip_policies>
routing_metric <1-16>
routing_protocol [none | ripv1 | ripv2]

```

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

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

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

RIP Policies - The following RIP policies are supported by the IP route:

- **Send Default** - *disabled* by default, causes router to advertise itself as the default router.
- **Send Routes** - *enabled* by default. Tells RIP to advertise (broadcast) its routes on the network every 30 seconds - is standard for a gateway router.
- **Send Subnets** - *disabled* by default. If this flag is on, only routes with the same network and with subnets on the same network are sent out the interface.
- **Accept Default** - *disabled* by default. Determines whether router accepts default route advertisements.
- **Split Horizon** - *enabled* by default. Records the interface over which it received a particular route and does not propagate its information about that route back over the same interface. This prevents network loops.

- **Poison Reverse** - *disabled* by default. Routes that were excluded due to the use of split horizon are instead *included* with infinite cost (16). The system continues to broadcast the route, but with an infinite cost. **IMPORTANT:** In order to perform poison reverse, you must also enable split horizon.
- **Flash Update** - *enabled* by default. It is also known as “triggered update”, meaning routes that have their metrics modified will be advertised immediately, instead of waiting for the next scheduled broadcast.

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

- **Send Compatibility** - Controls the selection of destination MAC and IP addresses. It is *enabled* by default. When enabled, *broadcast* address is used; when disabled, *multicast* address is used.
- **RIP V1 Receive** - Controls the receipt of RIP version 1 updates. When RIP version 1 is the selected routing protocol, this policy is *enabled* by default, which means RIP version 1 packets are received. (When RIP version 2 is chosen, this policy is *enabled* by default, meaning RIP version 1 packets are received.
- **RIP V2 Receive** - Controls receipt of RIP version 2 updates. When RIP v1 is the selected routing protocol, this policy is *enabled* by default, which allows RIPv1 packets to be received. When RIP version 2 is selected, this policy is *enabled* by default, allowing RIPv2 packets to be received. RIPv2 is backward compatible.
- **Silent** - This flag tells RIPv2 not to send updates. It is *disabled* by default.

Parameters	Description
<network_name>	Designation of the IP network for which you want to set parameters. Limit: 64 ASCII characters
broadcast_algorithm	Algorithm determines which address is used in broadcasts to represent the entire network. Choices: <ul style="list-style-type: none"> ■ IETF - the IETF standard: nnn.nnn.nnn.255 (default) ■ BSD - 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: 3464 .
rip_authentication_key	ASCII string used for RIPv2 authentication.
rip_export_metric	Number of hops to advertise routes via this IP network. This value is set only when <i>RIPv1</i> or <i>RIPv2 routing_protocol</i> is selected. When the routing protocol is <i>none</i> , this value is automatically reset to the default: 0 . Range: 0-15
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 <i>NO_</i> in front is used to disable the policy. Default indicated by (D) . <i>Note:</i> For Poison Reverse to work properly, Split Horizon must also be enabled. <ul style="list-style-type: none"> ■ SEND_Default/NO_SEND_Default(D) ■ SEND_ROUTES(D)/NO_SEND_ROUTES ■ SEND_SUBNETS/NO_SEND_SUBNETS(D) ■ ACCEPT_Default/NO_ACCEPT_Default (D) ■ SPLIT_HORIZON(D)/NO_SPLIT_HORIZON ■ POISON_REVERSE/ NO_POISON_REVERSE(D) ■ FLASH_UPDATE(D)/NO_FLASH_UPDATE ■ SEND_COMPAT(D)/NO_RIPV1_SEND ■ RIPv1_RECEIVE(D)/NO_RIPv1_RECEIVE ■ RIPv2_RECEIVE(D)/NO_RIPv2_RECEIVE ■ SILENT (default is disabled)



routing_metric	Sets routing metric (number of hops between HiPer ARC and its destination) for use on IP network. Metric is set when the <i>routing_protocol</i> is configured as <i>ripv1</i> or <i>ripv2</i> . When <i>routing_protocol</i> is changed to none, the metric is changed back to the default value of 1. A metric value of 16 effectively shuts off RIP on that interface. The configured metric value is globally saved and retrieved after system reboot when the save all command is issued. A metric is considered the cost to use an interface with lower metrics corresponding to better, more direct routes. When employing primary and backup routers with RIP enabled, you can set a low metric on the primary router interface (eth:1) and a higher metric on the backup router interface (eth:2). Range 1-16 . Default: 1
routing_protocol	Sets routing protocol to be used on IP network. Choices are: none , RIP version 1 , or RIP version 2 . Default: None

set ip pool <pool name>

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

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

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

set ip route <IP_hostname or network address>

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

Modifies the IP route created using the **add ip route** command, described.

Parameters	Description
<IP hostname or IP network address>	IP address or host name of the remote destination, in the format <i>nnn.nnn.nnn.nnn</i> , entered <i>with</i> or <i>without</i> a mask specifier. The mask specifier can be 'A', 'B', 'C', or 'H' (host), or a numeric value from 8 to 30 (32 if a host) that describes the number of one bits in the mask. You can also specify the netmask in the <i>xxx.xxx.xxx.xxx</i> format. If you do not specify a mask, the system will self-generate it (based on the network address) for all routes except <i>host</i> routes, for which you <i>must</i> specify a mask. For help counting the bits, see <i>Appendix C: addressing Schemes</i> for a handy bitmask table.
gateway	Host name or IP address of the next hop to the specified IP network address
metric	Number of hops the destination is removed from the specified IP network address. Range: 1-15

set ip routing

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

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

Note: IP routing must be disabled before setting these values.

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

Parameters	Description
autonomous_system_number	Value associated with a protocol not currently supported. Disregard this value. Range: 1-65535
metric_maximum_entries	Most next hop entries the Next Hop Hash Table can hold. Default: 512 . Range: 256-65535
router_id	IP address of HiPer ARC. If value not specified, the system will take a user-configured internal IP address for this value, or the eth:1 value if no internal value is specified.
rip_flags	Flags indicate at which level a RIP instance is disabled or configured. Choices are: <ul style="list-style-type: none"> ▪ Metrics - Specifies how to increment metrics using RFC1058. ▪ Send_request - Sends a RIP request for routing data when an interface first comes up.

set ip unnumbered_link local_address <IP_address>

Specifies the local IP address supplied to unnumbered PPP or SLIP users when they dialup HiPer ARC. When the IP address is configured as 0.0.0.0, this option is *not* set. If the local IP address is not set using this command, the *internal* IP address of HiPer ARC will be used as the local IP address. If an internal IP address also is not set, the IP address of one of the Ethernet interfaces (eth:1/eth:2) will be used as the local IP address.

Important: This command allows multiple HiPer ARCs to report the same LAN address to users for LAN-to-LAN routing purposes. Be careful not to configure an unreachable address as the reported address for HiPer ARC or unpredictable actions may occur. Be aware that HiPer ARCs sharing a LAN address will answer a ping from a client but the answer may not return from the expected HiPer ARC.

This command may be used to:

- Select a specific local address from an *internal* IP address or *Ethernet* IP addresses when more than one of the Ethernet interfaces are configured and/or an internal IP address is configured.
- Set an *arbitrary* IP address as the *reported* local address for PPP/SLIP unnumbered links. Note that in this case, no IP route will be added in HiPer ARC for this arbitrary local IP address. This address is not considered as an IP address of HiPer ARC.

Local and remote IP addresses are configured on a *user* basis with **set network user** and **set dialout user** commands. Also, the **show ip settings** command displays this configuration.

See the **set ip_application_source_address** command for information about configuring HiPer ARC Ethernet addresses for RADIUS and SYSLOG servers.

set ipx network <network_name>

```

delay_ticks [number]
diagnostics [disable | enable]
maximum_learning_retries [number]
netbios [enable | disable]
netbios_cache_timer [seconds]
netbios_max_hops [number]
netbios_name_cache [disable | enable]
packet_maximum_size [number]

```

```

rip [auto_off | auto_on | on | off]
rip_age_multiplier [number]
rip_broadcast [enable | disable]
rip_gap_timer [number]
rip_packet_size [number]
rip_periodic [disable | enable]
rip_update_interval [number]
sap [auto_off | auto_on | on | off]
sap_age_multiplier [number]
sap_broadcast [enable | disable]
sap_gap_timer [number]
sap_nearest_replies [on | off]
sap_packet_size [number]
sap_periodic [enable | disable]
sap_update_interval [number]

```

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

Parameters	Description
<network_name>	Designation of the IPX network. Maximum size: 64 characters.
delay_ticks	Interval in number of ticks it takes to reach this IPX network. Default: 1 for LAN networks, 40 for WAN networks. Range: 0 -65535 .
diagnostics	Whether 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_cache_timer	Interval a NetBIOS system is kept in the cache. Default: 60 seconds
netbios_name_cache	Whether or not to cache a list of the other NetBIOS systems on this IPX network. Default: Disabled
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 this IPX network supports. Max size: 1600 bytes
rip	Turns RIP: on , off , auto_on or auto_off for this network. Default: On
rip_age_multiplier	Number to multiply the rip_update_interval by, to obtain the value for the aging out the entries in the RIP database. Default: 3
rip_broadcast	Enables/disables RIP broadcasts. Default: Enabled
rip_gap_timer	Interval the system waits between sending RIP packets. Default: 1
rip_packet_size	Size of RIP packets. Default: 446 bytes
rip_periodic	Enables/disables sending of RIP periodic updates. Default: Enabled
rip_update_interval	How often RIP should send periodic updates. Range: 1-500 seconds . Default: 60 seconds
sap	Turns SAP: on , off , auto_on or auto_off for this network. Default: On
sap_age_multiplier	Number to multiply the sap_update_interval by, to obtain the value for aging out entries in the SAP database. Range: 1-1080 . Default: 3
sap_broadcast	Enables, disables SAP broadcasts. Default: Enabled
sap_gap_timer	Interval the system should wait between sending SAP packets. Default: 1
sap_nearest_replies	Whether or not SAP will look for its nearest neighbors. Default: YES
sap_packet_size	Size of SAP packets. Default: 510 bytes
sap_periodic	Enables/disables sending of SAP periodic updates. Default: Enabled
sap_update_interval	How often RIP should send periodic updates. Range: 1-500 seconds . Default: 60 seconds

set ipx system

```
default_gateway [ipx_host_address]
```

initial_pool_address [ipx_network_address]
max_hops [number]
name [string]
number [internal network number]
pool_members [number]
ppp_users_network_address [ipx_address]
priority [number]

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

Parameters	Description
default_gateway	Default router for the dynamic IPX network.
initial_pool_address	First IPX address used to dynamically assign IPX network.
max_hops	Greatest number of hops this network will make to locate an IPX system. Range: 1-64 .
name	Designation for the dynamic IPX network.
number	Network address for the dynamic IPX network. This value is required to run various IPX services. See add ipx service command for more information.
pool_members	Number of addresses to reserve in the pool of IPX addresses used when dynamically assigning IPX networks. Range: 1-4096
ppp_users_network_address	Unique IPX network address assigned to unnumbered PPP dialin users only if they are configured through the set network user <name> ipx command with the address <code>fffffffc</code> . The address is expressed in the format: <code>xxxxxxx.</code> Values of <code>fffffffc</code> or <code>fffffffe</code> are invalid.
priority	Preference for the dynamic IPX network. Range: 1-3

set l2tp

ack_timeout <milliseconds>
control_receive_packet_window <number>
data_receive_packet_window <number>
flow_control <enable | disable>
load_balancing <enable | disable>
loglevel <disable | control_pkt_only | ctrl_and_headers_of_data_pkt | ctrl_and_data_pkt>
max_sessions <number>
max_tunnels <number>
num_retransmissions <number>
num_terminators <number>
reassembly_timeout <milliseconds>
reply_timeout <number>
retransmission_interval <seconds>
tunnel_challenge <enable | disable>

Configures default L2TP tunnel attributes on HiPer ARC. These values can be overridden by RADIUS. L2TP tunnels can also be enabled locally using the **set tunnel user** command. .

Parameters	Description
ack_timeout	Number of milliseconds the L2TP facility waits to send and acknowledge to its peer when there is no data or control packets to piggyback the acknowledgement to. The default causes immediate acknowledgment when no data or control packets are pending. Recommended value 500 - 600 . Default: 500
control_receive_packet_window	Size in number of packets of the control channel receive window sent to the L2TP facility's peers. After this number of control packets is acknowledged as received by the L2TP client, more packets are transmitted by the L2TP server. Default: 7
data_receive_packet_window	Size in number of packets of the data channel receive window sent to the L2TP facility's peers. After this number of data packets is acknowledged as received by the L2TP client, more packets are transmitted by the L2TP server. Default: 7
flow_control	Enables/disables data tunnel flow control. Default: Enable
load_balancing	When enabled, Hiper ARC accesses least-used LNS over the last 60 seconds. Default: Enable



loglevel	Logging level to set to dump packets to the Console. Default: Disable
max_sessions	Maximum number of simultaneous active sessions HiPer ARC can support. Limit: 256 . Range: 0 - 256
max_tunnels	Maximum number of simultaneous active tunnels HiPer ARC can support. Limit: 256
num_retransmissions	Number of retransmissions the L2TP facility tries before assuming its peer is unreachable. The default causes the stack to not try retransmissions. Default: 0
num_terminators	Number of concurrent tunnels HiPer ARC can <i>initiate</i> at one time. But, HiPer ARC can maintain up to 256 concurrent tunnels. Limit and Default: 64
reassembly_timeout	Number of milliseconds the L2TP facility uses to determine the window to use before reassembling out of order packets. A low value increases the chance out-of-sequence packets will be lost (which MAY cause the PPP decompression engine to reset), a high value increases the time period where the L2TP stack processes packets which were received out of order (especially in the case of a packet which was lost within the network). The default may cause all out of sequence packets to be lost. Default: 0
reply_timeout	Number of seconds the L2TP facility waits until a timeout occurs in receiving a response to the keep-alive (hello) message. Default: 0
retransmission_interval	Period in seconds between retransmissions of control packets which haven't been acknowledged. Default: 2 seconds .
tunnel_challenge	LNS asks LAC for password. If enabled, only authenticated tunnel requests are honored. Default: Disabled . When enabled, requires all incoming tunnels to perform authentication

set l2tp lns <1-9>

shared_secret <string>

security_level <none | control | data | both>

Sets parameters for the specified l2tp network server created by the **add l2tp lns** command.

Parameters	Description
<l2tp server number>	The indexed value for the specified L2TP network server. Range: 1-9
shared_secret	The password shared by the L2TP network server and access concentrator (LAC). Limit: 256 ASCII characters.
security_level	The degree of HMAC-MD5 packet encryption the L2TP network server will perform: <ul style="list-style-type: none"> ▪ data - encryption for data packets only ▪ control - encryption for data packets only ▪ both - encryption for data and control packets ▪ none - no encryption performed. <i>Default</i>

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>	Defines preferred rank in which a login host will be used (from first preference of 1 to least preference of 10). Use list login_hosts to see the preference number associated with a login host.
rlogin_port	TCP port number you wish to configure for RLOGIN access to the login host. If you do not specify it here, and the user does not specify the TCP port from the CLI rlogin command, then the default is 513 . Limit: 65535 . Default: 513
telnet_port	TCP port number you wish to configure for TELNET access to the login host. If you do not specify it here, and the user does not specify the TCP port from the CLI telnet command, then the default is 23 . Limit: 65535 . Default: 23

clearTCP_port	TCP port number you wish to configure for ClearTCP access to the login host. There is no default TCP port number. Limit: 65535 . Default: 6000
---------------	--

set maximum_local_users <number>

Configures the total number of users that can be created locally on HiPer ARC. See the **show maximum_local_users** command to display settings. Maximum: **1000**.

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]
disable_authentication [async_ppp | none | ppp | sync_ppp]
filter_access [on | off]
host_address [IP_address or name]
host_type [prompt | select | specified]
init_script [name]
input_filter [name]
login_service [telnet | rlogin | cleartcp | ping]
message [login_message]
output_filter [name]
password [string]
prompt [prompt_message]
prompt_style [local | remote]
protocol [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 with this command can also be configured using **set switched interface**, but this command sets multiple interfaces with one command. Issue the **show interface settings** command to view configuration.

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

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

Parameters	Description
<group_name>	Designation of the modem group. Defaults: all , slot:1 , slot:2 , slot:3 , etc. Limit: 64 ASCII characters.
access	Sets access type for switched interface. Modem can allow dial-in , dial-out or both (two-way). Default: two-way



disable_authentication	<p>Sets enabling/disabling of authentication for types of dial-in users on a <i>per interface</i> basis. If authentication is disabled and a PPP call is auto-detected, the interface to which the user has dialed in will be checked for a configured user name which must previously have been entered using the <i>user_name</i> parameter in the above command. If <i>user_name</i> is specified for the particular interface, all user profile information will be forwarded without authentication. If no <i>user_name</i> is configured on the specified interface, <i>default</i> user's profile will be forwarded without authentication. The types of calls you can specify to disable authentication for are:</p> <ul style="list-style-type: none"> ▫ None - Authentication is <i>not</i> disabled for any type of PPP call. Default ▫ Async_ppp - Authentication is disabled if the incoming call is autodetected as a PPP <i>asynchronous</i> call ▫ Sync_ppp - Authentication is disabled if the incoming call is autodetected as a PPP <i>synchronous</i> call ▫ PPP - Authentication is disabled if the incoming call is autodetected as a PPP call <p><i>Note:</i> When used, this feature disables all other types of authentication included local, RADIUS and TACACS+ authentication.</p>
connection_type	<p>Sets the connection type for switched interface. Options:</p> <ul style="list-style-type: none"> ▫ Direct_net - Uses the protocol parameter's setting to create a network (virtual node) connection. Employs <i>user name</i> and <i>password</i> specified in this command. Authentication is done by the network protocol such as PPP. <i>Direct_net does not support</i> the SLIP protocol. ▫ Direct_conn - Employs <i>user name</i> and <i>password</i> specified in this command to establish a login type connection to the target host. Authentication is accomplished by the target host. If user name and password are not specified with this choice, user "<i>default</i>" is employed. ▫ Normal - Prompts for both <i>user name</i> and <i>password</i>. Default ▫ Prompt_user_only - Prompts for <i>user name</i> only and authenticate with the <i>password</i> specified in this command. ▫ No_prompt - Does not prompt. Authenticates with the <i>user name</i> and <i>password</i> specified in this command. If user name and password are not specified with this choice, user "<i>default</i>" is employed.
dial_prefix	Prefix added to all phone numbers dialing from this port. Limit: 64 ASCII characters.
filter_access	Turns filtering ON or OFF. Default: Off
host_type	<p>Identifies how dial in connection is set up. Options:</p> <ul style="list-style-type: none"> ▫ prompt - prompted to enter host name or address. Default ▫ select - a host is chosen from a login host list you specify, configured by the set connection command. ▫ specified - connected to IP address configured here.
host_address	IP address to connect a dial-in user to, if the host type is specified, and connection type is <i>direct_conn</i> or <i>direct_net</i> .
init_script	Name of modem initialization script used. Maximum size: 7 ASCII characters. If you are setting an <i>init_script</i> for a Modem Pool or Interface the <i>init_script</i> name must already exist. A null string ("") indicates the name will be deleted. Default: USR_int
input_filter	File name of filter screening incoming data.
login_service	<p>The login service to use, if the connection type is not <i>direct_net</i>. Options:</p> <ul style="list-style-type: none"> ▫ TELNET. <i>Default</i> ▫ RLOGIN ▫ ClearTCP ▫ Ping - user pings a login host, receives a successful/unsuccessful message and is disconnected.

message	String to display to a dial-in user when connection is set. Limit: 64 ASCII characters You can use \$value to stipulate more parameters in the message line for identification purposes. <ul style="list-style-type: none"> ▫ \$date - current date according to system uptime ▫ \$callid - user's call identification according to system uptime ▫ \$port - port occupied by user (slot:x/mod:y) ▫ \$hostname - user's host name ▫ \$sysname - user's system name (same as hostname) ▫ \$time - time of call according to system uptime <i>Note:</i> The message, if it includes spaces, must be enclosed in quotations. Use the show user command to view the message as configured. See <i>Chapter 9: Administrative Tools</i> for more information.
output_file	File name of filter screening outgoing data.
password	Parameter used if the connection type is no_prompt or prompt_user_only. Limit: 63 ASCII characters.
prompt	String to present the dial-in user. Limit: 256 ASCII characters.
prompt_style	Specifies whether prompting of the username and password for the interface in this modem group will be provided by HiPer ARC (Local), or by a distant security service such as RADIUS or TACACS+ (remote). Default: Local
protocol	Protocol to connect with, if the connection type is direct_net. SLIP is not supported by direct_net connection type. Default: PPP
TCP_port	TCP port number for the login host. Parameter used when connection type is <i>direct_conn</i> or <i>direct_net</i> . Limit: 65535
type	Specifies type of connection allowed on interface. <ul style="list-style-type: none"> ▫ Login port only allows login users ▫ Network port only allows network users ▫ Login_network allows either type. Default
user_name	Designation for the switched interface, used if connection type is no_prompt. Limit: 64 ASCII characters.

set mpip

server_state <off | on>
client_state <off | on>
port <number>

Configures MPIP port numbers and on/off status for any HiPer ARC acting as a MPIP server or client. Setting this command doesn't affect the MPIP Server and MPIP Client tables. ...

Parameters	Description
server_state	Turns all MPIP servers on or off. Default: off
client_state	Turns all MPIP clients on or off. Default: on
port	The UDP port for the MPIP server and client. Default: 5912 . Range: 0-65,535

set mpip client <IP_address>

sharedsecret <string>
type <hiperarc | netserver>

Configures MPIP client parameters you set with the **add mpip client** command.

Parameters	Description
<IP address>	Unique identifier of the MPIP client.
sharedsecret	Password shared by the MPIP client and server. Limit: 16 ASCII characters.
type	The product type of the MPIP client: HiPer ARC or NETServer . The distinction between types is relevant only to a HiPer ARC configured as an MPIP server - NETServer-based MPIP clients must specify NETServer type. Default: HiPer ARC

```

set mpir server <IP_address>
    port <number>
    priority <1-32>
    sharedsecret <string>

```

Configures MPIP server parameters you set with the **add mpir server** command.

Parameters	Description
<IP address>	Unique identifier of the MPIP server.
port	The UDP port all HiPer ARC MPIP servers use. Default: 5912
priority	Rank specifying preference of MPIP server used. If two servers share the same priority, the server with the smaller IP address takes precedence. Default: 1 . Range: 1-32
sharedsecret	Password shared by the MPIP client and server. Limit: 16 ASCII characters.

```

set network service <admin_name>
    close_active_connections [true | false]
    data [string]
    server_type [service_name]
    socket [socket_number]

```

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

Parameters	Description
<admin_name>	Designation you assigned to network service with the add network service command. Limit: 64 ASCII characters.
close_active_connections	Indicates whether or not to close any active connections when a service is shut by disable network_service . Default: False
data	TELNET and ClearTCP Ancillary Data. This field contains server-specific configuration data. See table which lists the configurable ancillary data parameters in the add network service command on page #.
server_type	Type of network service you wish to assign to this administration name. Available services: <ul style="list-style-type: none"> ▪ ClearTCPD - daemon enables access to a modem group on socket 0. Uses TCP. ▪ DialOut - supports dial-out connections to IP hosts on socket 32773. Uses TCP. ▪ SNMPD - daemon supports SNMP on socket 161. Uses UDP. ▪ TFTPD - daemon supports file transfer service on socket 69. Uses UDP. ▪ TELNETD - daemon supports TELNET, either to the CLI or a modem group on socket 23. Uses TCP.
socket	The port the server listens on. For TFTP, TELNET and ClearTCP, it is the TCP or UDP port number. Socket numbers are the joined sender's (or receiver's) IP address and service type's port number. Range: 0-65535

```

set ntp

    polling_interval [64-1024]
    primary_server [IP_name or address]
    retransmissions [0-200]
    secondary_server [IP_name or address]
    timeout [1-60]

```

Sets parameters for the Simple Network Time Protocol client process, which references a clock located on the Internet. This is useful to specify the server you want HiPer ARC to access for time synchronization. Support for NTP is based on RFC 2030, using Unicast mode only. See the **show ntp settings** command to display ntp configuration. .

Parameters	Description
------------	-------------

polling_interval	Period in seconds the NTP process takes to gather time synchronization information. Default: 600 seconds
primary_server	IP address or host name of the server HiPer ARC will contact first for time synchronization.
retransmissions	Maximum number of times a request is retransmitted to a specified server before the server is considered unavailable. Range: 1 - 200 attempts . Default: 5 attempts
secondary_server	IP address or host name of the server HiPer ARC will contact for time synchronization whenever the primary server is unavailable.
timeout	Number of seconds since a request has been sent to a server, after which period the request is considered timed-out. Range: 1 second - 1 minute . Default: 10 seconds

set packet_logging

logging [all | radius | none]

packet_size [0-493 bytes]

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

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

set pbus reported_base <0 | 1>

Sets the base to report modem slot/span/channel settings for packetbus modems. This affects vendor-specific fields (slot and channel) in RADIUS authentication and accounting packets. For example, when this field is set to *0*, the first modem on the first span in the first slot is reported as *slot=0,span=0,channel=0*. If this field were set to *1*, this modem is referred to as *slot=1,span=1,channel=1*. Use **show pbus settings** command to display settings.

set pbus reported_port_density <1-256>

Configures peak modem availability across HiPer ARC slots to correlate with the RADIUS NAS-Port attribute. RADIUS uses this attribute to specify the physical slot and port a user logs in on HiPer ARC. RADIUS also uses NAS-PORT to associate filter change requests with users.

If QUADs and HDMS are mixed in the chassis, set the reported-port-density to the maximum (24).

The NAS port ID is calculated using this formula: slot number(0-15) x (report_port_density) + [channel(0-255)] + reported_base (Port Desn default 256).

set pbus trap

active [enable | disable]

congestion [enable | disable]

error [enable | disable]

inactive [enable | disable]

lost [enable | disable]

Informs the Network Management Agent whether traps should be sent to the Network Management Card when a particular event (described below) occurs on a packet bus connection. By default, the trap is enabled

for all packet bus connections on the gateway card. You can enable/disable any function but for all interfaces only. Use the **list pbus traps** to display values.

Parameters	Description
active	Pbus session is active. Can be disabled by enabling the interface down. Default: Enable
inactive	Pbus session is inactive. Can be enabled by bringing the interface up. Default: Enable
congestion	Contention on packets for space to transmit on pbus. Default: Enable
lost	Pbus session down. Default: Enable
error	Pbus session error occurred. Default: Enable

set ping maximum_rows <rows in table>

Sets maximum number of rows permissible in the Remote Ping Table. Note that setting this parameter to a number smaller than the current number of rows will not cause any row deletions immediately but in the future. Use the **show ping settings** command to view configuration. Default: **20**. Range: **1-1000**.

set ping service_loss_system <IP_name or address>

frequency [1-200 seconds]

misses_allowed [1-1000]

timeout [1-6000 seconds]

Sets parameters configured by the **add ping_service_loss_system** command. Use the **list ping service_loss_systems** command to display configuration. See page Creates a configurable ping that monitors IP connectivity across the network to a specified server. If service is lost to the server, HiPer ARC notifies the NMC (which can be configured) to use auto-response to busy out all chassis modems so no more calls are answered and any hunt groups will answer to other systems. Based on the ICMP ping protocol, this command checks the IP address for each time period specified. If no response is received before the timeout expires, HiPer ARC busies out all modems. Pings continue after modems busy out and when connectivity to all modems is restored, modem service is restored. for more details.

Parameters	Description
<ip name or address>	IP name or IP address of the system you want pinged.
frequency	Interval in seconds between ping requests. Default: 30 . Range: 1-200 .
misses_allowed	Number of ping failures allowed before busying out modems. Default: 1 . Range: 1-10 .
timeout	Interval in seconds to wait before busying out modems. Default: 10 . Range: 1-60 .

set ppp

authentication_preference <chap | default | eap | ms_chap | pap | radius_eap_proxy>

ccp_modemtype_accept <none | all,digital,compressed_analog ,uncompressed_analog>

dns_usage <system | ppp | none>

nbns_primary <ip address>

nbns_secondary <ip address>

pppdns_primary <ip_nbns_address>

pppdns_secondary <ip_nbns_address>

receive_authentication [none | pap | chap | any | eap | ms_chap | encrypted_any | radius_eap_proxy]

session_start_message <string>

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

Note: Users who dial in and receive a compressed_analog connection (MNP5 or V.42bis) won't receive PPP compression. Payload compression is set by the parameter - not header compression as set for a user.

Parameters	Description
authentication_preference	If the <i>receive_authentication</i> value is set to ANY , this value will set the authentication type for the <i>first</i> attempt. If the Default setting is selected, authentication types will be negotiated in this order of preference: CHAP, EAP, MS_chap and PAP. This value works in conjunction with <i>receive_authentication</i>
ccp_modemtype_accept	The call type for which PPP compression will be attempted/accepted. Issuing this command overrides the <i>compression_algorithm</i> parameter set by the set network user <name> ppp command. <ul style="list-style-type: none"> None - No PPP data compression for any call type All - PPP data compression will always be attempted Digital - PPP data compression only for digital calls. Default Compressed_analog - PPP data compression only for compressed (modem compression) analog calls. Uncompressed_analog - PPP data compression only for uncompressed (modem compression) analog calls. Default
dns_usage	Enables/disables HiPer ARC to supply clients with Domain Name System (DNS) server addresses used in IPCP negotiation. Default: On
nbns_primary	IP address of the primary NetBIOS name server
nbns_secondary	IP address of the secondary NetBIOS name server
pppdns_primary	The Domain Name Server (DNS) primary server address used in IPCP negotiation. This will be used only if there is no user-specific value available.
pppdns_secondary	The Domain Name Server (DNS) secondary server address used in IPCP negotiation. This will be used only if there is no user-specific value available.
receive_authentication	The authentication protocol HiPer ARC uses to authenticate its PPP peer (the peer can employ a protocol of its choice). This value works in conjunction with <i>authentication_preference</i> . If the <i>Any</i> or <i>Encrypted_any</i> value is selected, the authentication protocol tried first from the group can be selected by specifying the <i>authentication_preference</i> parameter. Note the following choices: <ul style="list-style-type: none"> If <i>receive_authentication</i> is set to <i>any</i>, then <i>authentication_preference</i> can be set to <i>CHAP</i>, <i>MS_chap</i>, <i>EAP</i>, <i>proxy_eap</i>, <i>PAP</i> or <i>default</i> (CHAP). If <i>receive_authentication</i> is set to <i>any</i>, then <i>authentication_preference</i> can be set to <i>CHAP</i>, <i>MS_chap</i>, <i>EAP</i>, <i>proxy_eap</i>, or <i>default</i> (CHAP). If <i>receive_authentication</i> is set to <i>any other value</i>, then the <i>authentication_preference</i> setting is ignored. Protocols are negotiated in this order of preference: CHAP, EAP, MS_chap and PAP. See Chapter 7: LAN-to-LAN Routing for details about CHAP and PAP. Options are: <ul style="list-style-type: none"> None - no user authentication requested PAP - only Password Authentication Protocol allowed with peer CHAP - only Challenge Handshake Authorization Protocol (MD5) authentication allowed with peer Any - any authentication method can be used EAP - only EAP_MD5 (native mode) authentication allowed with peer MS_chap - only MS_chap authentication allowed with peer Encrypted_any - either CHAP, MA_chap, or EAP-MD5 authentication allowed Radius_eap_proxy - only EAP negotiated, and all EAP packets are proxied to the RADIUS server

session_start_message	<p>A message string to display at a client's terminal when a connection is established and PPP is begun in HiPer ARC. You can add additional values as follows:</p> <ul style="list-style-type: none"> ▮ %server_ip - identification of HiPer ARC's local (server's) IP address ▮ %client_ip - identification of remote (client's) IP address <p>For example:</p> <p>set ppp session "PPP session beginning now from %server_ip to %client_ip."</p> <p>If the string is surrounded by double quotes, you can insert an escape character 'I' inside the quoted string. If the string is followed by the characters b, f, n, r, t or v, HiPer ARC will place special characters in the string, as follows:</p> <ul style="list-style-type: none"> ▮ \b = backspace ▮ \f = formfeed ▮ \n = newline ▮ \r = carriage return ▮ \t = tab ▮ \v = vertical tab <p>If the string is followed by an x, the next two characters will be interpreted as a hexadecimal constant as follows:</p> <ul style="list-style-type: none"> ▮ x0A = 0x0a <p>If the string is followed by <i>any other character</i>, that character will be placed in the token.</p> <p>Other rules state:</p> <ul style="list-style-type: none"> ▮ a double quote (") will place the double quote in the token ▮ a forward slash '/' will place one forward slash in the token
-----------------------	---

set pptp <number>

data_channel_delayed_ack_timeout <milliseconds>
data_channel_reassembly_timeout <milliseconds>
data_channel_receive_packet_window <number>
echo_reply_timeout <seconds>
flow_control <enable | disable>
idle_timeout <number>
load_balancing <enable | disable>
loglevel <disable | control_pkt_only | ctrl_and_headers_of_data_pkt | ctrl_and_data_pkt>
max_seek_descriptors <number>
max_sessions <number>
max_tunnels <number>

Configures flow characteristics for a PPTP tunnel on HiPer ARC. PPTP tunnels can also be enabled locally using the **set tunnel user** command.

Parameters	Description
<number>	Stack index number.
data_channel_delayed_ack_timeout	Number of milliseconds the PPTP stack waits to send and acknowledge to its peer when there is no data packets to piggyback the acknowledgement to. The default causes immediate acknowledgment when no data packets are pending. Default: 0
data_channel_reassembly_timeout	Number of milliseconds the stack uses to determine the window to use before reassembling out of order data packets. A low value increases the chance out-of-sequence packets will be lost (which MAY cause the PPP decompression engine to reset), a high value increases the time period where the pptp stack processes packets which were received out of order (especially in the case of a packet which was lost within the network). The default may cause all out of sequence packets to be lost. Default: 0
data_channel_receive_packet_window	Size in number of packets of the data channel receive window sent to the stack's peers. Range: 0-256
echo_reply_timeout	Number of seconds the PPTP stack waits until a timeout occurs in receiving a response to the keep-alive (hello) message. Default: 0

flow_control	Enables/disables data tunnel flow control. Default: Disable
idle_timeout	Interval in seconds waited before the control tunnel is timed out. Range: 0-65535
load_balancing	When enabled, Hiper ARC accesses least-used LNS over the last 60 seconds. Default: Enable
loglevel	Logging level to set to dump packets to the console. Default: Disable
max_sessions	Maximum number of simultaneous active sessions the stack can support. Default: 0 . Range: 1-451
max_seek_descriptors	Highest number of tunnel endpoints the PPTP stack can remain simultaneously connected to. Range: 1-451 . Default: 8
max_tunnels	Maximum number of simultaneous active tunnel sessions per tunnel the stack can support. Range: 1-451

set radius

attribute_style <standard | ascend>
authentication_algorithm <fall_through | round_robin>
interim_accounting_interval <period>

Sets RADIUS authentication parameters including the descriptive *style* of attributes you prefer to use, the *authentication* procedure employed and the *interval* between accounting packet transmission.

The `authentication_algorithm` parameter works in the following manner. HiPer ARC refers to its Authentication Table for the IP addresses of RADIUS servers when RADIUS requests are received. When no response is received from the primary server within a specified interval, the RADIUS request is re-transmitted to the primary *and* secondary servers via a *fall-through* algorithm. Another available selection process shares the authentication load using a *round_robin* algorithm to query the primary, secondary or tertiary servers until an authentication response is received. This is done by HiPer ARC's Authentication Table which keeps track of the last server tried successfully, making the next authentication request to the previously successful server first. If during this cycle the maximum retransmission value is reached, authentication requests are terminated. You may configure this value using the **set authentication retransmission** command. Default: **round_robin**

Setting the *interim accounting interval* specifies how often checkpoint accounting packets are sent to the accounting server.

Parameters	Description
attribute_style	Method used to describe RADIUS attributes. Choices: standard or ascend
authentication_algorithm	Algorithm type to be used in selecting a RADIUS authentication server from those servers available: Fall-through or round_robin .
interim_accounting_interval	Interval in seconds between interim accounting packet transmissions by HiPer ARC. Range: 5 -3,600 seconds

set security_service <radius | tacacsplus>

Generates RADIUS or TACACS+ service upon HiPer ARC bootup. Configuring this service to *tacacsplus* enables EAP support. Default: **Radius**

set service_loss_busyout radius

frequency [interval]

Sets the interval at which network connectivity will be checked by a RADIUS server. If service is lost to the RADIUS server after a specified period (*frequency*), HiPer ARC will busy out the Hub's modems. HiPer ARC will continuously poll the RADIUS server until connectivity is restored and, at that point, restore the Hub's modem's to their normal state. Default: **60 seconds**. Range: **1-200 seconds**.



set slip session_start_message <string>

Configures a message string to display at a client's terminal when a connection is established and SLIP is begun in HiPer ARC. Limit: **256 ASCII** characters. You can add additional values as follows:

- **%server_ip** - identification of HiPer ARC's local (server's) IP address
- **%client_ip** - identification of remote (client's) IP address

For example:

```
set slip session "SLIP session beginning now from %server_ip to %client_ip."
```

If the string is surrounded by double quotes, you can insert an escape character 'I' inside the quoted string. If the string is followed by the characters **b, f, n, r, t or v**, HiPer ARC will place special characters in the string, as follows:

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

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

- **x0A** = 0x0a

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

Other rules state:

- a double quote (") will place the double quote in the token
- a forward slash '/' will place one forward slash in the token

set snmp community <name>

```
access [ro | rw | adm]
address [IP_address]
community_pool [name]
validate_address [use_address | use_pool]
```

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

Parameters	Description
<community_name>	Group designation for a pool of management stations which authorize SNMP requests.
access	Determines what type of access to SNMP MIBs the added user will have. Options are Read Only (RO), Read Write (RW) and Administrator (ADM). Administrator allows <i>read access to all objects</i> and <i>write access to all writeable objects</i> . RO is the default on public (0.0.0.0) networks and RW the default on private networks.
address	IP address of this SNMP management station, expressed in the form <i>nnn.nnn.nnn.nnn</i>
community_pool	Designation for the pool of IP addresses comprising this SNMP community. Limit: 64 ASCII characters.

validate_address	Method to determine access to this management station. The <i>use_address</i> value uses the specified IP address to validate access. The <i>use_pool</i> value uses the list of IP addresses specified in the <i>community_pool</i> value to validate access.
------------------	--

set snmp trap_community <community_name>
 address [IP_address]
 trap_community_pool [name]
 trap_validate_address [use_address | use_pool]

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 trap_communities**.

Parameters	Description
<community_name>	Trap group designation for a pool of management stations which authorize SNMP requests.
address	IP address of this SNMP management station, expressed in the form <i>nnn.nnn.nnn.nnn</i>
community_pool	Designation for the trap pool of IP addresses comprising this SNMP community. Limit: 64 ASCII characters.
trap_validate_address	Method to determine access to this management station. The <i>use_address</i> value uses the specified IP address to validate access. The <i>use_pool</i> value uses the list of IP addresses specified in the <i>trap_community_pool</i> value to validate access.

set switched interface <slot:x/mod:y>
 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]
 disable_authentication [none | async_ppp] | sync_ppp | ppp]
 filter_access [on | off]
 host_address [IP_name or address]
 host_type [prompt | select | specified]
 init_script [name]
 input_filter [name]
 login_service [telnet | rlogin | cleartcp | ping]
 message [login_string]
 output_filter [name]
 password [user_password]
 prompt [prompt_message]
 prompt_style [local | remote]
 protocol [ppp | slip]
 tcp_port [port_number]
 type [network | login | login_network]
 user_name [user name]

Configures port parameters for the specified switched (modem) interface (slot:2/mod:1, e.g.). To display switched interfaces you have configured, use the **list switched interfaces** command. To view settings for a particular interface, use the **show interface** <interface name> **settings** 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.*

Parameters	Description
<interface_name>	The switched interface (slot:x/mod:y) to modify. Limit: 64 ASCII characters.

access	Sets access type for switched interface. The modem can allow dial-in only, dial-out only or both (TWO-WAY). Default: Two-way
at_command	String representing any generic AT command. When implemented, output is shown immediately on CLI.
connection_type	<p>Sets connection type for switched interface. Options:</p> <ul style="list-style-type: none"> ▫ Direct_net - Uses the protocol parameter's setting to create a network (virtual node) connection. Employs <i>user name</i> and <i>password</i> specified in this command. Authentication is done by the network protocol such as PPP. <i>Direct_net does not support</i> the SLIP protocol. ▫ Direct_conn - Employs <i>user name</i> and <i>password</i> specified in this command to establish a login type connection to the target host. Authentication is accomplished by the target host. If user name and password are not specified with this choice, user "<i>default</i>" is employed. ▫ Normal - Prompts for both <i>user name</i> and <i>password</i>. Default ▫ Prompt_user_only - Prompts for <i>user name</i> only and authenticate with the <i>password</i> specified in this command. ▫ No_prompt - Does not prompt. Authenticates with the <i>user name</i> and <i>password</i> specified in this command. If user name and password are not specified with this choice, user "<i>default</i>" is employed.
dial_prefix	Prefix added to all phone numbers dialing from this port. Limit: 7 characters.
filter_access	Turns filtering ON or OFF. Default: Off
disable_authentication	<p>Sets enabling/disabling of authentication for types of dial-in users on a <i>per interface</i> basis. If authentication is disabled and a PPP call is auto-detected, the interface to which the user has dialed in will be checked for a configured user name which must previously have been entered using the <i>user_name</i> parameter in the above command. If <i>user_name</i> is specified for the particular interface, all user profile information will be forwarded without authentication. If no <i>user_name</i> is configured on the specified interface, <i>default</i> user's profile will be forwarded without authentication. The types of calls you can specify to disable authentication for are:</p> <ul style="list-style-type: none"> ▫ None - Authentication is <i>not</i> disabled for any type of PPP call. Default ▫ Async_ppp - Authentication is disabled if the incoming call is autodetected as a PPP <i>asynchronous</i> call ▫ Sync_ppp - Authentication is disabled if the incoming call is autodetected as a PPP <i>synchronous</i> call ▫ PPP - Authentication is disabled if the incoming call is autodetected as a PPP call <p><i>Note:</i> When used, this feature disables all other types of authentication included local, RADIUS and TACACS+ authentication. Default: None</p>
host_address	IP address to connect a dial-in user to, if the host type is specified, and connection_type is direct_conn or direct_net.
host_type	<p>Identifies how connection is established. Dial-in user is:</p> <ul style="list-style-type: none"> ▫ Prompt - prompted to enter a host name or address. ▫ Select - connected to a login host, selected from the list of login hosts, determined by the host_select field in the <i>set connection</i> command. Default ▫ Specified - connected to the configured IP address.
init_script	Name of modem initialization script used. Maximum size: 7 ASCII characters. If you are setting an init_script for a Modem Pool or Interface the init_script name must already exist. A null string ("") indicates the name will be deleted. Default: USR_int
input_filter	File name of filter screening incoming data.
login_service	<p>Login service to use if the connection_type is <i>not</i> direct_net. Options:</p> <ul style="list-style-type: none"> ▫ TELNET. <i>Default</i> ▫ RLOGIN ▫ ClearTCP ▫ Ping - user pings a login host, receives a successful/unsuccessful message and is disconnected.

message	String to display to a dial-in user when connection is set. Limit: 64 ASCII characters You can use \$value to stipulate more parameters in the message line for identification purposes. <ul style="list-style-type: none"> ▪ \$date - current date according to system uptime ▪ \$callid - user's call identification according to system uptime ▪ \$port - port occupied by user (slot:x/mod:y) ▪ \$hostname - user's host name ▪ \$sysname - user's system name (same as hostname) ▪ \$time - time of call according to system uptime <i>Note:</i> The message, if it includes spaces, must be enclosed in quotations. Use the show user command to view the message as configured. See <i>Chapter 9: Administrative Tools</i> for more.
output_filter	File name of filter screening outgoing data.
prompt	String to present the dial-in user. Default: login . Limit: 64 ASCII characters.
prompt_style	Specifies whether prompting of the username and password on this interface will be provided by HiPer ARC (Local), or by a distant security service such as RADIUS or TACACS+ (remote). Default: Local
password	Used if connection_type is no_prompt or prompt_user_only. Limit: 63 ASCII characters.
protocol	Protocol (PPP) to connect with, if connection type is direct_net. SLIP is not supported by <i>direct_net</i> connection type. Default: PPP
tcp_port	TCP port number for login host. Value used for <i>direct_conn</i> or <i>direct_net</i> connection types. Limit: 65535
type	Type of connections to allow on the switched interface. <ul style="list-style-type: none"> ▪ Login port allows login users only ▪ Network port allows network users only ▪ Login_network allows either type. Default
user_name	Designation for the switched interface, used if connection type is <i>no_prompt</i> . Limit: 64 ASCII characters

set syslog <IP_address>

allow_all_auth_levels [yes | no]

facility [log_auth | log_local0 | | log_local1 | log_local2 | log_local3 | log_local4 | log_local5 | log_local6 | log_local7]

loglevel [critical | unusual | common | verbose]

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

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

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

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

The four levels of logging are:

- **Critical** - a serious system error, which may effect system integrity. **Default**
- **Unusual** - an abnormal event, which the system should recover from
- **Common** - a regularly occurring event

- **Verbose** - a regular periodic event, e.g. a routing update message.

Parameters	Description
<IP_address>	SYSLOG address where information is directed.
allow_all_auth_levels	Permits or denies transmission of all loglevel SYSLOG messages by the Auth facility. Default: Yes
facility	SYSLOG facility where output is sent. See choices above. Default: log_auth
loglevel	SYSLOG loglevel to which output is assigned. See choices above.

Note: Do not confuse set facility and set syslog commands. The set facility determines which messages are generated on the console or to a telnetted PC - depending on the loglevel specified for each facility. The set syslog command, on the other hand, determines which messages are saved - depending on the global loglevel you've set for the particular SYSLOG host.

set system

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

Specifies system information, displayed using *show system*. The transmit authentication keyword (Limit: **64 ASCII** characters) is used when the HiPer ARC receives a challenge - typically during LAN to LAN or L2TP/PPTP 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 ASCII** characters.

Parameters	Description
contact	Name of HiPer ARC administrator.
location	Site of the HiPer ARC.
name	Designation of your HiPer ARC.
transmit_authentication_name	Remote account name. <i>Note:</i> In LAN-to-LAN and L2TP/PPTP connections, this name must match the user name at the far end of the connection.

set tacacsplus interim_accounting_interval <5-3600>

Configures the interval in minutes to issue a watchdog accounting request to the TACACS+ server. Watchdog requests provide updated accounting information for a dialup user connection. Default: **240**. Range: **5-3600**.

set tap id <number>

address <IP_address>
facility <log_auth | log_local0 | log_local1 | log_local2 | log_local3 | log_local4 | log_local5 | log_local6 | log_local7>
format <hex | ascii | clear>
loglevel <critical | unusual | common | verbose>

Configures a tap on a session previously created with the **add tap** command. Use the **delete tap id** command to terminate the tap.

Parameters	Description
<number>	Identification number of particular tap to be configured which corresponds to tap entry in the table. Range: 1-99
address	Syslogd address where tap information is directed.
facility	Syslog facility where output is sent. See choices above. Default: log_auth
format	Text style in which tap output is formatted. Choices: Hexadecimal , ASCII or clear text.
loglevel	Syslog loglevel to which output is assigned. See choices above.

set tap user <name>

address <IP_address>
facility <log_auth | log_local0 | log_local1 | log_local2 | log_local3 | log_local4 | log_local5 | log_local6 | log_local7>
format <hex | ascii | clear>
loglevel <critical | unusual | common | verbose>
output <syslog>
port_tap <disabled | enabled>

Configures tap settings for the specified user as created by the **add tap user** command. Use the **delete tap id** command to terminate the tap.

Parameters	Description
address	The syslogd address where tap information is directed to.
facility	The syslog facility where output is sent. See choices above. Default: log_auth
format	The text style in which the tap output is formatted. Choices: Hexadecimal , ASCII or Clear text.
loglevel	The syslog loglevel to which output is assigned. See choices above.
output	Tap output is directed to a syslog host.
port_tap	Switch to turn tap on or off for the specified user: Enabled or Disabled .

set tcp keepalive_interval <period>

Configures a period of inactivity (in seconds) on a TCP session after which a TCP keep-alive packet is sent on the session to learn whether it is still active. The inactive period begins after this command is issued. This command is used in conjunction with the **enable tcp keepalive_interval** command. See **enable**, **disable tcp keepalive** and **show tcp settings** commands for more information. Range: **1-2147483** seconds. The enable/disable configuration is **disabled** by default.

set tcp maximum_connections <number>

Sets the total number of TCP connections HiPer ARC can support. TCP services include TELNET and ClearTCP. Range: **0-4096**.

set tftp request <input_file_name>

action <get | put>
max_timeout <1-300>
mode <ascii | octet>
rexmt_timeout <1-60>
server <IP_name_or_IP_address>

Configures requests to the TFTP server created with the **add tftp request** command. Entries placed in the TFTP Client Request Table are the names of files that are either requested *from* or sent *to* the TFTP server.

Parameters	Description
<input_file_name>	Designation of file to be requested from or sent to the TFTP server.
action	Type of request sent to the TFTP server. Choices: Put or Get
max_timeout	Interval in seconds HiPer ARC waits for a response from the TFTP server before the TFTP request is cancelled. Range: 1-300 . Default: 25 seconds
mode	The text format the file will be transmitted as. Choices: ascii or octet . Default: ASCII
rexmt_timeout	Retransmission timeout - interval in seconds HiPer ARC waits before retransmitting a TFTP request. Range: 1-60 . Default: 5 seconds
server	Name or IP address of the TFTP server.

set time <time>

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

set traceroute maximum_rows <number>

Sets a ceiling of traceroute entries in the Traceroute Table. Setting this value to a number smaller than the current number of rows will NOT cause any row deletions - but, the effect will be noted in future attempts at row creation. Range: **1-255**. Default: **20**. See **traceroute**, **list traceroute**, **delete traceroute**, and **show traceroute** commands for more information.

Set User Commands

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

set user <user_name>

alternate_phone_number [number]
chat_script_name [name]
expiration [date]
idle_timeout [interval]
input_filter [filter_name]
message [string]
modem_group [group_name]
output_filter [filter_name]
password [password]
phone_number [number]
port_limit [number]
session_timeout [seconds]
type [login,network,callback,dialout,manage]

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

Parameters	Description
<user_name>	Name of user, previously defined using add user. Limit: 64 ASCII characters.
alternate_phone_number	Number to dial if the first number is busy. Limit: 33 ASCII characters. <i>Note:</i> This value is overridden when a dialout script specified in the set dialout user command is issued.
chat_script_name	Designation of the Chat Script associated with this user. See add chat_script command for more.
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 (not activated). Range: 1 - 86400 seconds . <i>Note:</i> change the default to configure this value.
input_filter	Designation of the filter file in FLASH memory to be applied to the input datastream.

message	String to display to a dial-in user when connection is set. Limit: 64 ASCII characters You can use \$value to stipulate more parameters in the message line for identification purposes. <ul style="list-style-type: none"> ■ \$date - current date according to system uptime ■ \$callid - user's call identification according to system uptime ■ \$port - port occupied by user (slot:x/mod:y) ■ \$hostname - user's host name ■ \$sysname - user's system name (same as hostname) ■ \$time - time of call according to system uptime <i>Note:</i> The message, if it includes spaces, must be enclosed in quotations. Use the show user command to view the message as configured. See <i>Chapter 9: Administrative Tools</i> for more.
modem_group	Name of modem group used to make connection to this <i>dial-out</i> user. <i>Important:</i> This value does not apply to a <i>dial-in</i> user.
output_filter	Name of the filter file in FLASH memory to be applied to the output datastream.
password	User's password (optional). Limit: 127 ASCII characters. You may enter a null password with: <i>password ""</i> .
phone_number	Primary phone number to make the connection. Limit: 33 ASCII characters. <i>Note:</i> This value is overridden when a dialout script specified in the set dialout user command is issued.
port_limit	The maximum number of dialin ports a local user can concurrently employ. This setting <i>does not apply</i> to TELNET users logged in through the Ethernet interfaces nor to remote users (RADIUS authenticated) who are assigned this value by the associated RADIUS server. Range: 1-475
session_timeout	Interval before timing out a session. Default: 0 (no setting)
type	Type of user added. A user may be one or more types but callback and dialout are mutually exclusive. <ul style="list-style-type: none"> ■ 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 dialout user <user_name>

```

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

```

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

- **Dialout sites** - user dials out to a remote location and is connected or prompted for a login.
- **Dialin/dialout** - user dials in to HiPer ARC, then dials out to a remote site and is connected.
- **TELNET/dialout** - user telnets into HiPer ARC then dials out to a remote site and is connected as a *shared_modem* user.

Script strings are limited to **240** characters which must be enclosed in **double quotes** if exceeding **64 ASCII** characters.

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

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

set dialout user <user name> site

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

Sets parameters for dialout users connecting to a remote network.

Parameters	Description
<user name>	Name user, previously defined using <i>add user</i> with dialout as the type.
address_selection	Determines how the IP address will be assigned for incoming (client) IP network connections. <ul style="list-style-type: none"> ▀ Negotiate - brokers IP address between remote client and local user. ▀ Assign - chooses address from IP pool, configured using <i>set ip system</i>. Default ▀ Specified - <i>must</i> use IP address set in <i>remote_IP_address</i> value.
default_route_option	Automatically sets the IP address of a remote default router by <i>negotiation</i> . This parameter takes precedence over a default route (gateway) set by add framed_route user or add ip defaultroute commands, which require <i>manual</i> IP address entry. Default: Disable
end_time	For a TIMED user, specifies when to tear down connection. Seconds field is optional.
ip	Determines if this connection supports IP or not. Default: Enable
ipx	Determines whether this connection supports IPX or not.
ipx_address	The address of the remote network.
remote_IP_address/ mask_specifier	For a remote IP connection, the IP network address assigned to the client, in the format <i>nnn.nnn.nnn.nnn</i> , with or without a mask specifier. The mask specifier can be in IP address format (<i>255.0.0.0</i> or greater and contiguous) or 'A', 'B', 'C', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If setting a user's IP address, the mask specifier is set to 'H' (for Host) or a numeric value of 32 . If you don't specify a mask, the system will generate it for you from the network address. Default: 0.0.0.0/H
send_password	Password sent to remote network. <i>Note:</i> passwords you defined with other commands are for dial-in users. Limit: 63 ASCII characters.
spoofing	Specifies spoofing across the remote connection, to save overhead on the dial-out line's connection. Default: Disable
start_time	Period to start a TIMED connection. Seconds field is optional.

type	Describes what type of dial out connection this is: <ul style="list-style-type: none"> ▫ Ondemand - makes connection when the system seeks a session with the remote network. ▫ Timed - makes connection at a set time ▫ Continuous - always keeps connection up ▫ manual - starts connection manually with CLI. Default
------	--

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

Specifies a framed (static) network to the user profile for dialup connections. See also **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. Range: 1-15 .

set login user <user name>
 host_type [prompt | select | specified]
 login_host_ip_address [IP_ name or address]
 login_host_name [IP_ name or address]
 login_service [rlogin | telnet | cleartcp | ping]
 tcp_port [number]
 terminal_type [string]

Sets parameters for users whose type is LOGIN.

Parameters	Description
<user name>	User to set parameters for, earlier defined using add user with login as type. Limit: 64 ASCII characters.
host_type	Options are: <ul style="list-style-type: none"> ▫ 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 <i>login_host_ip_address</i> of this command.
login_host_IP_address	IP address or host name of the remote host.
login_host_name	Designation of of host to be resolved at time of connection.
login_service	Service used to login to the remote host. Choices: <ul style="list-style-type: none"> ▫ Rlogin ▫ Telnet. <i>Default</i> ▫ ClearTCP ▫ Ping - user pings a login host, receives a successful/unsuccessful message and is disconnected.
tcp_port	TCP Port number the remote host expects this login to use. Limit: 65535
terminal_type	Terminal type used for the remote connection, e.g. VT100. Limit: 64 ASCII characters

set network user <name>

header_compression [none | tcpip]
mtu [number]
multicast_proxy [enabled | disabled]
network_service [ppp | slip]
send_password [user_password]
spoofing [enable | disable]

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

header_compression	Sets TCP/IP compression or no header compression. Default: TCPIP
mtu	Maximum Transfer Unit - largest data packet size (bytes) allowed. Default: 1514 . Range: 64-8192
multicast_proxy	Reports WAN-attached IGMP clients to HiPer ARC's Ethernet interface, or vice versa: Enabled or Disabled . Default: Disabled
network_service	Type of network service. Default: PPP
send_password	Password sent to the remote network. Limit: 15 ASCII characters.
spoofing	Spoofing across remote connect to save overhead on dial-out line. Default: Disabled .

set network user <user name> **igmp**

max_response_time [1-10]
multicast_forwarding [enabled | disabled]
multicast_proxy [enabled | disabled]
query_interval [5-65535]
robustness [1-5]
routing [enabled | disabled]
version [1,2]

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

Parameters	Description
max_response_time	The interval a host has to respond to the IGMP query. Default: 10 . Range: 1-10 seconds
multicast_forwarding	Multicast packets are forwarded when enabled. Default: Disabled
multicast_proxy	Multicast addresses that are joined or learned on the specified interface are joined on the proxy interface that is configured with the set ip multicast proxy interface command. Default: Disabled
query_interval	The frequency at which IGMP Host-Query messages are sent on the specified interface. Default: 125 . Range: 5-65535
robustness	Tuning parameter for expected packet loss on a subnet. If packet loss on a subnet is expected to be high, robustness may be increased. Range: 1-5 . Default: 2
routing	Will attempt to become the IGMP querier on this interface. Default: Disabled
version	The version of IGMP running on this interface. This object can be used to configure a router capable of running either version. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. Default: 2

set network user <name> **ip**

address_selection [negotiate | assign | specified]
default_route_option [enable | disable]
remote_ip_address [IP_name or network address/mask_specifier]
rip [ripv1 | ripv2]
rip_authentication_key [string]
rip_policies_update [rip policies]
routing [listen | send | both | none]
usage [enable | disable]

Specifies parameters for IP users whose *type* is network. Routing for network users is host-based, so the subnet specified by the *remote_ip_address* parameter is a 32-bit mask, supplied either by the administrator or automatically, by HiPer ARC.

Note: Administrators creating RADIUS users should consult *Appendix E: RADIUS and TACACS+ Systems* for more information.

Important: *Negotiate* address selection does not support SLIP. Also, if using routing, you must turn it on since the default is *none*.

Parameters	Description
<user name>	User, who must have network as the type.
address_selection	Determines how IP address will be assigned for incoming (client) IP network connections. <ul style="list-style-type: none"> ▪ Negotiate - brokers IP address between remote client and local user. Note: Not available with SLIP. ▪ Assign - chooses address from IP pool, configured using set ip system. Default. ▪ Specified - <i>must</i> use IP address set in remote_IP_address value.
default_route_option	Automatically sets the IP address of a remote default router by <i>negotiation</i> . This parameter takes precedence over a default route (gateway) set by add framed_route user or add ip defaultroute commands, which require <i>manual</i> IP address entry. Default: Disable
remote_IP_address/ mask_specifier	For a remote IP connection, the IP network address assigned to the client, in the format <i>nnn.nnn.nnn.nnn</i> , with or without a mask specifier. The mask specifier can be in IP address format (255.0.0.0 or greater and contiguous) or 'A', 'B', 'C', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If setting a user's IP address, the mask specifier can also be 'H' (for Host) or a numeric value of 32 . If you don't specify a mask, the system will generate it for you from the network address. Default: 0.0.0.0/H
rip	Selects either RIPv1 or RIPv2. Default: RIPv1
rip_authentication_key	Authorizes RIP updates using a stored password. Maximum string length: 64 ASCII characters.
rip_policies_update	Allows user to enable or disable RIP policies. See 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) . <i>Note:</i> For Poison Reverse to work properly, Split Horizon must also be enabled. SEND_DEFAULT/NO_SEND_DEFAULT(D) SEND_ROUTES(D)/NO_SEND_ROUTES SEND_SUBNETS/NO_SEND_SUBNETS(D) ACCEPT_DEFAULT/NO_ACCEPT_DEFAULT(D) SPLIT_HORIZON(D)/NO_SPLIT_HORIZON POISON_REVERSE(D)/NO_POISON_REVERSE FLASH_UPDATE(D)/NO_FLASH_UPDATE SEND_COMPAT(D)/NO_RIPV1_SEND RIPV1_RECEIVE(D)/NO_RIPV1_RECEIVE RIPV2_RECEIVE(D)/NO_RIPV2_RECEIVE SILENT (default is disabled)
routing	Sets routing type (RIP packets) accepted on this connection. The choices: <ul style="list-style-type: none"> ▪ Listen - detects packets destined for system's networks ▪ Send - routes packets destined for the remote network ▪ Both - both listens and sends ▪ None - ignores all routing packets. Default.
usage	Sets interface to enable/disable IP protocol. Default: Enable

set network user <user name> ipx

address [ipx network address]
rip_age_multiplier [interval]
rip_update [interval]
routing [all | listen | respond | send | none]
sap_age_multiplier [interval]
sap_update [interval]
usage [enable | disable]
wan [enable | disable]

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

Parameters	Description
address	IPX address of the remote network. When configuring for an unnumbered IPX network, set this value to <i>ffffffc</i> . Default: 00000000
rip_age_multiplier	Sets holding multiplier for data received in RIP periodic updates. Default: 3
rip_update	Sets interval, in seconds, between RIP periodic updates. Default: 60 seconds
routing	Sets type of IPX RIP and SAP packets to accept on this connection. <ul style="list-style-type: none"> ▫ Listen - detects RIP/SAP packets headed for system's networks ▫ Send - routes packets destined for remote network ▫ Respond - if requested, will respond with IPX RIP or SAP data. Default ▫ All - Detects, sends, responds with RIP/SAP packets ▫ None - ignores all routing packets
sap_age_multiplier	Sets holding multiplier for data received in SAP periodic updates. Default: 3
sap_update	Sets interval, in seconds, between SAP periodic updates. Default: 60 seconds
usage	Sets interface to enable/disable IPX protocol. Default: Enabled
wan	Protocol used between two IPX networks negotiating the IPX network number for a WAN connection. Both ends of the connection must enable this protocol for it to work. Default: Disabled

set network user <user name> ppp

channel_decrement [percent]
channel_expansion [percent]
compression_algorithm [ascend | auto | microsoft | none | stac]
encryption_algorithm [none | auto | microsoft_40bit | microsoft_128bit | required]
expansion_algorithm [constant | linear]
max_channels [number]
min_size_compression [number]
primary_dns_server <ip_dns_address>
receive_acc_map [hex_number]
reset_mode_compression [auto | every_packet | every_error]
secondary_dns_server <ip_dns_address>
transmit_acc_map [hex_number]

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

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

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

Parameters	Description
<user name>	Name user, previously defined using add user with network as the type.
channel_decrement	When line usage on the second channel drops below this percentage, PPP drops the second (QUAD) or more (HDM only) channels. Default: 0 . Recommended: 20 . Range: 1-100%
channel_expansion	When the line usage of the first channel exceeds this percentage, PPP adds the second (QUAD) or more channels (HDM: up to 16). Specifying 100% disables the second and additional channels for multilink PPP. Default: 0 . Recommended: 60 . Range: 1-100%

compression_algorithm	Specifies the proprietary compression algorithm PPP uses via negotiation. Choices are: ASCEND , MICROSOFT , STAC and NONE . Default: AUTO . <i>Note:</i> This value can be <i>overridden</i> by using the set ppp ccp_modemtype [digital,compressed_analog, uncompressed_analog,none,all] command. If you know the type of traffic your connection will bear, using this command is beneficial.
encryption_algorithm	Type of encryption algorithm to employ for this user. Choices: <ul style="list-style-type: none"> None - no encryption used on this link. Auto - attempt to negotiate all encryption algorithms is made, but if none are successful, the link remains up. Microsoft_40bit - only 40-bit MPPE (Microsoft Point-to-Point Encryption) is used, if not available, the link fails. Microsoft_128bit - only 128-bit MPPE is used, if not available, the link fails. Required - either 40-bit or 128-bit MPPE is used (128-bit first), if neither is available, the link fails.
expansion_algorithm	Specifies which type of expansion algorithm to handle bandwidth allocation. <ul style="list-style-type: none"> CONSTANT - A long-term measurement and allocation of traffic bandwidth best for constant datastreams, such as file transfer. Default LINEAR - A short-term measurement and allocation of traffic bandwidth, best for bursty traffic, such as interactive users.
max_channels	Sets how many channels to use for multi-link PPP (MLPPP). This value either invokes PPP to negotiate for MLPPP with the remote system (more than 1) or does not try to negotiate for MLPPP (1). The actual number of channels used is determined by channel_decrement and expansion parameters. MLPPP is on by default with a value of 2 . <i>Note:</i> To ensure that MLPPP is running on both ends of a connection, do not lower the default value of 2 otherwise MLPPP may fail. For HDM cards only, you may set up to 16 channels.
min_size_compression	Data packet size that PPP decides is big enough to start compression. Data packets smaller than that will not be compressed. Range: 0-2048 bytes . Default: 256
primary_dns_server	The first-in-line DNS server chosen to resolve names or addresses for this user.
receive_acc_map	Determines whether the system will use the asynchronous control character map to filter out incoming data. Default: FFFFFFF
reset_mode_compression	Determines how often PPP examines packets to decide when to renegotiate the optimum compression algorithm. Default: AUTO
secondary_dns_server	The second-in-line DNS server chosen to resolve names or addresses for this user.
transmit_acc_map	Determines whether the system will use the asynchronous control character map to filter out outgoing data. Default: FFFFFFF

set tunnel user <user_name>**client_endpoint** <string>**group** <string>**medium_type** <ipv4>**password** <user_password>**security** <none | control_only | data_only | both_data_and_control>**server_endpoint** <string>**type** <none | pptp | l2tp>

Configures parameters for local users employing tunneling via L2TP, PPTP or other protocols. Authentication is performed using a Message Integrity Check (MIC) which is added to each packet generated from the shared secret (password or key). This key is renegotiated often between server/client peers. An additional degree of security is available for control, data or data and control packets.

Parameters	Description
<user_name>	Name of the user, previously defined using the add user command. Limit: 64 ASCII characters.

type	The tunneling protocol this user will employ. Choices: <ul style="list-style-type: none"> ■ none - No tunneling specified ■ pptp - Point-To-Point Tunneling Protocol - Microsoft's tunneling protocol. Default ■ l2tp - Layer 2 Tunneling Protocol
medium_type	The transport layer of the tunnel medium used when creating tunnels. Choices: <ul style="list-style-type: none"> ■ ipv4 - <i>Default</i>
client_endpoint	The IP address of the initiator-end of the tunnel. Limit: 64 ASCII characters
server_endpoint	The IP address of the server-end of the tunnel. Limit: 64 ASCII characters.
password	The shared secret between tunnel server and client. Limit: 63 ASCII characters.
group	Group ID of the tunneled session. Limit: 64 ASCII characters.
security	Additional degree of security to perform on control or data packets for this tunnel. Choices: none , control-only , data-only , or both-data-and-control .

Show all Commands

Display all parameters for *all entries* in tables associated with particular commands. See individual **show** commands to display all parameters of a *single table entry* or **list** commands to display a *limited number of parameters for all entries* in a table. The commands include:

show all aaa_servers
show all active interfaces
show all filters
show all interfaces
show all ip networks
show all ipx networks
show all l2tp tunnels
show all lan interfaces
show all networks
show all sessions
show all switched interfaces
show all users

Show Commands

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

show aaa_server <name>
 preference <1-10>

Displays the settings of the specified TACACS+ server you configured with the **add aaa_server** command. It lists:

- **IP Address** - IP address of the AAA server. Default: **0.0.0.0**
- **State** - Switch to turn AAA server on or off. Default: **ENABLED**
- **Encryption** - Enables/disables encryption of entire data packet. Default: **Off**
- **Passthru** - When the last AAA server's Passthru is enabled, HiPer ARC allows users access even if authentication has failed for all servers in that domain. This value is used in conjunction with directed request. Default: **Disabled**
- **Port** - Port number on the AAA server. TACACS+ standard port number: **49**. Range: **1-65,535**

- **Preference** - Priority ranking of domains that specifies how servers are chosen. Highest preference - **1**, lowest: **10**. Range: **1-10**
- **Server Name** - Familial name for the AAA server to be identified by DNS. Limit: **64** ASCII characters.

For example:

INFORMATION FOR AAA NAME: aaa

Preference:	1
IP address:	149.112.189.18
Server Name:	
Port:	49
Pass Through:	DISABLED
State:	ENABLED
Encryption:	OFF

show aaa_server <name>
preference <1-10> **settings**

See command described above. The commands are similar.

show accounting or **show accounting settings**

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

ACCOUNTING SETTINGS:

- **Primary Server Status** - current status of primary RADIUS server. Default: *Enabled*
- **Primary Server** - IP address of the primary RADIUS server
- **Primary First Backup Server** - IP address of the primary RADIUS first backup server
- **Primary Second Backup Server** - IP address of the primary RADIUS second backup server
- **Primary Destination Port** - Destination port of the RADIUS primary server
- **Primary First Backup Destination Port** - Destination port of the primary RADIUS first backup server
- **Primary Second Backup Destination Port** - Destination port of the primary RADIUS second backup server
- **Secondary Server Status** - current status of secondary RADIUS server. Default: *Enabled*
- **Secondary Server** - IP address of the secondary RADIUS server
- **Secondary First Backup Server** - IP address of the secondary RADIUS first backup serve
- **Secondary Second Backup Server** - IP address of the secondary RADIUS second backup server
- **Secondary Destination Port** - Destination port of the RADIUS secondary server
- **Secondary First Backup Destination Port** - Destination port of the secondary RADIUS first backup server
- **Secondary Second Backup Destination Port** - Destination port of the secondary RADIUS second backup server
- **Source Port** - RADIUS accounting port - Default: *1813*
- **Retransmission Timeout** - number of seconds between retransmissions. Default: *5*
- **Accounting Start Time** - the point at which accounting was begun by the **enable accounting** command.

- **Log Unauthenticated Calls** - current state of feature which logs calls failing prior to authentication.
Default: *True*
- **Active Accounting Server (Primary)** - primary server currently in use for accounting
- **Active Accounting Server (Secondary)** - secondary server currently in use for accounting

ACCOUNTING SETTINGS:

The Primary Server Status is:	ENABLED
Primary Server is:	134.125.211.9
Primary First Backup Server is:	0.0.0.0
Primary Second Backup Server is:	0.0.0.0
Primary Destination Port is:	1646
Primary First Backup Destination Port:	1813
Primary Second Backup Destination Port:	1813
The Secondary Server Status is:	ENABLED
Secondary Server is:	0.0.0.0
Secondary First Backup Server is:	0.0.0.0
Secondary Second Backup Server is:	0.0.0.0
Secondary Destination Port is:	1646
Secondary First Backup Destination Port:	1813
Secondary Second Backup Destination Port:	1813
Source Port is:	1813
Retransmission Timeout:	5
Accounting Start Time:	CONNECTION
Log Unauthenticated Calls	TRUE
Active Accounting Server (Primary):	149.112.113.213
Active Accounting Server (Secondary):	0.0.0.0

show accounting counters

Displays statistics stored by RADIUS accounting servers.

- **Number Of Local Users** - number of LAN users RADIUS is tracking
- **Number of Active Users** - sum of users RADIUS is tracking
- **UDP Packets Received** - number of packets received from RADIUS
- **UDP Packets Retransmitted** - number of packets sent to RADIUS
- **Round Robin switching count** - number of times servers are switched in each server group
- **Percent Queue Full** - Portion of the queue filled in each server group
- **Number of Packets Outstanding** - sum of packets left by each server group
- **Number of Packets Discarded** - sum of packets thrown away by each server group

ACCOUNTING COUNTERS:

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

PRIMARY SERVER GROUP COUNTERS

Round Robin switching count:	1
Percent Queue Full:	0
Number of Packets Outstanding	0

ACCOUNTING COUNTERS:	
Number of Packets Discarded:	0
SECONDARY SERVER GROUP COUNTERS	
Round Robin switching count:	0
Percent Queue Full:	0
Number of Packets Outstanding:	0
Number of Packets Discarded:	0

show atm1483 pvc <name> or show atm1483 pvc <name> settings

Displays a specified Permanent Virtual Circuit (PVC) you created for RFC-1483 compliant networks with the **add atm1483 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*. The command lists:

ATM 1483 PVC pvc_0_48 SETTINGS	
VPI	0
VCI	48
Network Name:	atm
Protocol	IP
Network address:	204.249.183.47
Interface:	atmaal:1
Peak Cell Rate:	100000
Status:	ENABLED

show atm1577 pvc <name> or show atm1577 pvc <name> settings

Displays a specified Permanent Virtual Circuit (PVC) you created for RFC-1577 compliant networks with the **add atm1577 pvc** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*.

ATM 1577 PVC atm1577pvc SETTINGS	
VPI	0
VCI	110
Network Name:	ip_atm1577
Interface:	atmaal:1
Peak Cell Rate:	100000
Status:	ENA

show atm_arp_server <name>

Displays settings for the particular ATM ARP server you configured with the **add atm_arp_server** command. The ATM ARP server maps IP addresses of connected servers to 20-byte ATM addresses. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*. It lists:

ATM ARP SERVER arp_server1 SETTINGS	
ATM address:	11.22.33.44.55.66.77.88.99.00.1122.33.44.55.66.77.88.99.00
Subnet address:	204.249.180.4
Interface:	atmnet:1
State:	ENABLE

show atmcfg <atmaal:1 | atmaal:2>

Displays the configuration for ATM interfaces (AAL) you set with the **enable ilmi** and **enable atmsig** commands. For more configuration information, see the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*. The commands lists:

- **ATM Configuration** - The specified ATM setting: **Signalling** and **ILMI**
- **Admin(istrative) Status** - whether the administrator has enabled or disabled the setting
- **Oper(ating) Status** - current state of the setting

ATM Configuration	Admin Status	Oper Status
Signalling:	ENABLED	ENABLED
ILMI:	ENABLED	ENABLED

show atm counters <ds3:x | e3:x | atmcell:x>

Displays statistics for all ATM interfaces. It lists:

DSX3 COUNTERS					
Receive Cells:					1890
Transmit Cells:					45284685
Elapsed Time:					702
Current Unavailable Seconds					0
Current Line Errored Seconds:					0
Current Line Code Violations:					0
Valid Intervals:					0
Interval Unavailable Seconds:					0
Interval Line Errored Seconds:					0
Interval Code Violations:					0
Total Unavailable Seconds:					0
Total Line Errored Seconds:					0
Total Code Violations:					0
DSX3 ALARMS					
RxRAI	TxRAI	RxAIS	TxAIS	LOF	LOS
OK	OK	OK	OK	OK	OK
CELL COUNTERS					
RX Cells:					1839
RX HEC Errors:					0
RX Unknown Protos:					0
TX Cells:					1816
TX Errors:					0

show authentication or **show authentication settings**

Displays the RADIUS and local user authentication settings, which you can modify using the **set authentication** command.

- **Local Authentication is** - Enabled (*default*)/Disabled
- **RADIUS Authentication is** - Enabled (*default*)/Disabled
- **Hint Assigned is** - whether IP address is assigned optionally by remote server. Enabled/Disabled (*default*)
- **Primary Server is** - IP address of the primary RADIUS server
- **Primary Destination Port is** - port number of the primary server. Default: **1645**

- **Secondary Server is** - IP address of the secondary RADIUS server
- **Secondary Destination Port is** - port number of the secondary server. Default: **1645**
- **Tertiary Server is** - IP address of the secondary RADIUS server
- **Tertiary Destination Port is** - port number of the secondary server. Default: **1812**
- **Source Port is** - port number of the source server. Default: **1812**
- **Retransmission Timeout** - interval between retransmissions. Default: **3 seconds**
- **Max Retranmissions** - number of retransmissions before failure reported. Default: **10 seconds**
- **Active Authentication Server** - the server currently in use for authentication

AUTHENTICATION SETTINGS

Local Authentication is	ENABLED
RADIUS Authentication is:	ENABLED
Hint Assigned is:	DISABLED
Primary Server is	122.122.122.134
Primary Destination Port is	1645
Secondary Server is:	0.0.0.0
Secondary Destination Port is:	1645
Tertiary Server is:	0.0.0.0
Tertiary Destination Port is:	1812
Source Port is:	1812
Retransmission Timeout:	3
Max Retranmissions:	10
Active Authentication Server:	134.145.213.21

show authentication counters

Displays the RADIUS and local user authentication counters.

- **Local Successful Authentications** - number of times user/password pair matched
- **Local Failed Authentications** - number of times user/password pair didn't match
- **Remote Primary Successful Authentications** - number of times RADIUS OK'd user on this server
- **Remote Primary Failed Authentications** - number of times RADIUS rejected user on this server
- **Remote Secondary Successful Authentications** - number of times RADIUS OK'd user on this server
- **Remote Secondary Failed Authentications** - number of times RADIUS rejected user on this server
- **Remote Tertiary Successful Authentications** - number of times RADIUS OK'd user on this server
- **Remote Tertiary Failed Authentications** - number of times RADIUS rejected user on this server
- **Remote Primary No Responses** - number of times RADIUS failed to answer an authentication request (with an error message) on this server
- **Remote Secondary No Responses** - number of times RADIUS failed to answer an authentication request (with an error message) on this server
- **Remote Tertiary No Responses** - number of times RADIUS failed to answer an authentication request (with an error message) on this server

AUTHENTICATION COUNTER

Local Successful Authentications	5
Local Failed Authentications	0

AUTHENTICATION COUNTER

Remote Primary Successful Authentications:	5
Remote Primary Failed Authentications	0
Remote Secondary Successful Authentications:	5
Remote Secondary Failed Authentications	0
Remote Tertiary Successful Authentications:	
Remote Tertiary Failed Authentications	0
Remote Primary No Responses:	1
Remote Secondary No Responses:	10
Remote Tertiary No Responses:	0

show authorization or **show authorization settings**

Displays whether TACACS+ remote authorization is **ENABLED** or **DISABLED**. Issue the **enable** or **disable authorization** command to change the present setting.

TACACS AUTHORIZATION SETTINGS

Remote Authorization is: **ENABLED**

show board command_line_parameters

Displays command line arguments used at boot time which you configured with the **set board command_line_parameters** command. For example:

Command Line Parameters: (null)

show board crashdump

A diagnostic tool for displaying information about a previous system crash stored in EEPROM. This is useful for debugging purposes only. Information shown includes the HiPer ARC version number, general purpose and other registers, and call stacks.

EXCEPTION 0300 CRASH DUMP (mm-dd-yy : 04-29-1998 hr-min-sec : 20-09-13)

AppVer: 4.0.29-24 KernVer: 0x00000028

GPRs:

R0: 0x2C4E20	R1: 0x01FAFCB8	R2: 0x000B0AE	R0x01B259CC
R4: 0x00000004	R5: 0x94003B7D	R6: 0x000017	R7: 0x01B4BA0C
R8: 0x01B4828C	R9: 0x01B395CC	R10: 0x4C000064	R11: 0x00000008
R12: 0x000001	R13: 0x000B8C7C	R14: 0x00000000	R15: 0x0045007C
R16: 0x0045005C	R17: 0x002710	R18: 0x00450068	R19: 0x00450054
R20: 0x00450040	R21: 0x00450048	R22: 0x00450058	R23: 0x00739EF8
R24: 0x000001	R25: 0x00000DF6	R26: 0x0045004C	R27: 0x002710
R28: 0x01C78D4C	R29: 0x01C78D88	R30: 0x00000004	R31: 0x01B259CC

CR: 0x84000000	XER: 0x20000004	LR: 0x2C3214	CTR: 0x2C06A0
SRR0: 0x2C322C	SRR1: 0x0000B93	DSISR: 0x04000000	DAR: 0x94003B7D

82660 Registers:

Err Status 1: 0x00, Err Status 2: 0x00, CPU Err: 0x14, PCI Err: 0x06
CPU/PCI address: 0x00054DFC, Sys Error address: 0x0005E940

Call Stack:

0x2C322C (Exception return address - SRR0)

EXCEPTION 0300 CRASH DUMP (mm-dd-yy : 04-29-1998 hr-min-sec : 20-09-13)

```
0x2C3214
0x2C4E20
0x2C7E8C
0x2C80B4
0x2BB4DC
0x003E8CFC
0x003E8E94
0x2007E8
0x2100
0x200034
```

show board settings

Displays information about the HiPer ARC hardware. For example:

```
Product Code:          03E800
Hardware Version:      00.109
Kernel Version:       0x00000028
Software Version:     V4.1.5
Serial Number:        2F746D70
Feature Key:          6973635F
Total System Memory:  56462 KB
CPU Type:             PPC 603E
CPU Speed (Mhz):      225
NIC Card ID:          19
NIC Card Name:        Dual DEC42 10/100 Ethernet
NAC Card ID:          12146
NAC Card Name:        HiPer Access Router NAC
```

DIP Switch Settings:

1	2	3	4	5	6	7	8	9	10
ON	ON	OFF	OFF	OFF	OFF	OFF	OFF	XXX	OFF

```
SW 1-2:  UI baud rate          115200
SW 3:    Engineering Fastboot: DISABLED
SW 4:    Autoload application:  ENABLED
SW 5:    UI Require Carrier:    ENABLED
SW 6:    L1 Data Cache:         ENABLED
SW 7:    L1 Instruction Cache:  ENABLED
SW 8:    L2 Cache:              ENABLED
SW 9:    Eng. Watchdog Disable: (CANNOT BE READ)
SW 10::  Manufacturing Test:    DISABLED
```

show bootrom ip interface <eth:x>

Displays IP boot configurations for the Ethernet interface (*eth:1* or *eth:2*). For example:

```
IP address:      122.212.214.70
IP Gateway:      122.212.214.254
TFTP Server:     122.212.213.1
IP Netmask       255.255.255.0
```

```
IP address:          122.212.214.70
TFTP Download:       NEVER
Load File Name:
Crashdump File Name:
```

show bootrom settings

Displays general boot configuration. For example:

```
Boot Mode:          FLASH
IP Configuration Source:  STATIC
Crash Upload:       DISABLED
Boot Interface:     eth:1
```

show bulk_file

Displays the name of the HiPer ARC bulk configuration file and any error associated with the file. This binary file is a concatenation of individual HiPer ARC configuration files (.CFG) used to upload to HiPer ARC. For example:

```
Bulk Configuration File Name:  ConfigBulkFile
Bulk Configuration Error:
```

show chassis slot <slot#> or show chassis slot <slot#> settings

Displays basic board information by slot number (1-16) in the chassis. For example:

```
CHASSIS SLOT 3 SETTINGS
Owner:          YES
Description:     Quad Anal-Digi V.34 Modem
Number of Ports: 4
Type:           DYNAMIC
```

show chat_script <name>

Displays the entire chat script file you added to the Chat Script table. For more information, see the **add**, **delete**, **verify** and **list chat_scripts** commands. Also, see *Appendix E: RADIUS and TACACS+ Systems*. It lists:

```
TIMEOUT 60;
begin:
  SEND "Enter Remote Host Name:";
  EXPECT %login_host;
  IF ($login_host == "abc.com") GOTO telnet;
  IF ($login_host == "def.com") GOTO telnet;
  IF ($login_host == "logout") GOTO exit;
  SEND "Invalid choice";
  GOTO begin;
telnet:
  TELNET $login_host;
exit:
  HANGUP
```

show clearTCP or show clearTCP settings

Displays the ClearTCP message (Default: **Connected**) when a ClearTCP client session is connected to the remote TCP host. It can be modified using the **set clearTCP connect_message** command. For example:

```
CLEARTCP SETTINGS
ClearTCP Connection Message::  Connected
```

show command or **show command settings**

Displays the settings for CLI commands. See **set command** to modify settings. Prompts can hold a maximum of 64 ASCII characters. It lists:

- **History depth** - Number of CLI commands issued by HiPer ARC which will display when pressing the up or down arrow keys
- **Current prompt** - Designation of prompt for a temporary CLI session
- **Local prompt** - Designation of prompt for a permanent CLI session
- **Console login required** - Whether login to the console is required
- **Console idle timeout** - Interval before a console session is timed out
- **Global terminal page break** - Whether global terminal page breaks are enabled or disabled
- **Global terminal settings rows** - Number of rows displayed to all HiPer ARC-connected systems
- **Local terminal page break** - Whether local terminal page breaks are enabled or disabled
- **Local terminal settings rows** - Number of rows displayed to locally-connected systems

History Depth:	10
Current Prompt:	HiPer>>
Local Prompt	HiPer>>
Console Login Required:	NO
Console Idle Timeout:	5
Currant Idle Timeout:	0
Global Terminal Page-break	ENABLED
Global Terminal Settings Rows	23
Local Terminal Page-break	DISABLED
Local Terminal Settings Rows	50

show configuration or **show configuration settings**

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

CONFIGURATION SETTINGS**System Identification:**

Name: HiperARC

Contact: Larry Cortese

RADIUS Authentication Remote: ENABLED Local: ENABLED

Primary Server: 166.165.166.139

Secondary Server: 0.0.0.0

Remote Accounting: ENABLED

Primary Server: 166.165.166.139

Secondary Server: 0.0.0.0

Interfaces:

eth:

slot:3/mod:1

slot:3/mod:1

internal

loopback

eth:

slot:3/mod:1

:slot:3/mod:1

CONFIGURATION SETTINGS

IP Forwarding: ENABLED	Routing: Enabled	RIP: ENABLED
ipnet	ETHERNET_II	eth:1
IP-loopback	LOOPBACK	loopback
		166.165.166.145/1
		127.0.0.1/A
IPX Default Gateway: 00000000	Maximum Hops: 15	
Dynamic Pool Beginning address:	000011	Members: 16
Networks:		
ipxnet	Ethernet_II	eth:1 10
PPP Receive Authentication: ANY		
Datalinks:		
8	Opened	
DNS Domain: hiyall-usr.com		
1	154.222.145.234	
camus	157.123.122.177	
scylla	157.123.122.158	
charybdis	157.123.122.149	

show connection or **show connection settings**

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

- **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

CONNECTION SETTINGS

Host Selection Method:	ROUND-ROBIN
Global User Name:	default
Service Prompt:	Login/Network User:
Message Prompt:	manage:

show connection counters

Displays the counters kept for dial-in connections.

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

COUNTER FOR CONNECTIONS

Number of Calls:	1
-------------------------	----------

show cpu utilization

Displays an estimate of HiPer ARC's CPU usage over various intervals. HiPer ARC utilizes excess processing power to lower system throughput latency. The CPU utilization values displayed are derived from an estimate of how quickly HiPer ARC polls under load versus the polling rate of HiPer ARC not under load.

If HiPer ARC were not running for the respective time period, the CPU percentage would be represented as 0%. The command lists:

CPU Utilization:

Instantaneous:	5%
Last Minute:	0%
Last Hour:	0%
Last Day:	0%

show critical_event or show critical_event settings

Displays where the log files for critical event messages are stored in FLASH memory. It lists:

- **Critical Event Sink** - where critical events are logged, default is @file:./log-file.local
- **Critical Event Backup** - where critical events are logged, if the first destination fails. Default: @file:./old-log-file.local
- **Critical Event Logging To Flash** - indicates whether logging of all critical errors into all sinks and FLASH is **ENABLED** or **DISABLED**.

System Date:	13-JUL-2041 19:25:11
System UpTime:	0d 00:12:30
Show Critical Event Logging To Flash:	DISABLED

show cross_connect <name>

Displays the specified ATM cross-connection for Virtual Path Indicators (VPI) and Virtual Channel Indicators (VCI) you configured with the **add cross_connect** command. For more configuration information, see Chapter 4: Configuring the DS3 Interfaces in the *Dual DS3 Asynchronous Transfer Mode (ATM) NIC Getting Started Guide*. The command lists:

CROSS CONNECT connect_0_100 SETTINGS

Port1:	1
VPI1:	0
VCI1:	700
Port2:	2
VPI2:	0
VCI2:	900
Peak Cell Rate:	100000
Oper Status Low->High	UP
Oper Status High->Low	UP
Cross Connect Row Status:	ENABLE
Cross Connect Admin Status:	UP

show date

Displays the system *date*, *time*, and *uptime*. The time is expressed in Greenwich Mean Time (GMT). For example:

System Date (Time in GMT)	13-JUL-2041 19:25:11
System UpTime:	0d 00:12:30

show default_global_call_type settings

Displays configuration for a HiPer ARC placing L2TP or PPTP (or NONE) calls only. See the **set global_call_type** command. Default: **None**. For example:

GLOBAL DEFAULT CALLTYPE	PPTP
-------------------------	------

show dialout or **show dialout settings**

Displays the current settings for the dialout server. You can modify the settings using the **set dialout** command.

DIALOUT SETTINGS

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

show direct_request

Displays all directed requests issued by TACACS+ as set by the **set direct_request** command. For example:

DIRECT REQUEST SETTINGS

The Delimiter:	@#%
The Timeout:	5
Status is:	Disabled

show dns or **show dns settings**

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

- **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
- **Cache Max TTL** - Maximum Time-To-Live period in seconds for resource records in this cache
- **Negative Cache Max TTL** - Maximum Time-To-Live period in seconds for negative cached authoritative errors
- **Caching** - Indicates whether function is **Enabled** or **Disabled**
- **Negative Caching** - Indicates whether function is **Enabled** or **Disabled**
- **Host Rotation** - Indicates whether function is **Enabled** or **Disabled**

DNS SETTINGS

Domain Name	eden-usr.com
Number Retries per Server:	1
Timeout Period in Seconds:	5
Cache Max TTL:	2147483
Negative Cache Max TTL	2147483
Caching:	ENABLED
Negative Caching:	ENABLED
Host Rotation:	ENABLED

show dns cache <1-65535>

Displays an entry in the DNS Cache Table. It lists:

- **Pretty Name** - Fully qualified name (resource record) the host connects to (at this row in the table). See RFC-1035, section 2.3.3 for more information.
- **Class** - DNS class of the resource record at this row in the table.
- **Type** - DNS type of the resource record at this row in the table.
- **TTL** - Time To Live period in seconds of the resource record
- **Elapsed TTL** - Period in seconds since resource record was received
- **DNS Server** - Host from which resource record was received, 0.0.0.0 if unknown.
- **Data** - RDATA portion of a cached RR. The value is in the format defined for the particular DNS class and type of the resource record. See RFC-1035, section 3.2.1 for more information.
- **(Error) Status** - Status column for the resolver cache table. Since only the agent (DNS resolver) creates rows in this table, the only values that a manager may write to this variable are the following: **Active**, **Destroy**

DNS CACHE ENTR

```

Pretty Name:  canary.mass-usr.co
Class:        1
Type:         1
TTL:          24761
Elapsed TTL   228
DNS Server    123.133.143.176
Data:
              92 73 78 c7
Status:       Active

```

show dns counters

Displays various counters for DNS.

- **Total Queries Received** - sum of DNS queries received.
- **Total Response Sent** - sum of DNS responses sent.
- **Responses from Client Processing** - DNS responses from local DNS Host Table.
- **Responses from Server Processing** - DNS responses from the DNS Server Table.
- **Success Responses from Server** - successful responses to DNS requests.
- **Error Response sent** - sum of failures to DNS requests, specifics shown below.

SPECIFIC ERROR COUNTERS

- **Format Errors** - Number of Format Error responses received by DNS.
- **Problems with Name Server** - internal server error.
- **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.

- **Non-authoritative Data Responses** - Number of requests made by the resolver for which a non-authoritative answer (cached data) was received.
- **Non-authoritative No Data Responses** - Number of requests made by the resolver for which a non-authoritative answer - no such data response (empty answer) was received.
- **Martians** - Number of responses received which were received from servers that the resolver does not think it asked.
- **Received Responses** - Number of responses received to all queries.
- **Unparseable Responses** - Number of responses received which were unparseable.
- **Fallbacks** - Number of times the resolver had to fall back to its seat belt information.
- **Good Caches** - Number of resource records the resolver has cached successfully.
- **Bad Caches** - Number of resource records the resolver has refused to cache because they appear to be dangerous or irrelevant. For example, resource records with suspiciously high TTLs, unsolicited root information, or those that don't appear to be relevant to the question the resolver asked.
- **Good Negative Caches** - Number of authoritative errors the resolver has cached successfully.
- **Bad Negative Caches** - Number of authoritative errors the resolver would have liked to cache but was unable to because the appropriate Resource Record was not supplied or looked suspicious.

show dns ncache <1-65535>

Displays an entry (row) in the DNS Negative Cache Table. It lists:

- **Pretty Name** - Fully qualified name (resource record) the host connects to (at this row in the table).
- **Class** - DNS class of the resource record at this row in the table.
- **Type** - DNS type of the resource record at this row in the table.
- **TTL** - Time To Live period in seconds of the resource record
- **Elapsed TTL** - Period in seconds since resource record was received
- **DNS Server** - IP address of the fully qualified name
- **Error Code** - Type of authoritative error indicated in the table. Types include:
 - **Nonexist(ant Name)** - authoritative name error
 - **No Data** - authoritative response with no error and no relevant data.
 - **Other** - some other cached authoritative error. At present, no such errors are known to exist.
- **(Error) Status** - Status column for the resolver negative response cache table. Since only the agent (DNS resolver) creates rows in this table. Types include: **Active, Destroy**

DNS NEGATIVE CACHE ENTR

Pretty Name	foo.mass-usr.com
Class:	1
Type:	1
TTL:	43200
Elapsed TTL:	207
DNS Server:	153.234.24.145
Error Code:	NONEXIST
Status:	Active

show events

Displays all events being directed to the console to also be echoed to the TELNET or dial-in session you are running. Any number of users can employ this function. The **hide events** command ends this directive. Events are configured with the **set facility** command.

show file <input_file_name>

Displays the contents of an ASCII file. For example:

```
HiPer>> show file easyfilter.fil
#filter
#IP:
#10 reject src-address = 220.159.132.13;
#20 accept src-address != 220.159.132.13
#30 reject udp-src-port = 69;
#40 reject tcp-src-port = 23;
#50 reject udp-dst-port = 69
#60 reject tcp-dst-port = 23;
```

show file <input_file_name> hex

Displays the contents of a hexadecimal file. For example (log-file.local):

000000	43453035	43453031	41742031	363a3537	CE05CE01At 16:57
0010	3a31342c	20466163	696c6974	79202255	14, Facility "User
0020	73657220	4d616e61	67657222	2c204c65	Manager",
000030	76656c20	22435249	54494341	4c223a3a	Level "CRITICAL":
000040	20415554	483a204e	6f206163	6b6e6f77	AUTH: No acknow
000050	6c656467	656d656e	74206672	6f6d2052	ledgement from
000060	41444955	53206163	636f756e	74696e67	RADIUS accounting
000070	20736572	76657273	2c207265	61636865	servers, reached
000080	64206d61	78206e00	43453032	41742031	max n*CE02At
000090	373a3136	3a31342c	20466163	696c6974	17:16:14, Facility
0000a0	79202255	73657220	4d616e61	67657222	"User Manager",

show filter <filter_name>

Displays the filter rules for all protocols specified in this file. The file name specified **MUST** be a filter file (*filter.fil*). See **show filter protocol** command below. Also, see the **edit** command to create or amend filter files.

*Note: A newly created filter file will not appear when this command is issued until the file is added to the Filter Table with the **add filter** command.*

For example (easyfilter.fil):

```
RULES FOR FILTER ./easyfilter.fil SHOW PROTOCOLS: ALL
#filter
IP:
10 reject src-address = 234.149. 82.139;
20 accept src-address != 234.149. 82.139;
30 reject udp-src-port = 69;
40 reject tcp-src-port = 23;
```

RULES FOR FILTER /./easyfilter.fil SHOW PROTOCOLS: ALL

50 reject udp-dst-port = 69

60 reject tcp-dst-port = 23;

IP-RIP

10 accept network = 244.49. 82.0;

20 deny

show filter <filter_name>**protocol** [ip, ip-call, ip-rip, ipx, ipx-call, ipx-rip, ipx-sap, login-access]

Displays filter rules based on protocol options specified. The filter name **MUST** be a filter file (*filter.fil*), as listed using **list filters**. Also see the **show filter** command above. It lists:

- **IP** - IP data filter rules
- **IP-CALL** - IP call filter rules
- **IP-RIP** - IP RIP advertisement filter rules
- **IPX** - IPX data filter rules
- **IPX-CALL** - IPX call filter rules
- **IPX-RIP** - IPX RIP advertisement filter rules
- **IPX-SAP** - IPX SAP advertisement filter rules
- **LOGIN-ACCESS** - Login access filter rules

show icmp or **show icmp settings**

Displays incoming login-access information including whether ICMP logged and ICMP Router Advertise are enabled. You can turn multicasting of ICMP router advertisements on or off with the **enable** or **disable icmp_router_advertise** command.

ICMP SETTINGS

ICMP Logging:	ENABLED
ICMP Router Advertise:Enabled	ENABLED

show icmp counters

Displays input and output counters for ICMP messages.

Note: Traceroute-generated packets received by HiPer ARC will not increment the ICMP error counts Time Exceeded and Destination Unreachable. Also, a number of ICMP error messages are sent to SYSLOG hosts while the Receive Destination Unreachable event is sent to the console.

Input Counters

- **Messages** - ICMP packets received
- **Errors** - ICMP packets received with errors
- **Destination Unreachable** - sum of ICMP messages received when a router cannot forward a packet to its specified destination. *Error messages sent to the console and CLI*
- **Time Exceeded** - sum of ICMP messages generated by a router when time has exceeded or a timeout has occurred while waiting for a packet segment. *Error messages sent to SYSLOG host*
- **Parameter Problems** - sum of ICMP messages generated by a router when it encounters an error. *Error messages sent to SYSLOG host*

- **Source Quench** - sum of ICMP messages informing a host it should slow data transmission to ease congestion. *Error messages sent to SYSLOG host*
- **Redirects** - sum of ICMP messages concerning a router advertising a host of a better next hop. *Error messages not logged*
- **Echos** - sum of ICMP request messages received, signifying transport system success
- **Echo Replies** - sum of ICMP reply messages received, indicating transport system success
- **Timestamps** - sum of ICMP request messages received seeking time from another machine for clock synchronization and estimated transit time purposes. *Error messages sent to SYSLOG host*
- **Timestamp Replies** - sum of ICMP timestamp reply messages
- **address Masks** - sum of ICMP address Mask Reply messages. *Error messages sent to SYSLOG host*
- **address Mask Replies** - sum of ICMP request messages concerning a host's ability to gather network information. *Error messages sent to SYSLOG host*
- **Advertise** - sum of router advertisements received by HiPer ARC
- **Solicit** - sum of host-generated router queries received by HiPer ARC. *Error messages sent to SYSLOG host*

Output Counters

- **Messages** - total of ICMP messages transmitted
- **Errors** - ICMP packets transmitted with errors
- **Destination Unreachable** - sum of these messages sent. *Error messages sent to SYSLOG host*
- **Time Exceeded** - sum of these messages sent. *Error messages sent to SYSLOG host*
- **Parameter Problems** - sum of these messages sent. *Error messages sent to SYSLOG host*
- **Source Quench** - sum of these messages sent
- **Redirects** - sum of these messages sent. *Error messages sent to SYSLOG host*
- **Echos** - sum of ICMP Echo (request) messages sent
- **Echo Replies** - sum of these messages sent
- **Timestamps** - sum of these messages sent
- **Timestamp Replies** - sum of these messages sent
- **address Masks** - sum of these messages sent
- **address Mask Replies** - sum of these messages sent. *Error messages sent to SYSLOG host*
- **Advertise** - sum of router advertisements sent by HiPer ARC. *Error messages sent to SYSLOG host*

show interface <interface_name> or **show interface settings**

Displays settings for the specified modem or Ethernet interface. This lists:

- **Description** - Name of the interface driver. **Ethernet**, **ATM** or **Modem** drivers.
- **Type** - Kind of physical serial interface. For example: **RS232** or **Ethernet-CSMA/CD**
- **Speed** - Estimate of the interface's current bandwidth in bits per second.
- **High Speed** - Estimate of the interface's current bandwidth in units of 1,000,000 bits per second, exceeding 20 million bits/second.
- **Administrative Status** - Permanently configured state of the interface. Choices: **Up** or **Down**

- **Operational Status** - Current state of the interface. Choices: **Up** or **Down**
- **Link Up/Down Traps** - Permanently configured value indicating whether linkUp/linkDown traps should be generated for this interface. Choices: **ENABLED** (*default*) or **DISABLED**
- **Promiscuous Mode** - When set to **FALSE** (*default*), this interface accepts packets/frames addressed only to this station. When set to **TRUE**, the station accepts all packets/frames transmitted on the network.
- **Connector Present** - When set to **TRUE** (*default*) the interface sublayer has a physical connector and **FALSE** (*default*) when otherwise.
- **Filter Access** - This switch allows user filters to override the specified interface filter. If set to **OFF** (*default*), user filters do not override the interface filters. If set to **ON**, user filters override the interface filter.
- **Last Change** - Last configuration change made to the interface, measured in system time.
- **Input Filter** - Name of the input filter enabled for the specified interface.
- **Output Filter** - Name of the output enabled filter for the specified interface.
- **Physical address** - MAC address of the specified Ethernet interface.
- **Host Type** - The type of host this dial-in user is currently connected to. Choices: **PROMPT**, **SELECT** and **SPECIFIED**. Default: **SELECT**
- **Connection Type** - Kind of connection this interface is configured for. Choices: **DIRECT_CONN**, **NORMAL**, **DIRECT_NET**, **NO_PROMPT**, and **PROMPT_USER_ONLY**. Default: **NORMAL**
- **Port Type** - The type of physical port configured. Choices: **NETWORK**, **LOGIN** and **LOGIN_NETWORK** (*default*)
- **User Name** - Name of connected user. This value is set only if the port is configured not to prompt for user name.
- **Access** - Direction of calls currently configured on this interface. Choices: **DIAL_IN**, **DIAL_OUT** or **TWO_WAY** (*default*).
- **Dial Prefix** - A number defining the prefix to the phone number.
- **Init Script** - Initialization script currently in use. Default: **USR_int**
- **TCP Port** - TCP port number you associate with the login service. Default: **0**. Range: **0-65535**
- **Protocol** - Currently connected protocol type. Choices: **PPP** or **SLIP**. Default: **PPP**
- **Prompt** - Dialin prompt you set for this interface. Limit: **64 ASCII** characters.
- **Prompt Style** - Specifies whether prompting of the username and password on this interface is provided by HiPer ARC (**LOCAL**), or by a distant security service - TACACS+ (**REMOTE**). Default: **LOCAL**
- **Message** - Salutation you specified for this interface. Limit: **64 ASCII** characters
- **Host address** - IP address of the host specified for this interface.
- **Authentication** - Indication of whether dialin user's profile is forwarded with (**ENABLED**) or without (**DISABLED**) authentication. Default: **ENABLED**
- **Login Service** - Type of login service you configured for this interface. Choices: **TELNET**, **rlogin** and **ClearTCP**. Default: **TELNET**.

INTERFACE slot:3/mod:1 SETTINGS

Description:	GWC Modem Driver
Type:	RS232
Speed:	33600
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 00:01:07
Input Filter:	
Output Filter:	
Host Type	SELECT
Connection Type:	NORMAL
Port Type:	LOGIN_NETWORKS
User Name:	larry
Access:	TWO_WAY
Dial Prefix:	
Init Script:	USR_int
TCP Port:	0
Protocol:	PPP
Prompt:	
login:	
Prompt Style:	LOCAL
Message:	Welcom to 3Com Total Control HiPer ARC (TM) Networks That Go The Distance (TM)
Host address:	134.122.145.167
Authentication:	ENABLED
Login Service:	TELNET

show interface <interface_name> **counters**

Displays counters for the specified interface.

Input Counters

- **Octets** - number of bytes received
- **Ucast** - number of Unicast packets received
- **MultiCast** - number of multicast packets received
- **BroadCast** - number of broadcast packets received
- **Discards** - Number of inbound packets 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** - number of unknown protocols in packet

Output Counters

- **Octets** - number of bytes transmitted
- **Ucast** - number of Unicast packets transmitted

- **MultiCast** - number of multicast packets transmitted
- **BroadCast** - number of broadcast packet transmitted
- **Discards** - Number of outbound packets 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)

show ip or show ip settings

Displays system-wide IP information.

- **IP System Host address** - IP address of the HiPer ARC
- **IP Forwarding** - *Enable* or *Disable* forwarding of IP packets
- **IP Address Pool Filtering** - *Enable* or *Disable* pool filtering
- **IP Address Pool Round Robin** - Whether IP addresses are allocated via the round robin method or not.
- **IP Multicast Proxy Interface** - HiPer ARC's IGMP proxy interface: If configured, the interface on which any groups learned or joined on other interfaces will be joined. This interface can be either HiPer ARC's **Eth:1** or **Eth:2** port or the **username** associated with the remotely attached host. Default: **None**
- **IP Multicast Heartbeat Status** - Indicates whether multicast heartbeat is **Enabled** or **Disabled**. Default: **Disabled**
- **IP Multicast Heartbeat Interface** - The interface on which multicast traffic for the specified group is monitored: *eth:1*, *eth:2*, or *slot:x/mod:y*. Default: **None**
- **IP Multicast Heartbeat Group** - The IP address of the multicast group being monitored.
- **IP Multicast Heartbeat Time** - The interval, in seconds, multicast traffic is being monitored. Default: **60 seconds**. Range: **0-65535**
- **IP Multicast Heartbeat Window** - The number of periods (in time values) multicast traffic is being monitored. Default: **5**. Range: **0-255**
- **IP Multicast Heartbeat Threshold** - The interval during which multicast traffic is not received after which an SNMP trap is issued. Default: **3**. Range: **0-65535**
- **IP Source address for RADIUS** - HiPer ARC's source IP address (where packets exit) supplied to an associated RADIUS server
- **IP Source address for SYSLOG** - HiPer ARC's source IP address (where packets exit) supplied to an associated SYSLOG server
- **IP Local address for Unnumbered Links** - Ethernet IP address supplied to remote PPP or SLIP users when they dialup HiPer ARC
- **IP source address for IGMP** - If configured, all IGMP packets sent from any of HiPer ARC's interfaces will use this address as its source address. Default: **0.0.0.0**

IP System Host address:	134.225.22.1760
IP Forwarding:	ENABLED
IP Address Pool Filtering:	ENABLED
IP Address Pool Round Robin:	ENABLED
IP Multicast Proxy Interface:	Eth:1
IP Multicast Heartbeat Status:	DISABLED



IP Multicast Heartbeat Interface:	NONE
IP Multicast Heartbeat Group:	0.0.0.0
IP Multicast Heartbeat Time:	60 seconds
IP Multicast Heartbeat Window:	5
IP Multicast Heartbeat Threshold:	3
IP source address for RADIUS:	0.0.0.0
IP source address for SYSLOG:	0.0.0.0
IP local address for unnumbered links:	0.0.0.0
IP source address for IGMP:	0.0.0.0

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 igmp <eth:1 | eth:2 | slot:x/mod:y>

Displays IP multicast settings for the specified interface.

- **IGMP Interface** - Network interface of HiPer ARC. **Eth:1**, **Eth:2** or **slot:x/mod:y**
- **Query Interval** - Period, in seconds, IGMP Host-Query messages are sent on this interface. Default: **125 seconds**
- **Max Response** - Maximum time a host has to respond to query requests on this interface. Default: **10 seconds**
- **Version** - The version of IGMP running on this interface. Default: **Version 2**

- **Querier** - Address of the IGMP Querier on the IP subnet to which this interface is attached.
- **Joins** - Number of times a group membership has been added on this interface - the number of times an entry for this interface has been added to the IGMP Cache Table. It indicates the amount of IGMP activity over time.
- **Robustness** - Setting for expected packet loss on a subnet. Default: **2**
- **Groups** - Current sum of multicast groups active on this interface.
- **Routing** - If enabled, indicates that HiPer ARC will try to become a querier on this interface. If disabled, indicates HiPer ARC will act as an IGMP host and only report multicast groups it joins. Default: **Disabled**
- **Multicast Forwarding** - Indicates if multicast packets will be received and transmitted on this interface. Default: **Disabled**
- **Multicast Proxy** - If enabled, indicates any multicast groups joined or learned on this interface will also be joined on the interface configured as the multicast proxy interface. Default: **Disabled**
- **IGMP Short Packets** - Sum of IGMP short packets received on the specified interface
- **IGMP Bad Checksum** - Sum of IGMP packets received with bad checksum on the specified interface
- **Queries Received** - Sum of IGMP queries received on the specified interface
- **Reports Received** - Sum of IGMP reports received on the specified interface
- **Reports For Known Groups Received** - Sum of IGMP reports for known groups received on the specified interface
- **Wrong Version Reports Received** - Sum of IGMP reports received with the wrong IGMP version number on the specified interface
- **Reports Sent** - Sum of IGMP reports sent on the specified interface

IGMP Interface	eth:1
Query Interval	125 seconds
Max Response	10 seconds
Version	2
Querier	135.122.143.143
Joins	1
Groups	1
Robustness	2
Routing	ENABLED
Multicast Forwarding	DISABLED
Multicast Proxy:	ENABLED
IGMP Short Packets	0
IGMP Bad Checksum	0
Queries Received	1
Reports Received	2
Reports For Known Groups Received	0
Wrong Version Reports Received	0
Reports Sent	3

show ip network <network_name> or **show ip network settings**

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

- **Interface** - interface this IP network runs on
- **Network address** - network address and subnet mask of HiPer ARC

- **Frame Type** - frame type used by HiPer ARC. Choices: **ETHERNET_II** or **SNAP**.
- **Mask** - subnet mask of HiPer ARC
- **Station** - station address of HiPer ARC
- **Broadcast Algorithm** - broadcast algorithm used for this network. Default: **IETF**
- **Max Reassembly Size** - maximum packet size allowed to be reassembled from fragments
- **IP Routing Protocol** - routing protocol used. Default: **None**
- **IP RIP Routing Policies** - routing policies used by RIP
- **IP RIP Authentication Key** - text string used for RIPv2 authentication
- **Status** - Enabled, ACTIVE, INACTIVE, Disabled
- **Reconfigure Needed** - FALSE or TRUE. When displaying the value TRUE, this setting notifies the administrator that the network should be reinitialized in order for a newly configured parameter to take effect. Using the **reconfigure** command allows the network to automatically re-enable without having to manually disable and enable the network. The value FALSE indicates no network editing has occurred and no reconfiguration is required.
- **IP Routing Metric** - routing metric configured for this network. Range **1-16**. Default: **1**.

SHOW IP NETWORK ipnet SETTINGS

```

Interface:                eth:11
Network address:          165.134.145.124/22
Frame Type                ETHERNET_I
Status:                   ENABLED
Reconfigure Needed:       FALSE
Mask                      255.255.252.0
Station:                  165.134.145.124
Broadcast Algorithm:      IETF
Max Reassembly Size:      3464
IP Routing Protocol:      RIPV2
IP Routing Metric:        1
IP RIP Routing Policies    SEND_ROUTES
                           SPLIT_HORIZON
                           FLASH_UPDATE
                           SEND_COMPAT
                           RIPV1_RECEIVE
                           RIPV2_RECEIVE

```

IP RIP Authentication Key

show ip routing or show ip routing settings

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

- **IP Router Administrative Status** - whether status is enabled or not. Default: **Enabled**
- **IP Static Remote Routes** - whether static routes are enabled or not. Default: **Enabled**
- **LAN Host address** - IP address of HiPer ARC
- **IP Autonomous System Number** - system number assigned. Default: **1**
- **IP Max Table Size** - maximum number of IP Routing Table entries allowed. Default: **1,415**
- **IP Max Metric Entries** - maximum metric entries allowed. Default: **512**

- **IP RIP** - whether RIP is enabled or not. Default: **Enabled**
- **IP Number RIP Interfaces** - number of RIP interfaces
- **IP Number RIP Neighbors** - number of IP RIP neighbors
- **IP RIP Flags** - type of IP RIP flags enabled

IP ROUTER SETTING

IP Router Administrative Status	Enabled
IP Static Remote Routes	Enabled
IP LAN Host address:	165.134.145.124
IP Autonomous System Number	1
IP Max Table Size:	1450
IP Max Metric Entries:	512
IP RIP:	Enabled
IP Number RIP Interfaces:	0
IP Number RIP Neighbors:	0
IP RIP Flags:	METRICS SEND_REQUEST

show ip security or **show ip security settings**

Displays state (enabled or disabled) of IP security settings. The settings shown below are defaults. See enable ip security_options commands on page enable ip security_option drop_all_fragoffset1 for more information.

IP SECURITY SETTINGS

Drop All Fragoffset1:	ENABLED
Drop TCP Fragoffset1	ENABLED
Disallow All Header Options	DISABLED
Disallow Source Route Options:	DISABLED

show ipx or **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
- **Number of Dynamic Pool Members** - number of addresses to reserve for dynamic IPX address assignments

IPX SETTINGS

Default Gateway:	0.00:00:00:00:00:00
PPP IPX Network address:	00000000
Name:	IPXNET
Network Number:	0
Max Hops:	15
Priority:	1
Dynamic address Pool Begin:	23

Number of Dynamic Pool Members: 200

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** - sum of IPX packets supplied locally containing structural errors
- **Discarded** - sum of outgoing packets discarded
- **Filtered Out** - sum of packets filtered out before transmission
- **Compression Errors** - sum of outgoing packets discarded due to compression errors
- **Socket Open Failures** - sum of outgoing packets discarded because a socket was not available

show ipx network <network_name> or show ipx network settings

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

- **Interface** - interface this IPX network uses: **ETH:1** or **ETH:2**
- **Network address** - network address of this IPX network
- **Frame Type** - frame type used by the interface (**ETHERNET II**, **NOVELL_8023**, **SNAP**, or **LOOPBACK**)
- **Maximum Packet Size** - maximum allowable packet size for this IPX network. Default: **1500**.
- **Status** - operational state of the network. Default: **ENABLED**
- **Network Delay (ticks)** - time in number of ticks it takes to reach this IPX network. Default: **1**
- **Network Learning Retries** - number of times this network will resend packets to discover its directly connected neighbors

- **Diagnostics** - sending of diagnostic packets. Default: **ENABLED**
- **NetBIOS** - support. Default: **ENABLED**
- **NetBIOS Name Caching** - support. Default: **DISABLED**
- **NetBIOS Cache Timer (sec)** - interval a NetBIOS system will be kept in the cache. Default: **60**
- **NetBIOS Maximum Hops** - most hops this network will make to locate a NetBIOS system. Default: **8**
- **RIP State** - status: **ON**, **OFF**, **AUTO ON**, or **AUTO OFF**. Default: **ON**
- **RIP Pace** - fastest pace, in packets per second, at which RIP packets may be sent on this circuit (*not settable via the CLI*)
- **RIP Update (sec)** - interval, in seconds, after which RIP periodic updates are transmitted. Default: **60**
- **RIP Age Multiplier** - number the *rip_update_interval* is multiplied by to obtain the *update* value. Default: **4**
- **RIP Max Packet Size** - largest allowable size of a RIP packet. Default: **446**
- **RIP Broadcast** - support. Default: **ENABLED**
- **RIP Periodic** - support. Default: **ENABLED**
- **SAP State** - support: **ON** or **OFF**. Default: **ON**
- **SAP Pace** - fastest pace, in packets per second, at which SAP packets may be sent on this circuit (*not settable via the CLI*). Default: **1**
- **SAP Update (sec)** - interval, in seconds, after which SAP periodic updates are transmitted. Default: **60**
- **SAP Age Multiplier** - number the *sap_update_interval* is multiplied by to obtain the *update* value. Default: **4**
- **SAP Packet Size** - greatest allowable size of a SAP packet. Default: **510**
- **SAP Broadcast** - support. Default: **ENABLED**
- **SAP Periodic** - support. Default: **ENABLED**
- **SAP Nearest Server Reply** - SAP seeks nearest neighbors: YES or NO. Default: **YES**

show ipx network <network_name> counters

Displays statistics for the specified IPX network.

- **RIP Out Packets** - sum of RIP packets transmitted
- **RIP In Packets** - sum of RIP packets received
- **SAP Out Packets** - sum of SAP packets transmitted
- **SAP In Packets** - sum of SAP packets received

```
SHOW IPX NETWORK ipxnet2 COUNTERS:
```

RIP Out Packets:	53
RIP In Packets:	30
SAP Out Packets:	1
SAP In Packets:	160

show ipx rip or show ipx rip settings

Displays information about RIP for IPX.

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

show ipx rip counters

Displays the sum of incorrect RIP packets.

show ipx sap or show ipx sap settings

Displays information about SAP for IPX.

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

show ipx sap counters

Displays the sum of incorrect SAP packets.

show l2tp or show l2tp settings

Displays settings for configured L2TP tunnels. See the **add** and **set lns** commands.

- **Maximum Number of Sessions** - Maximum number of simultaneous active sessions L2TP supports. Maximum: **450**
- **Maximum Number of Tunnels** - Maximum number of simultaneous active tunnels L2TP will support. Since sessions are multiplexed within a single tunnel, this value displays the number of L2TP tunnels supported *per tunnel*. Maximum: **450**
- **Number of Control Channel Seek Descriptor** - Number of tunnel terminators L2TP can simultaneously connect to. Default: **64**
- **Flow Control** - Indicates whether L2TP uses flow control on the data tunnel. Default: **Enabled**
- **Data Channel Delayed Acknowledgement Timeout** - Interval in milliseconds L2TP will wait to send acknowledge its peer when there are no data or control packets to piggyback the acknowledge to. Default: **500**
- **Data Channel Reassembly Timeout** - Interval in milliseconds L2TP uses to determine the window to use before reassembling out-of-order packets. A low value increases the chance that out-of-sequence packets will be lost. A high value increases the period when L2TP processes packets received out of order. The default of 0 may drop all out-of-sequence packets.
- **Control Channel Receive Packet Window** - Size of the control channel receive buffer awaiting acknowledgment by the system's peers. Default: **7**
- **Data Channel Receive Packet Window** - Size of the data channel receive buffer awaiting acknowledgment by the system's peers. Default: **7**
- **Inactivity Idle Timeout** - Interval in seconds L2TP will wait inactively and send a Hello packet. Default: **0**
- **Echo reply timeout** - Interval in seconds L2TP waits until a time-out occurs in receiving a response to the Hello message.
- **Logging Level** - The logging level L2TP is set to. Choices: *Disabled, Control Packets, Control and Data Packet Headers and Control and Data Packets*
- **Load balance status** - Indicates whether load balancing is **ENABLED** or **DISABLED**.
- **Number of Retransmissions** - Number of retransmissions l2tp will try before assuming its peer is unreachable. The default value of **0** cause l2tp to stop retransmissions. Maximum: **3**
- **Retransmission Interval** - Interval in seconds between retransmissions

- **Tunnel Challenge** - When enabled requires all incoming tunnels to perform encryption. Default: **DISABLED**

L2TP SETTINGS

Maximum Number of Sessions:	451
Maximum Number of Tunnels:	451
Number of Control Channel Seek Descriptors:	64
Flow Control:	ENABLED
Data Channel Delayed Acknowledgement Timeout	500
Data Channel Reassembly Timeout	0
Control Channel Receive Packet Window:	7
Data Channel Receive Packet Window:	7
Inactivity Idle Timeout:	60
Echo reply timeout:	90
Logging Level:	CONTROL PACKETS
Load balance status:	ENABLED
Number of Retransmissions:	3
Retransmission Interval:	2
Tunnel Challenge:	DISABLED

show l2tp counters

Displays statistics for configured L2TP tunnels.

- **Number of Active Tunnels** - Sum of currently active tunnels
- **Active Sessions** - Sum of currently active sessions
- **Fail Authentications** - Number of authentications failed by this L2TP stack since last initialized
- **Malformed Packets** - Sum of malformed packets received by this L2TP stack since last initialized
- **Control Tunnel Receive Packets** - Sum of control packets received by this L2TP stack since last initialized
- **Control tunnel receive packets with data** - Sum of control packets received with data by this L2TP stack since last initialized
- **Control tunnel receive packets without data** - Sum of zero length control packets received by this L2TP stack since last initialized
- **Processed control tunnel receive packets** - Sum of received control packets processed with data by this L2TP stack since last initialized
- **In sequence control tunnel receive packets** - Sum of control packets received in-sequence by this L2TP stack since last initialized
- **Out of sequence control tunnel receive packets** - Sum of control packets received out-of-sequence by this L2TP stack since last initialized
- **In order control tunnel receive packets** - Sum of control packets received in order by this L2TP stack since last initialized
- **Out of order control tunnel receive packets** - Sum of control packets received out-of-order by this L2TP stack since last initialized
- **Flow discarded control tunnel receive packets** - Sum of control packets discarded due to flow control by this L2TP stack since last initialized
- **Out of order discarded control tunnel receive packets** - Sum of control packets received and discarded due to ordering by this L2TP stack since last initialized
- **Control tunnel send packets** - Sum of control packets transmitted by this L2TP stack since last initialized
- **Control tunnel with data send packets** - Sum of control packets transmitted with data by this L2TP stack since last initialized

- **Control tunnel without data send packets** - Sum of zero length control packets transmitted without data by this L2TP stack since last initialized
- **Control tunnel flow control timeout** - Sum of control tunnel timeouts due to flow control experienced by this L2TP stack since last initialized
- **Local control tunnel flow control enables** - Sum of local control tunnel flow control enables experienced by this L2TP stack since last initialized
- **Remote control tunnel flow control enables** - Sum of remote control tunnel flow control enables experienced by this L2TP stack since last initialized
- **Control tunnel reassembly timeout** - Sum of control tunnel reassembly timeouts experienced by this L2TP stack since last initialized
- **Data tunnel receive packets** - Sum of data packets received by this L2TP stack since last initialized
- **Data tunnel with data receive packets** - Sum of data packets received with data by this L2TP stack since last initialized
- **Data tunnel without data receive packets** - Sum of zero length data packets received by this L2TP stack since last initialized
- **Processed data tunnel receive packets** - Sum of received data packets processed with data by this L2TP stack since last initialized
- **In sequence data tunnel receive packets** - Sum of data packets received in-sequence by this L2TP stack since last initialized
- **Out of sequence data tunnel receive packets** - Sum of data packets received out-of-sequence by this L2TP stack since last initialized
- **In order data tunnel receive packets** - Sum of data packets received in order by this L2TP stack since last initialized
- **Out of order data tunnel receive packets** - Sum of data packets received out-of-order by this L2TP stack since last initialized
- **Flow discarded data tunnel receive packets** - Sum of data packets discarded due to flow control by this L2TP stack since last initialized
- **Out of order discarded data tunnel receive packets** - Sum of data packets received and discarded due to ordering by this L2TP stack since last initialized
- **Data tunnel send packets** - Sum of data packets transmitted by this L2TP stack since last initialized
- **Data tunnel with data send packets** - Sum of data packets transmitted with data by this L2TP stack since last initialized
- **Data tunnel without data send packets** - Sum of zero length data packets transmitted without data by this L2TP stack since last initialized
- **Data tunnel flow control timeouts** - Sum of data tunnel timeouts due to flow control experienced by this L2TP stack since last initialized
- **Local data tunnel flow control enables** - Sum of local data tunnel flow control enables experienced by this L2TP stack since last initialized
- **Remote data tunnel flow control enables** - Sum of remote data tunnel flow control enables experienced by this L2TP stack since last initialized
- **Data tunnel reassembly timeouts** - Sum of data tunnel reassembly timeouts experienced by this L2TP stack since last initialized

show l2tp lns <number>

Displays settings for a local LNS entry on the LAC side of a L2TP tunnel.

L2TP LNS	1
IP address:	149.112.222.13

Tunnel security level:	BOTH
Tunnel Challenge:	ENABLED

show l2tp tunnel <number>

Displays statistics of the specified L2TP tunnel. It lists:

- **Local control tunnel ID** - identifier of the specified local control tunnel
- **Peer control tunnel ID** - identifier of the specified remote control tunnel
- **Control tunnel state** - current status of the specified control tunnel
- **Local init connection** - indicates whether tunnel was established locally or not
- **IP address** - remote peer's IP address
- **Local receive packet window** - size of local send window
- **Remote receive packet window** - size of remote receive window
- **Control tunnel receive packets** - sum of control packets received on the control tunnel
- **Control tunnel receive packets with data** - sum of control packets received with data
- **Control tunnel receive packets without data** - sum of zero length packets received
- **Processed control tunnel receive packets** - sum of receive packets that were processed
- **In sequence control tunnel receive packets** - sum of packets received in sequence
- **Out of sequence control tunnel receive packets** - sum of packets received out of sequence
- **In order control tunnel receive packets** - sum of packets received in order
- **Out of order control tunnel receive packets** - sum of packets received out of order
- **Flow discarded control tunnel receive packets** - sum of received packets discarded due to flow control
- **Out of order discarded control channel receive packets** - sum of received packets discarded due to ordering
- **Control tunnel send packets** - sum of packets transmitted
- **Control tunnel send packets with data** - sum of packets transmitted with data
- **Control tunnel send packets without data** - sum of zero length packets transmitted
- **Control tunnel flow control timeouts** -sum of timeouts caused by flow control
- **Control tunnel flow control on** - status of local flow control: **Enabled** or **Disabled**
- **Local control tunnel flow control enables** - sum of local flow control enables for the control session
- **Remote control tunnel flow control on** - status of remote flow control: **Enabled** or **Disabled**
- **Remote control tunnel flow control enables** - sum of remote flow control enables for the control session
- **Control tunnel reassembly timeouts** - sum of reassembly timeouts
- **Remote host name** - host name of the L2TP peer

show l2tp tunnel <number> session <number>

Displays statistics for a specified L2TP tunnel session.

- **Remote call id** - session identifier for this control channel tunnel
- **Peer Name** - peer session name on this interface - typically the login name of the remote user
- **Session Duration** - number of milliseconds the session has been up on this interface
- **Line state** - current status of the control tunnel: *Allocated, Waiting, Calling, Offering, Answering, Connected, Disconnecting Local, Disconnecting Remote, Lost*
- **Call device number** - logical device the L2TP stack uses internally; useful for debugging purposes.
- **Call serial number** - serial number applied to the session
- **Connect BPS** - baud rate this session was established at

- **Call bearer type** - bearer type for this session: *Analog* or *Digital*
- **Session frame type** - framing type for this session: *Asynchronous* or *Synchronous*
- **Local receive packet window** - local send window size for this session
- **Remote receive packet window** - remote send window size for this session
- **Remote window type** - indicates whether windowing (sequencing of L2TP packets) is **Enabled** or **Disabled** on the remote side of the tunnel
- **Local window type** - indicates whether windowing (sequencing of L2TP packets) is **Enabled** or **Disabled** on the local side of the tunnel
- **Data tunnel receive packets** - sum of data packets received on the data tunnel for this session
- **Data tunnel receive packets with data** - sum of packets received on the data tunnel for this session which contained data
- **Processed data tunnel receive packets** - sum of packets received on the data tunnel for this session which were processed
- **In sequence data tunnel receive packets** - sum of packets received in sequence on the data tunnel for this session
- **Out of sequence data tunnel receive packets** - sum of packets received out of sequence on the data tunnel for this session
- **In order data tunnel receive packets** - sum of packets received in order on the data tunnel for this session
- **Out of order data tunnel receive packets** - sum of packets received out of order on the data tunnel for this session
- **Flow discarded data tunnel receive packets** - sum of packets received on the data tunnel for this session which were discarded due to flow control
- **Out of order discarded data tunnel receive packets** - sum of packets received on the data tunnel for this session which were discarded due to ordering
- **Data tunnel send packets** - sum of packets transmitted on the data tunnel for this session
- **Data tunnel send packets with data** - sum of packets transmitted on the data tunnel for this session containing data
- **Data tunnel send packets without data** - sum of zero length packets transmitted on the data tunnel for this session
- **Data tunnel flow control timeouts** - sum of flow control timeouts experienced on the data tunnel for this session
- **Local data tunnel flow control on** - current state of local flow control for this data tunnel session
- **Local data tunnel flow control enables** - sum of local flow control enables for this data tunnel session
- **Remote data tunnel flow control on** - current state of remote flow control for this data tunnel session
- **Remote data tunnel flow control enables** - sum of remote flow control enables for this data tunnel session
- **Data tunnel reassembly timeout** - sum of re-assembly timeouts for this data tunnel session

show maximum_local_users

Configures the total number of users that can be created locally on HiPer ARC. See the **show maximum_local_users** command to display the setting. Maximum: **1000**.

Maximum Number Of Local Users:	1000
--------------------------------	------

show memory

Displays HiPer ARC's DRAM (Dynamic Random Access Memory) usage.

- **Total System Memory Resources** - total amount of usable memory for router applications
- **Free Memory** - amount of memory not in use
- **Code Size** - amount of memory used by code
- **Initialized Data Size, Uninitialized Data Size, Stack Size** - static data areas

SYSTEM MEMORY RESOURCE

Total System Memory Resources:	55087 KB
Free Memory:	43240 KB
Code Size:	2052 KB
Initialized Data Size:	316 KB
Uninitialized Data Size:	3733 KB
Stack Size:	512 KB

show memory utilization

Displays system DRAM memory usage resources as well as periodic memory usage checks. It lists:

- **Total System Memory Resources** - total amount of usable memory for router applications
- **Free Memory** - amount of memory not in use
- **Code Size** - amount of memory used by code
- **Initialized Data Size, Uninitialized Data Size, Stack Size** - static data areas
- **Free Memory Current Value** - amount of memory currently not in use
- **Free Memory 1 Hour Before** - amount of memory not in use one hour ago
- **Free Memory 12 Hour Before** - amount of memory not in use 12 hours ago
- **Free Memory 24 Hour Before** - amount of memory not in use 24 hours ago
- **Total Buffer Cache** - total amount of memory in pre-allocated buffer header
- **Free Buffer Cache** - amount of unused memory in pre-allocated buffer header

SYSTEM MEMORY RESOURCE

Total System Memory Resources:	55087 KB
Code Size:	2052 KB
Initialized Data Size:	316 KB
Uninitialized Data Size:	3733 KB
Stack Size:	512 KB
Free Memory Current Value:	42552 KB
Free Memory 1 Hour Before:	42554 KB
Free Memory 12 Hour Before:	42554 KB
Free Memory 24 Hour Before:	UNKNOWN
Total Buffer Cache:	4000
Free Buffer Cache:	28972

show modem_group <name>

Displays the switched interfaces that belong to the specified modem group and their status. For example:

MODEM GROUP boston INTERFACES 3

Interfac	Statu
slot:3/mod:1	ACTIVE
slot:3/mod:2	ACTIVE
slot:3/mod:3	ACTIVE

show mpip or **show mpip settings**

Displays MPIP server configuration you set with the **set mpip server** command. For example:

MPIP Server State	ON
MPIP Client State	ON
MPIP UDP Port	5912

show network <name> or **show network settings**

Displays the configured settings for the specified network. For an example, see the output from the **show ip network** command above.

show network <name> **counters**

Displays the statistical counters for the specified network. IP does not maintain network counters, though..

SHOW IPX NETWORK ipxnet COUNTERS:	
RIP Out Packets:	2484
RIP In Packets:	113484
SAP Out Packets:	2266
SAP In Packets:	699788

show nmc or **show nmc settings**

Displays the current settings for the following Network Management Card (NMC). See associated enable/disable commands for more information.

- **NMC Chassis Awareness** - either **ENABLED** (default) or **DISABLED**
- **Dynamic Slot Assignment (DSA)** - either **ENABLED** or **DISABLED** (default)
- **DSA Idle Rebalancing** - either **ENABLED** or **DISABLED** (default)

Note: Dynamic Slot Assignment cannot be enabled unless chassis awareness is enabled. If chassis awareness is disabled, this will turn off DSA. If DSA is enabled, this will enable chassis awareness. For example:

NMC SETTINGS	
Chassis Awareness:	ENABLED
Dynamic Slot Assignment:	DISABLED
DSA Idle Rebalancing:	DISABLED

show nmc counters

Displays Dynamic Slot Assignment (DSA) statistics for the Network Management Card (NMC). This information is useful for debugging purposes. For example:

NMC COUNTERS	
DSA Query Requests RX:	1
DSA Query Responses TX:	1
DSA Service Requests TX:	1
DSA Slot Assignments RX:	2
DSA Request Round TX:	1
DSA Invalid Packet RX:	0



show nmc status

Displays whether the Network Management Card is present in the Total Control Chassis. When a query from the NMC to HiPer Arc is posted, its date and time are recorded. The command lists, for example:

NMC Status

Last NMC Query was received at: 14-MAY-1998 14:34:21

Alternately, if the NMC is not present, the command may list the following:

NMC Status

Last NMC Query was received at: No NMC Queries Received Yet, Probably NMC is Absent

show ntp or show ntp settings

Displays Simple Network Time Protocol settings you configured for HiPer ARC using the **set ntp** command. For example:

Primary Server is	titanic
Secondary Server is:	queenmary
Status	ENABLED
Polling Interval (Seconds)	600
Max Retransmissions	5
Retransmission Timeout:	10

show packet_logging or show packet_logging settings

Displays settings for packet size and logging. See the **set packet_logging** command for more information. For example:

PACKET LOGGING SETTING

Logging Packet Type:	NONE
Logging Packet Size:	0

show pbus settings

Displays base setting and port density of modem slot/span/channel settings you specified for packetbus modems with the **set pbus reported_base** and **set pbus reported_port_density** commands. This affects vendor-specific fields in RADIUS authentication and accounting packets. See the **set pbus reported_base** command for more information.

PBUS SETTINGS

Reported Base:	1
Port Density:	256

show ping or show ping settings

Displays general ping settings you specified using the **ping** and **set ping maximum_rows** commands. For example:

Maximum Rows in Table	20
Verbose Mode:	NO
Background Mode	NO

show ping row <row_number> or show ping row <row_number> settings

Displays settings for the specified row in the Remote Ping Table. Range: **1-1000**. These settings reflect the configuration you specified using the **ping** command. For example:

```

PING SETTINGS for ROW: 1 DESTINATION: ilysium
Status:                                ACTIVE
Resolved IP address:                   155.155.121.143
Count:                                100
Interval                              1
Size:                                  64
Timeout:                              20
Self Destroy Delay:                   10

```

show ping row <row_number> counters

Displays counters for the specified row in the Remote Ping Table. These settings reflect the configuration you specified using the **ping** command. This command displays:

- **Status** - The present state of this row. Possible states include: 'notReady', 'notInService' and 'active'.
- **Count** - Number of pings to be transmitted in this sequence.
- **Requests Sent** - Number of pings sent when this row became active.
- **Replies Received** - Number of pings received when this row became active.
- **Timeouts Occured** - Number of requests timed-out since this row became active.
- **Last Round Trip** - The round trip time in milliseconds experienced by the last request-reply iteration. A round trip value of **-1** indicates failed resolution.
- **Minimum Round Trip** - The minimum ping round trip time in milliseconds, not including timed out requests.
- **Maximum Round Trip** - The maximum ping round trip time in milliseconds, not including timed out requests.
- **Average Round Trip** - The average ping round trip time in milliseconds, not including timed out requests.
- **Creation Time** - When this row was created in terms of system up time.
- **Activation Time** - When this row was last activated in terms of system up time.
- **Last Changed Time** - When any object in this row was last changed in terms of system up time.

```

PING COUNTERS for ROW: 1 DESTINATION: ilysium
Status:                                ACTIVE
Count:                                100
Requests Sent:                         71
Replies Received                       64
Timeouts Occured                      6
Last Round Trip (ms)                   250
Minimum Round Trip (ms)                0
Maximum Round Trip (ms):               480
Average Round Trip (ms)                81
Creation Time:                         40
Activation Time                        40
Last Changed Time                      0d 00:07:56

```

show ping server <host name or IP_address> **counters**

Displays ping server counters associated with the ping server you specified in the **add ping service_loss_system** command.

*Note: Average Time is expressed in milliseconds. Also, a value of -1 indicates the ping system failed. See **show ping server settings** below for more information.*

PING SERVER COUNTERS for SERVER		cassava
Status		ENABLED
Time Since Contacted:		-1
Pings Sent		0
Pings Received		0
Timeouts		0
Unreachables:		0
Average Time (ms)		0

show ping server <host name or IP_address> or **show ping server settings**

Displays ping server settings you specified with the add ping service_loss_system command. A value of -1 indicates failure of ping system. It lists:

- **Status** - whether this system is being pinged regularly or not. Default: **Enabled**
- **Frequency** - interval between each ping request. Default: **30 seconds**
- **Misses Allowed** - number of ping messages that can be missed before the modems are busied out. Default: **1**
- **Time Out** - how long a ping request can be outstanding before it is considered to have failed. Default: **2**
- **Reachable** - whether the ping server is connected
- **Time Since Contacted** - number of seconds since the server was reached
- **address** - address of system

PING SERVER SETTINGS for SERVER		cassava
Status		ENABLED
Frequency:		30
Misses Allowed		1
TimeOut		10
Reachable		UNTRIED
Time Since Contacted:		-1
address:		0.0.0.0

show ppp on interface <slot:x/mod:y> or **show ppp on interface settings**

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

SETTINGS for PPP BUNDLE 1

- **Operational Status** - *Opened or Not Opened*
- **Number Active Links** - number of links active on this PPP bundle
- **User Profile** - user whose parameters were used in creating links
- **Local MMRU** - MRU the remote entity uses when sending packets to local PPP entity. Default: **1514**
- **Remote MMRU** - MRU the local entity uses when sending packets to remote PPP entity. Default: **1514**

- **Local Endpoint Class** - type of address used as the identifier - **IEEE MAC address**
- **Local Endpoint Length** - maximum length of the local Endpoint Discriminator address. Default: **6**
- **Local Endpoint ID** - *MAC address* of local Endpoint Discriminator
- **Remote Endpoint Class** - value of remote Endpoint Discriminator Class, which indicates the type of address being used as the identifier
- **Remote Endpoint Length** - maximum length of remote Endpoint Discriminator address
- **Remote Endpoint ID** - *IP address* of remote Endpoint Discriminator

SETTINGS for PPP BUNDLE 1 COMPRESSION

- **Operational Status** - *Opened or Not Opened*
- **Compression Protocol** - protocol used by the local PPP entity when it compresses the local PPP entity to the remote PPP entity. Default: **VJ-TCP**

SETTINGS for PPP LINK

- **Operational Status** - *Opened or Not Opened*
- **Interface Index** - index number of the interface used
- **Local MRU** - MRU the remote entity uses when sending packets to local PPP entity. Default: **1514**
- **Remote MRU** - MRU the local entity uses when sending packets to remote PPP entity. Default: **1514**
- **Local to Peer ACC Map** - value of the ACC Map used for sending packets from the local PPP entity to the remote PPP entity
- **Peer to Local ACC Map** - ACC Map used by the remote PPP entity when transmitting packets to the local PPP entity
- **Local To Remote Protocol Compression** - Indicates whether the local PPP entity will use Protocol Compression when transmitting packets to the remote PPP entity. Default: **Enabled**
- **Remote To Local Protocol Compression** - Indicates whether the remote PPP entity will use Protocol Compression when transmitting packets to the local PPP entity. Default: **Enabled**
- **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. Default: **Enabled**
- **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. Default: **Enabled**

SETTINGS for PPP LINK - AUTHENTICATION

- **Operational Status** - *Opened or Not Opened*
- **Local To Remote Compression Protocol** - protocol used by the local PPP entity when it compressed the remote PPP entity. Default: **CHAPMD5**
- **Remote To Local Compression Protocol** - protocol used by the remote PPP entity when it compressed the local PPP entity.

SETTINGS for PPP BUNDLE	20
Operational Status:	Opened
Number Active Links:	1
User Profile:	n1
Local MMRU	1514

```

SETTINGS for PPP BUNDLE                                20
Remote MMRU:                                           1514
Local Endpoint Class:                                 IEEE MAC address
Local Endpoint Length:                                6
Local Endpoint ID:                                    00:00:00:03:00:65
Remote Endpoint Class:                                Null Class
Remote Endpoint Length:                               0
Remote Endpoint ID:                                   Class=0x1:Length=0x0

SETTINGS for PPP BUNDLE 20 COMPRESSION
Operational Status:                                   NotOpened
Compression Protocol:                                 NONE

SETTINGS for PPP BUNDLE 20 IP PROTOCOL
Operational Status:                                   Opened
Local To Remote Compression Protocol:                 VJ_TCP
Remote To Local Compression Protocol:                 VJ_TCP
Local Max Slot ID:                                    15
Remote Max Slot ID:                                   15
Local IP address:                                     172.152.42.72
Remote IP address:                                    192.112.226.200

SETTINGS for PPP LINK 20 - 8
Operational Status:                                   Opened
Interface Index                                       8
Local MRU:                                            1514
Remote MRU:                                           1514
Local to Peer ACC Map:                               a0000
Peer to Local ACC Map:                               0
Local To Remote Protocol Compression:                 ENABLED
Remote To Local Protocol Compression:                 ENABLED
Local To Remote AC Compression:                       ENABLED
Remote To Local AC Compression:                       ENABLED

SETTINGS for PPP LINK 20 - 8 AUTHENTICATION
Operational Status:                                   Opened
Local To Remote Authenticate Protocol:                 CHAPMD5
Remote To Local Authenticate Protocol:                 NONE

```

show ppp on interface <slot:x/mod:y> 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** - sum of frames judged too long
- **Transmit Frames** - sum of frames received from the PPP application for transmission over this link
- **Bytes from Upper Layer** - sum of bytes handed down from an upper layer application for this link
- **Bytes to Lower Layer** - sum of bytes received from a lower layer application for this link
- **Received Frames** - sum of frames received on this link
- **Bytes to Upper Layer** - sum of bytes handed up to an upper layer application over this link
- **Bytes from Lower Layer** -sum of bytes received from a lower layer application over this link

show ppp or show ppp settings

Displays global settings for PPP. You can modify DIAL-IN Users Authentication using the **set ppp receive_authentication** command. Modify the system transmit authentication name by using the **set system** command.

- **DIAL-IN Users Authenticate PAP or CHAP** - Indicates whether PPP requires dialin users to authenticate strictly via: *PAP, CHAP, ANY, EAP-MD5; with ANY, NONE, or ENCRYPTED-ANY (CHAP, EAP-MD-5, MS-CHAP) or RADIUS-EAP-PROXY*. Default: *None*
- **System Transmit Authentication Name** - remote account keyword used by PPP at the datalink layer for WAN connections.
- **PPP offloading** - Indicates, when enabled, that PPP framing can be offloaded to the modem card, if modem card is capable of doing it. Default: **ENABLED**
- **CCP attempted for call types** - Indicates the types of call for which the Compression Control Protocol will be enabled in the HiPer ARC PPP module. Possible values are: *all, none, digital, compressed analog* and *uncompressed analog*. Default value: **DIGITAL** and **UNCOMPRESSED ANALOG**.
- **Primary NBNS Server address** - IP address for the primary NetBIOS Name Server (NBNS) server. In the absence of a user-specific NBNS address, this will be sent in IPCP negotiation.
- **Seconday NBMS Server address** - IP address for the secondary NetBIOS Name Server (NBNS) server. In the absence of a user-specific NBNS address, this will be sent in IPCP negotiation.
- **DNS Configuration Usage** - Indicates, when enabled, that PPP will take DNS addresses from HiPer ARC's DNS table in the absence of user-configured DNS addresses. Choices: **SYSTEM**, **PPP** or **NONE**
- **Primary PPP DNS Server address** - Globally configured PPP DNS primary server IP address, used if user-configured DNS addresses are not available, for IPCP (IP Control Protocol) negotiation.
- **Secondary PPP DNS Server address** - Globally configured PPP DNS secondary server IP address, used if user-configured DNS addresses are not available, for IPCP (IP Control Protocol) negotiation.

- **Session Start Message** - Displays string you specified to indicate the beginning of a PPP session.

PPP AUTHENTICATION

DIAL_IN Users Authenticate:	ANY
PPP Authentication Preference:	DEFAULT
System Transmit Authentication Name:	HiPer
PPP offloading :	ENABLED
CCP will be attempted for call type(s) :	DIGITAL UNCOMPRESSED_ANALOG
Primary NBNS Server address:	0.0.0.0
Secondary NBNS Server address:	0.0.0.0
DNS configuration Usage:	SYSTEM
Primary PPP DNS Server address:	0.0.0.0
Secondary PPP DNS Server address:	0.0.0.0
PPP session start message:	Hi 142.212.114.57, you're connected to 253.23.43.54.

show ptp or show ptp settings

Displays settings for configured PPTP tunnels.

- **Maximum Number of Sessions** - Maximum number of simultaneous active sessions PPTP supports.
- **Maximum Number of Tunnels** - Maximum number of simultaneous active tunnels PPTP will support. Since sessions are multiplexed within a single tunnel, this value displays the number of PPTP tunnels supported *per tunnel*.
- **Number of Control Channel Seek Descriptor** - Number of tunnel terminators PPTP can simultaneously connect to. Default: **8**
- **Authentication Type** - Whether PPTP seeks encryption from its peers. Default: **Disabled**
- **Flow Control** - Whether PPTP uses flow control on the data tunnel. Default: **Enabled**
- **Data Channel Delayed Acknowledgement Timeout** - Interval in milliseconds PPTP will wait to send acknowledge its peer when there are no data or control packets to piggyback the acknowledge to. Default: **500**
- **Data Channel Reassembly Timeout** - Interval in milliseconds PPTP uses to determine the window to use before reassembling out-of-order packets. A low value increases the change that out-of-sequence packets will be lost. A high value increases the period when PPTP processes packets received out of order. The default of 0 may drop all out-of-sequence packets.
- **Control Channel Receive Packet Window** - Size of the control channel receive window sent to PPTP's peers. Default: **7**
- **Data Channel Receive Packet Window** - Size of the data channel receive window sent to PPTP's peers. Default: **7**
- **Inactivity Idle Timeout** - Interval in seconds PPTP will wait inactively and send a Hello packet. Default: **0**
- **Echo reply timeout** - Interval in seconds PPTP waits until a time-out occurs in receiving a response to the Hello message.
- **Load balance status** - Whether load balancing is **Enabled** or **Disabled**.

- **Logging Level** - The logging level PPTP is set to. Choices: *Disabled, Control Packets, Control and Data Packet Headers and Control and Data Packets* .

PPTP SETTINGS	
Maximum Number of Sessions:	451
Maximum Number of Tunnels:	451
Number of Control Channel Seek Descriptors:	64
Flow Control:	ENABLED
Data Channel Delayed Acknowledgement Timeout	500
Data Channel Reassembly Timeout	0
Data Channel Receive Packet Window:	7
Inactivity Idle Timeout:	60
Echo reply timeout:	90
Load balance status:	ENABLED
Logging Level:	CONTROL PACKETS

show pptp counters

Displays statistics for configured PPTP tunnels.

- **Number of Active Tunnels** - Sum of currently active tunnels
- **Active Sessions** - Sum of currently active sessions
- **Malformed Packets** -
- **Control Tunnel Receive Packets** -
- **Processed Control Tunnel Receive Packets** -
- **Control Tunnel Send Packets** -
- **Data Tunnel Receive Packets** - Sum of data packets received
- **Data Tunnel With Data Receive Packets** - Sum of data packets received with data
- **Data Tunnel Without Data Receive Packets** - (zero length bytes) dataless acknowledgement packets
- **Processed Data Tunnel Receive Packets** - Sum of received and processed data packets
- **In Sequence Data Tunnel Receive Packets** - Sum of data packets received in sequence
- **Out of Sequence Data Tunnel Receive Packets** - Sum of data packets received in out of sequence
- **In Order Data Tunnel Receive Packets** - Sum of data packets received in order
- **Out of Order Data Tunnel Receive Packets** - Sum of data packets received out of order
- **Flow Discarded Data Tunnel Receive Packets** - Sum of receive data packets dropped due to flow control
- **Out of Order Discarded Data Tunnel Receive Packets** - Sum of out of order receive data packets dropped
- **Data Tunnel Send Packets** - Sum of send data packets
- **Data Tunnel With Data Send Packets** - Sum of data packets sent containing data
- **Data Tunnel Without Data Send Packets** - Sum of data packets sent without data
- **Data Tunnel Flow Control Timeouts** - Sum of data channel flow control timeouts
- **Local Data Tunnel Flow Control Enables** - Sum of data channel flow control enables
- **Remote Data Tunnel Flow Control Enables** - Sum of remote data channel flow control enables
- **Data Tunnel Reassembly Timeouts** - Sum of data channel reassembly timeouts

show pptp tunnel <number>

Displays statistics of the specified PPTP tunnel. It lists:

- **Local control tunnel ID** - identifier of the specified local control tunnel
- **Peer control tunnel ID** - identifier of the specified remote control tunnel
- **Control tunnel state** - current status of the specified control tunnel
- **Local init connection** - indicates whether tunnel was established locally or not
- **IP address** - remote peer's IP address
- **Local receive packet window** - size of local send window
- **Remote receive packet window** - size of remote receive window
- **Control tunnel receive packets** - sum of control packets received on the control tunnel
- **Control tunnel receive packets with data** - sum of control packets received with data
- **Control tunnel receive packets without data** - sum of zero length packets received
- **Processed control tunnel receive packets** - sum of receive packets that were processed
- **In sequence control tunnel receive packets** - sum of packets received in sequence
- **Out of sequence control tunnel receive packets** - sum of packets received out of sequence
- **In order control tunnel receive packets** - sum of packets received in order
- **Out of order control tunnel receive packets** - sum of packets received out of order
- **Flow discarded control tunnel receive packets** - sum of received packets discarded due to flow control
- **Out of order discarded control channel receive packets** - sum of received packets discarded due to ordering
- **Control tunnel send packets** - sum of packets transmitted
- **Control tunnel send packets with data** - sum of packets transmitted with data
- **Control tunnel send packets without data** - sum of zero length packets transmitted
- **Control tunnel flow control timeouts** -sum of timeouts caused by flow control
- **Control tunnel flow control on** - status of local flow control: **Enabled** or **Disabled**
- **Local control tunnel flow control enables** - sum of local flow control enables for the control session
- **Remote control tunnel flow control on** - status of remote flow control: **Enabled** or **Disabled**
- **Remote control tunnel flow control enables** - sum of remote flow control enables for the control session
- **Control tunnel reassembly timeouts** - sum of reassembly timeouts
- **Remote host name** - host name of the PPTP peer

show pptp tunnel <number> session <number>

Displays statistics for a specified PPTP tunnel session.

- **Remote call id** - session identifier for this control channel tunnel
- **Peer Name** - peer session name on this interface - typically the login name of the remote user
- **Session Duration** - number of milliseconds the session has been up on this interface
- **Line state** - current status of the control tunnel: *Allocated, Waiting, Calling, Offering, Answering, Connected, Disconnecting Local, Disconnecting Remote, Lost*
- **Call device number** - logical device the L2TP stack uses internally; useful for debugging purposes.
- **Call serial number** - serial number applied to the session
- **Connect BPS** - baud rate this session was established at
- **Call bearer type** - bearer type for this session: *Analog* or *Digital*
- **Session frame type** - framing type for this session: *Asynchronous* or *Synchronous*
- **Local receive packet window** - local send window size for this session

- **Remote receive packet window** - remote send window size for this session
- **Remote window type** - indicates whether windowing (sequencing of L2TP packets) is **Enabled** or **Disabled** on the remote side of the tunnel
- **Local window type** - indicates whether windowing (sequencing of L2TP packets) is **Enabled** or **Disabled** on the local side of the tunnel
- **Data tunnel receive packets** - sum of data packets received on the data tunnel for this session
- **Data tunnel receive packets with data** - sum of packets received on the data tunnel for this session which contained data
- **Processed data tunnel receive packets** - sum of packets received on the data tunnel for this session which were processed
- **In sequence data tunnel receive packets** - sum of packets received in sequence on the data tunnel for this session
- **Out of sequence data tunnel receive packets** - sum of packets received out of sequence on the data tunnel for this session
- **In order data tunnel receive packets** - sum of packets received in order on the data tunnel for this session
- **Out of order data tunnel receive packets** - sum of packets received out of order on the data tunnel for this session
- **Flow discarded data tunnel receive packets** - sum of packets received on the data tunnel for this session which were discarded due to flow control
- **Out of order discarded data tunnel receive packets** - sum of packets received on the data tunnel for this session which were discarded due to ordering
- **Data tunnel send packets** - sum of packets transmitted on the data tunnel for this session
- **Data tunnel send packets with data** - sum of packets transmitted on the data tunnel for this session containing data
- **Data tunnel send packets without data** - sum of zero length packets transmitted on the data tunnel for this session
- **Data tunnel flow control timeouts** - sum of flow control timeouts experienced on the data tunnel for this session
- **Local data tunnel flow control on** - current state of local flow control for this data tunnel session
- **Local data tunnel flow control enables** - sum of local flow control enables for this data tunnel session
- **Remote data tunnel flow control on** - current state of remote flow control for this data tunnel session
- **Remote data tunnel flow control enables** - sum of remote flow control enables for this data tunnel session
- **Data tunnel reassembly timeout** - sum of re-assembly timeouts for this data tunnel session

show prompting

Displays the type of CLI prompting specified for Login/Network users on HiPer ARC. When configured by the **enable prompting single_level** command, the *Login/Network* prompt is bypassed for those users - and they are deposited directly at the *HiPer>* prompt line. It lists:

Single Level Prompting: **ENABLED**

show radius or show radius settings

Displays current RADIUS accounting and authentication configuration.

Attribute Style:	ASCEND
Authentication Algorithm:	ROUND_ROBIN

Attribute Style:	ASCEND
Interim Accounting Interval Status:	Enabled
Interim Accounting Interval:	120

show remote user <user_name>

Displays settings for the specified user, currently connected to HiPer ARC. Settings displayed will vary with the type of user connected. See the **set** and **add user** commands for more information.

- **User Name** - Name of the currently connected user
- **Service Type** - Type of network service employed by the user: *Login, Framed, Callback, Dialout, Administrative*
- **NAS IP Address** - IP address of HiPer ARC
- **NAS Port** - Port attribute of HiPer ARC
- **Login Ip Host** - IP address of the host this user is currently logged into
- **Login Service** - Type of login service employed by this user: *Telnet, Rlogin, TCP, Ping*
- **Login Port** - Port number on HiPer ARC where this user is connected
- **State** - Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Class** - Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Session Timeout** - Interval in seconds this user has to remain connected before being timed out
- **Idle Timeout** - Interval in seconds this user has to remain idle before being timed out
- **Port Limit** - Maximum number of dialin ports a user can concurrently employ
- **Min(imum) Compression size** - The minimum packet size for which compression will be done
- **Port Tap** - Indicates whether the Port Tap feature is enabled or not
- **Port Tap Format** - Indicates the Port Tap format type: *Hex(decimal), ASCII, Clear(TCP)*
- **Tap Output** - Indicates where output from the tap is destined: *Screen, Syslog*
- **Tap Facility** - Endpoint where tap information can be directed
- **Tap Priority** - Preference levels of messages that can be logged: *Critical, Unusual, Common, Verbose*
- **Tap IP Address** - The IP address of the SYSLOG where Tap information is destined

User Name:	larry
Service Type:	Login
NAS IP Address:	134.23.120.24
NAS Port:	0
Login IP Host:	134.23.121.4
Login Service:	Telnet
Login Port:	23
State:	larry
Class:	gina
Session Timeout:	60 seconds
Idle Timeout:	30 seconds
Port Limit:	2
Min Compression size:	(null)
Port Tap:	Enabled
Port Tap Format:	Hex
Tap Output:	Syslog
Tap Facility:	Authentication

Tap Priority:	Critical
Tap IP Address:	134.23.129.23

show rs232 interface

```
dte_in_sig
dte_out_sig
sync_errs
```

This command is not supported in the present release.

show security_option or show security_option settings

Displays status of SNMP user access, security service and administration by remote users. You can modify SNMP user access using the **enable** or **disable security_option snmp** commands. You can modify administration by remote user using the **enable** or **disable security_option remote_user** commands.

- **SNMP User Access** - *Enabled* (default) or *Disabled*
- **Security Service** - *RADIUS* or *TACACS+*
- **Administration by Remote DialinUser** - *ON* (default) or *OFF*
- **Administration by Remote TELNET user** - *ON* (default) or *OFF*

SECURITY OPTION SETTINGS

SNMP User Access:	ENABLED
Security Service:	RADIUS
Administration by Remote TELNET User:	ON
Administration by Remote Dialin User:	ON

show service_loss_busyout or show service_loss_busyout settings

Displays service loss busyout settings for RADIUS and ping, including frequency of busyouts and busyout status. Use the **set service_loss_busyout** and **add ping_service_loss_system** commands to configure this RADIUS/PING function and the **enable service_loss_busy_out command** to enable RADIUS or PING busyout. For example:

SERVICE LOST BUSYOUT SETTINGS

RADIUS Busyout:	DISABLED
RADIUS Busyout Frequency:	60
RADIUS Busyout Status:	START
PING Busyout:	DISABLED

show session <user_name>

Displays the session configuration for the specified user. It lists:

- **Service Type** - Type of network service employed by the user: *Login, Framed, Callback, Dialout, Administrative*
- **Port Limit** - Maximum number of dialin ports a user can concurrently employ
- **Session Timeout** - Interval in seconds this user has to remain connected before being timed out
- **Idle Timeout** - Interval in seconds this user has to remain idle before being timed out
- **Speed of Connection** - Estimate of the session's current bandwidth in bits per second.
- **NAS IP Address** - IP address of HiPer ARC
- **NAS Port** - Port attribute of HiPer ARC

- **State** - Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Class** - Value returned by RADIUS server (in Access-Challenge packet) during CHAP authentication
- **Login Ip Host** - IP address of the host this user is currently logged into
- **Login Service** - Type of login service employed by this user: *Telnet, Rlogin, TCP, Ping*
- **Login Port** - Port number on HiPer ARC where this user is connected

INFORMATION FOR SESSION	larry
Service Type:	Administrative
Port Limit:	2
Session Timeout:	2000
Idle Timeout:	600
Speed of Connection:	Auto
NAS IP Address:	147.14.24.157
NAS Port:	0
State:	larry
Class:	boston
Login IP Host:	147.14.34.23
Login Service:	Telnet
Login Port:	23

show slip or show slip settings

Displays SLIP configurations. Indicates, when enabled, that SLIP framing can be offloaded to the modem card - if the modem card is capable of doing it - and the *start message* - which appears when the SLIP connection comes up. Default: **enabled**.

See the **add slip session_start_message** command for information on writing the message. For example:

SLIP offloading	Enabled
SLIP Session Start Message:	SLIP connection starting. Your ss %client_ip \n

show snmp or show snmp settings

Displays whether the SNMP Authentication Traps setting is *enabled* (or *disabled*) to indicate authentication-failures, which you can modify using **enable** or **disable snmp authentication traps** commands. Default: **Enabled**.

show snmp community_pool <pool_name>

Displays the IP address of the specified SNMP community address pool. See the **add snmp community_pool** command for more information. It lists:

Community Pool	shrewsbury
	132.113.122.188

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

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 trap_community_pool <name>

Displays the specified SNMP trap community and IP addresses of associated trap communities defined using the **add snmp trap_community** command. It lists:

```
Community Pool  sayhey
2.2.2.2
2.2.2.3
2.2.2.4
```

show tunnel switch_counters

Displays switch statistics for L2TP and PPTP tunnels including the sum of total or current L2TP tunnels switched to PPTP tunnels and vice versa. It lists:

TUNNEL SWITCH COUNTERS	
Number of total PPTP Tunnels switched to PPTP:	10
Number of total PPTP tunnel switched to L2TP:	10
Number of total PPTP tunnel switched to L2TP:	10
Number of total L2TP tunnel switched to L2TP:	5
Number of current PPTP tunnel switched to L2TP:	5
Number of current PPTP tunnel switched to PPTP:	5
Number of current L2TP tunnel switched to PPTP:	5
Number of current L2TP tunnel switched to L2TP:	5

show system or **show system settings**

Displays system information.

- **System Descriptor** - company designation of HiPer ARC including build date
- **Object ID** - identifies this system to SNMP managers
- **System UpTime** - time the system has been running since last boot
- **System Contact** - name of person responsible for system. Modify using **set system** command
- **System Name** - modify using **set system** command
- **System Location** - site where system is located. Modify using **set system** command
- **System Services** - for example, Internet EndToEnd Applications
- **System Transmit Authentication Name** - system-wide keyword for PPP on the WAN, modified using **set system** command
- **System Version** - loaded release version of the system software
- **Reset EEPROM Settings On Bootup** - whether earlier-saved EEPROM settings are reapplied upon bulk configuration download. Default: **DISABLED**

SYSTEM DESCRIPTION**System Descriptor:**

3Com Corporation HiPer Access Router Card Built on Aug 10 1998 at 23:02:01.

Object ID:	1.3.6.1.4.1.429.2.19
System UpTime:	0d 00:56:00
System Contact:	Larry Cortese
System Name	HiperMAN
System Location	Westboro
System Services:	Internet EndToEnd Applications
System Transmit Authentication Name:	HiPer
System Version:	V4.1.0
Reset EEPROM Settings On Bootup:	DISABLED

show tacacsplus or **show tacacsplus settings**

Displays TACACS+ watchdog accounting configuration such as the specified interval to issue an accounting watchdog request to the TACACS+ server and whether that interval service is enabled or disabled. It lists:

Interim Accounting Interval Status:	ENABLED
Interim Accounting Interval:	240

show tcp or **show tcp settings**

Displays system-wide TCP settings.

Note: Most of these settings cannot be edited.

TCP SETTINGS

- **Retransmission Algorithm** - type of algorithm used. Default: **Van Jacobson**
- **Minimum Timeout** - minimum retransmission timeout interval. Default: **0**
- **Maximum Timeout** - maximum retransmission timeout interval. Default: **240000** seconds.
- **Maximum Connections** - sum of TCP connections allowed. Default: **1024**
- **TCP Nagle Algorithm** - state of the Nagle algorithm which, when enabled, prohibits one octet-sized TCP packet transmissions to an output buffer until there is sufficient data to fill a maximum-sized segment. Default: **Enabled**
- **Keep-Alives** - status of the keep-alive function
- **Keep-Alive Interval** - period in seconds of receive inactivity before a keep-alive packet is sent

TCP SETTINGS

Retransmission Algorithm:	Van Jacobson
Minimum Timeout:	0
Maximum Timeout:	240000
Maximum Connections:	1024
TCP Nagle Algorithm:	ENABLED
Keep-Alives:	ENABLED
Keep-Alive Interval:	30

show tcp counters

Displays system-wide TCP statistics.

TCP COUNTERS

- **Active Opens** - number of times TCP connections have made a direct transition to SYN-SENT state from CLOSED state
- **Passive Opens** - number of times TCP connections have made a direct transition to SYN-RCVD state from LISTEN state
- **Attempt Fails** - number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state
- **Resets** - number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state
- **Currently Established** - number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT
- **Input Segments** - sum of segments received
- **Output Segments** - sum of segments sent, including those on current connections but excluding those containing only retransmitted octets
- **Retransmitted Segments** - sum of segments retransmitted

show telnet or **show telnet settings**

Displays the status of the TELNET escape and trying message features (ENABLED (*default*) or DISABLED). It is set using **disable/enable telnet escape** and **trying_message** commands. It lists:

TELNET SETTINGS	
TELNET Escape:	ENABLED
TELNET Trying Message:	ENABLED

show tftp request <input_file_name>

Displays statistics of the specified request for TFTP service. It lists:

- **Filename** - Name of file to be requested from or sent to the TFTP server.
- **Server** - Name or IP address of the TFTP server
- **Action** - Type of request send to the TFTP server. **PUT** or **GET**
- **Mode** - The text format the file is transmitted as. Choices: **ASCII** or **OCTET** (binary). Default: **ASCII**
- **Retransmit Timeout** -Interval in seconds HiPer ARC waits for a reply from the TFTP server before retransmitting a TFTP request. Range: **1-60**. Default: **5 seconds**
- **Maximum Timeout** - Interval in seconds HiPer ARC waits for a response from the TFTP server before the TFTP request is cancelled. Range: **1-300**. Default: **25 seconds**
- **Status** - State of each current TFTP request in the table:
 - **Normal** - Request is in the table or has been successfully completed
 - **Getting** - Initial state: TFTP server is receiving a file
 - **Putting** - Initial state: TFTP server is sending a file
 - **Error** - Request has finished unsuccessfully and will generate an error message
- **Error String** - Error message detailing why TFTP request has failed

SHOW TFTP REQUEST FOR FILE filter.in	
Server:	scylla
Action:	GET
Mode:	ASCII
Retransmit Timeout:	5
Maximum Timeout:	25
Status	NORMAL
Error String:	

show time

Displays the system *date*, *time*, and *uptime*. The present time is expressed in Greenwich Mean Time (GMT). For example:

System Date (Time in GMT)	13-JUL-2041 19:25:11
System UpTime:	0d 00:12:30

show traceroute or **show traceroute settings**

Displays the maximum number of traceroutes configurable using the set **traceroute maximum_rows** command. See **traceroute**, **list traceroute**, **delete traceroute**, and **set traceroute maximum_rows** commands for more information. For example:

Maximum Rows in Table:	20
------------------------	----

show traceroute row <number> settings

Displays results of the specified trace (entry in the Traceroute Table) using the **traceroute** command. It lists:

- **State** - Status of the specified traceroute in the table. Possible states:
 - **WAITING DNS** - waiting for DNS resolution
 - **DNS FAILED** - destination address could not be resolved
 - **BAD address** - resolved IP address is illegal
 - **HOPS EXCEEDED** - maximum number of hops was exceeded
 - **DEST UNREACHABLE** - trace timed out because route to the host could not be found
 - **TRACING** - performing traceroute
 - **COMPLETED SUCCESSFULLY** - traceroute completed successfully
 - **RESOURCE FAILURE** - not enough resources to complete the command
- **Hop Timeout** - Interval in seconds before HiPer ARC retries a hop. Default: **3**
- **Hop Probes** - maximum attempts HiPer ARC makes to learn a hop before moving to the next hop. Default: **3**
- **Max Hops** - maximum number of hops HiPer ARC takes to trace before quitting. Default: **30**
- **UDP Port** - HiPer ARC port number used trying to find the route. Default: **33434**
- **Data Size** - amount of data in bytes sent in the traceroute packet. Range: **1-8184 bytes**
- **Hop Count** - number of hops HiPer ARC takes to reach the destination.

TRACEROUTE SETTINGS for ROW: 1 DESTINATION:

10.0.0.2

State:	COMPLETED SUCCESSFULLY
Hop Timeout:	3
Hop Probes:	3
Max Hops:	30
UDP Port:	33434
Data Size:	1
Hop Count:	2

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>

settings

all_settings

Displays the parameters defined for the specified user.

- **Settings** - Displays settings for the specified user with the exception of *disabled IP*, *IPX*, *Tap Status* and *Tunnel Type* parameters.
- **All_settings** - Displays *all* settings for the specified user.

The type of information displayed depends on the type of user you specify. You can issue the **list users** command to see which users are defined, and what *type(s)* user each is. An example of a login/dialout/network/manage follows. Note that this user may not be typical. Defaults are indicated by **(D)**.

INFORMATION FOR USER: administrator

Status:	ACTIVE
Type:	LOGIN MANAGE
Expiration:	NONE
Message:	Welcome to Nirvana, Mr. Tweedy
Phone Number:	(D)
Alternate Phone Number:	(D)
Input Filter:	(D)
Output Filter:	(D)
Modem Group:	all (D)
Session Timeout in seconds:	0 (D)
Idle Timeout in seconds:	0 (D)
Port Limit:	11
Tap Status:	DISABLED
Tap Format:	ASCII
Tap Output:	SYSLOG
Tap Facility:	LOG_AUTH
Tap Loglevel:	CRITICAL
Tap Address:	0.0.0.0 (D)

PARAMETERS FOR LOGIN USERS:

Login Service:	TELNET (D)
TCP Port:	23 (D)
Terminal:	vt100 (D)
Login Host Name:	barney
Login Host:	0.0.0.0 (D)
Host Type:	SELECT (D)

PARAMETERS FOR DIALOUT USERS:

Start Time:	00:00:00 (D)
End Time	00:00:00 (D)
Local IP address	0.0.0.0 (D)
Dial Type	MANUAL (D)
Connection Speed:	AUTO (D)
Send Password:	
Connection Script	
Send-1:	(D)

INFORMATION FOR USER: administrator

Reply-1:	(D)
Send-2:	(D)
Reply-2:	(D)
Send-3:	(D)
Reply-3:	(D)
Send-4:	(D)
Reply-4:	(D)
Send-5:	(D)
Reply-5:	(D)
Send-6:	(D)
Reply-6:	(D)

PARAMETERS FOR NETWORK USERS

Network Service	PPP	(D)
Header Compression	TCPIP	(D)
Spoofing:	DISABLED	(D)
MTU:	1514	(D)
IP Usage:	ENABLED	(D)
Address Selection:	ASSIGN	(D)
Remote IP Address:	0.0.0.0/H	(D)
IP Routing:	NONE	(D)
IP RIP Routing Protocol:	RIPV1	(D)
IP RIP Routing Policies	SEND_ROUTES	
	SPLIT_HORIZON	
	POISON_REVERSE	
	FLASH_UPDATE	
	SEND_COMPAT	
	RIPV1_RECEIVE	
	RIPV2_RECEIVE	
IP RIP Authentication Key:	babylon5	
Default Route Option	DISABLED	(D)
IGMP Query Interval:	125 seconds	
IGMP Max Response:	10 seconds	
IGMP Version:	2	
IGMP Robustness:	2	
IGMP Routing:	DISABLED	(D)
Multicast Forwarding:	DISABLED	(D)
Multicast Proxy:	DISABLED	(D)
IPX Usage:	ENABLED	(D)
IPX Address:	00000000	(D)
IPX Routing:	RESPOND	(D)
IPX WAN Usage:	DISABLED	(D)
IPX RIP Update:	60	
IPX RIP Age Multiplier:	4	
IPX SAP Update:	60	
IPX SAP Age Multiplier:	4	

PARAMTERS FOR TUNNEL USERS:

INFORMATION FOR USER: administrator

```

Tunnel Type:                None    (D)
Medium Type:                IPV4
Client Endpoint:
Server Endpoint:
Private Group ID:
Security:                   None

```

PARAMETERS for NETWORK PPP USERS

```

Max Channels:               2      (D)
Channel Decrement Percent:  0      (D)
Channel Expansion Percent:  0      (D)
Expansion Algorithm:        CONSTANT (D)
Receive ACC Map:           ffffffff (D)
Transmit ACC Map:          ffffffff (D)
Compression Algorithm:     AUTO    (D)
Compression Reset Mode:    AUTO    (D)
Min Compression Size       256     (D)
Encryption Algorithm:      NONE    (D)
Primary DNS Server:        0.0.0.0
Secondary DNS Server:      0.0.0.0

```

TELNET Commands

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

telnet <IP_name or address>

Establishes a TELNET client session with the specified IP host name or address. 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 address> **TCP_port** <number>

Establishes a TELNET client session with the specified IP host name or address using the specified TCP port number. It works just like the TELNET command, except you also specify the TCP port number to be used. Default TCP port number: **23**. Maximum: **65535**

TFTP Command

tftp or **tftp** <IP_name or address>

Initiates *command mode* Trivial File Transfer Protocol (TFTP) service. You can specify an IP address/name to directly access the client or issue the **tftp** command with your choice of ancillary values. Alternately, you can issue the **add tftp request** command to configure and the **enable tftp request** command to activate TFTP service. For more information, type *man tftp* with TFTP enabled. The command parameters are:

Value	Effect
ascii	Set text mode to ASCII. Default
binary	Set text mode to OCTET

Value	Effect
connect [host_name]	Connect to the remote TFTP server
get [remotefile] [localfile]	Receive a file
help	Print help information
mode [ascii binary]	Set file transfer mode: ASCII or Binary
put [localfile] [remotefile]	Send a file
quit	Exit TFTP
rexmt	Set the retransmission timeout interval. Range: 1-60 . Default: 5 seconds
status	Show current TFTP request status
timeout	Set maximum timeout interval. Range: 1-300 . Default: 25 seconds
trace	Toggle packet tracing
verbose	Toggle verbose mode echoes command
?	Print help information

For example, at the HiPer>> prompt, type:

tftp ENTER

status ENTER

The command lists:

Connected to status.

Mode: netascii Verbose: off Tracing: off

Rexmt-interval: 5 seconds, Max-timeout: 25 seconds

Traceroute Command

traceroute <IP_name or address>

maxhops [number]

port [UDP port]

retries [retries per hop]

size [data size]

timeout [timeout per hop]

Displays the route (each hop) that a data packet takes from its source to a specified destination on the network and the time in milliseconds to reach each hop and return. Traceroute utilizes ICMP to monitor network messages and UDP to send out the packet. The command also can be implemented from an SNMP station. Router DNS services are always used to resolve names and/or verify addresses in dot notation. An address of zero indicates there was no response from that hop.

Note: A row will timeout after 30 minutes and automatically be deleted. Also, a row can be deleted at any time, regardless of its state of status.

Also see set traceroute maximum_row, show traceroute, list traceroute and delete traceroute commands for more information.

Be aware that traceroute-generated packets received by HiPer ARC will not increment ICMP error counters (Time Exceeded and Destination Unreachable). Error messages are generated for the following reasons:

- **DNS Failed** - destination address could not be resolved due to timeout or other reason

- **Bad address** - resolved IP address is illegal
- **Hop Timeout** - timeout occurred
- **Hops Exceeded** - maximum number of hops exceeded
- **Dest(ination) Unreachable** - a route to the host could not be found
- **Tracing** - performing traceroute
- **Resource Failure** - not enough resources to complete the command

Parameters	Description
<IP name or address>	IP name or address of destination to target. Maximum characters: 255 .
maxhops	Maximum number of hops traceroute runs before quitting. Default: 30 . Range: 1-255 .
port	UDP port number that the probe is sent to. Value should be an unused port on the destination host. Default: 33434 . Range: 1-65000
retries	Number of times to attempt a given hop. Range: 1-10
size	Amount of data in bytes to send in the traceroute packet. A larger data size slows down performance and provides no additional information. Default: 1 . Range: 1-8184 .
timeout	Interval in seconds before hop times out; not for completion of the command. Default: 3 . Range: 1-60 .

The command will generate all information received up to resolution or failure.

HOP	address	ROUND-TRIP-TIME
1	154.112.254.24	100
2	154.112.254.254	100
3	154.112.124.254	100
4	154.112.170.2	100
5	154.112.79.1	200
6	154.112.63.253	100
7	153.234.24.145	200
8	137.039.037.067	250
9	Unknown	0
10	Unknown	0
11	Unknown	0
12	157.130.064.098	260
DEST UNREACHABLE		

Unassign Command

unassign interface <interface_name_list>
modem_group <group_name>

Removes the specified interface from the list of interfaces you previously assigned to the specified modem group. You specify interfaces for a modem group when you add a modem group, using **add modem_group interface**. You can also add interfaces to that modem group using **assign interface modem_group**. You can see which interfaces you have assigned to an existing modem group using the **show modem_group** command.

Verify Command

verify filter <filter_name>

Verifies the syntax of a filter file, which has been previously added to the table. If you update a filter file and TFTP it to the FLASH file system, and the file already exists in the Filter Table, 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.

verify chat_script <name>

Verifies the syntax of the specified file previously added to the Chat Script table. This command is useful when a file has been edited and requires its syntax be checked. For more information, see the **add**, **delete**, **show** and **list chat_scripts** commands. Also, see *Appendix E: RADIUS and TACACS+ Systems*.

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_address>

Links a dial-in user to the specified IP host using a default login service and port number. After connecting, the user is prompted for a login and password to the host. For example:

```
HiPer: connect came
      Trying 167.132.143.167 ...
      Connected to 167.132.143.167
      Escape character is ^]
Hummingbird Communications Ltd., Telnet Daemon V5.
Username: lcortese
Password:
```

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* section to learn how to exit the CLI.

rlogin <ip_name_or_address>

Establishes an rlogin client session with the specified IP host name or IP address. You must have run add DNS host or add DNS server for the system to recognize an IP host name.

rlogin <ip_name_or_address> **TCP_port** <number>

Establishes an rlogin client session with the specified IP host name or IP address using the specified TCP port number. The default rlogin TCP port number is 513. You must have run add DNS host or add DNS server for the system to recognize an IP host name.

telnet <ip_name_or_address>

Establishes a TELNET connection to the specified IP address or host name. You must have run add DNS host or add DNS server for the system to recognize an IP host name.

telnet <ip_name_or_address> **tcp_port** <number>

Sets a TELNET connection to the specified IP address or host name with the specified TCP port number. The default port number is 23. You must have a domain name server specified or have added the host name via add DNS host and add DNS server commands for the system to recognize an IP host name.



You should run RIP when setting up a global IP network if you intend to support TCP services such as TELNET, rlogin and ClearTCP. Without RIP on the internal network, you won't learn of remote networks should the Ethernet interface be disabled.

TELNET Commands

The following commands are available to Console port users who Telnet from the Console port. Such users can access these commands by using the TELNET escape command: **Ctrl]** (right bracket). This function is not supported for login users.

close

Ends the active TELNET connection.

help

Describes the available commands.

send <string>

Transmits a TELNET control character. The available commands are:

Parameters	Description
AYT	Are you there
IP	Interrupt process
BRK	Break
AO	Abort output
EC	Erase character
EL	Erase link
GA	Go ahead
NOP	No operation
EOR	End of record
SYNC	Synchronize
ESC	Escape

set escape <string>

Allows changing the TELNET escape character from **Ctrl]** (right bracket] to something else. Control characters are specified using the carat character followed by the character. For example, to set the TELNET escape character to *Ctrl x*, type:

```
set escape ^ x
```

status

Displays the IP address of the remote host you are Telnetted to and the value of the TELNET escape character.

CLI Exit Commands

These commands are available to dial-in (modem) and TELNET (LAN) users so they can disconnect from the CLI.

bye, exit, leave, quit

Leaves the CLI, but keeps this connection open. These commands return you to the dial-in user or TELNET commands.

logout

Leaves the CLI and closes this connection. This ends the dial-in user or TELNET session.

Command Features

The command language has several built-in features that make it easier to use. When abbreviating commands, it's sometimes difficult to remember 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) or left arrow	go back one character
(Ctrl f) or right arrow	go forward one character
(Esc b)	go back one word
(Esc f)	go forward one word
(Ctrl a)	go to beginning of command
(Ctrl c)	escape from CLI process
(Ctrl e)	go to end of command
(Ctrl d) or (Ctrl k)	delete character

Command Retrieval

Command retrieval retrieves commands from the history of previous commands entered. You can display the current command history using the history command. You can change the number of commands kept in the command history buffer using the set command history command.

(Ctrl p) or up arrow	recall previous command in history list
(Ctrl n) or down arrow	recall next command in history list



Positional Help

Positional help displays the list of possible parameters when you type **?** (question mark) after any command or parameter. It then redisplay 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 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.

Output Pause

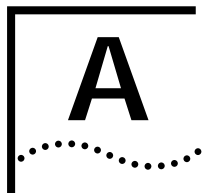
When output to your screen pauses because more than 24 lines are waiting for display, you can press **ENTER** to display one more *line of output*, **ESC** to display *one more page* of output or **q** to *quit* the command.

Command Kill

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

Comments

;	Nothing following the semicolon will be processed. This is useful when you are writing CLI script files. See a description of the do command in <i>Chapter 9: Administrative Tools</i> to run a CLI script.
---	--



NOTICES & TECHNICAL SPECIFICATIONS

Chapter Overview

This chapter describes:

- Safety compliances and certifications
- Hardware specifications
- Environmental specifications
- Power specifications
- Network Application Support (NAS) backplane pinouts
- System standards and specifications
- Software specifications

Safety Compliances & Certifications—U.S.

The following compliance statement is required by the FCC.

FCC Part 15 Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For More Information

If these suggestions don't help, you might consult the following booklet:

Interference to Home Electronic Entertainment Equipment Handbook

You can order the booklet from the U.S. Government Printing Office, Washington, DC 20402. Ask for stock number 004-000-00498-1.

Hardware Specifications

The table below describes basic hardware specifications.

Certification	Complies with FCC Part 15, UL-listed, CSA-approved
Processor	PowerPC 603E, 200 MHz
Dynamic Read Access Memory (DRAM)	64 MB, upgradeable to 128 MB
FLASH Read Only Memory (ROM)	8 MB, 1 MB reserved
Compatibility	PCI Dual 10/100 Base-T Ethernet NIC, Quad modem & HDM, NMC, DSP, EdgeServer, NETServer, Dual T1 & PRI cards
Physical Dimensions	12.9 x .79 x 6.9 inches 32.9 x 2.0 x 17.5 centimeters
Certification	Complies with FCC Part 15, UL-listed, CSA-approved

Environmental Specifications

The table below specifies shipping and storage and operating specifications.

Shipping and storage	Temperature: -25° to +75° Celsius, -13° to +167° Fahrenheit Relative Humidity: 0 to 95% non-condensing
Operating	Temperature: 0° to +40° Celsius, 32° to +104° Fahrenheit Relative Humidity: 0 to 95% non-condensing

Power Specifications

The table below details Total Control power usage figures based on the card or card set installed in the chassis. Card sets include NAC, NIC and any other auxiliary system cards required for proper operation. If chassis current-in totals more than 70 amps, the 130-amp power supply must be used. Amps-in equal .54 at nominal line voltage of 230 VAC, 1.04 at 120 VAC and 2.60 at -48 VDC.



Figures below reference the 70/130 amp TCENH chass with integral fan tray only (not the 45A chass).

Configuration Choices	+5.2 Volt Current (A)	+/- 12.2 Volt Current (A)	Watts	BTUs
HiPer ARC	4		20.8	70.9
HiPer ARC +Enet Set	6		31.2	106.4
HiPer ARC +Token Set	6.5		33.8	115.3
HiPer ARC Max. Set	7		36.4	124.1
HiPer DSP	4.3		22.4	76.2
HiPer DSP Mezzanine	.5		2.6	8.9
HiPer DSP NIC only	.6		3.1	10.6
Dual 10/100 RISC Gateway	2		10.4	35.5

Configuration Choices	+5.2 Volt Current (A)	+/- 12.2 Volt Current (A)	Watts	BTUs
HiPer DSP Set Domestic	4.9		25.5	86.9
HiPer DSP Set International	5.4		28.1	95.8
EdgeServer Set	4.5		23.4	79.8
EdgeServer	4.5		23.4	79.8
Digital Quad Modems	2.1		10.9	37.2
Quad Modem NIC	1		5.2	17.7
486 NETServer	3		15.6	53.2
NET Enet NIC	1.5		7.8	26.6
NET Token NIC	2		10.4	35.5
NMC (486SX)	3		15.6	53.2
NMC Enet NIC	1.5		7.8	26.6
Dual PRI NAC	1.5		7.8	26.6
Dual PRI NIC	.5		2.6	8.9
Backplane	1.5	N/A	7.8	26.6
Fan Tray	N/A	3	73.2	249.6

Network Application Support (NAS) Backplane Pinouts

The following table lists backplane pinouts and signals. .

	Row A	S	Row B	S	Row C	S	Row D	S
1	PB_CLK33	B	GND	P	NAC_DLK	B	GND	E
2	GND	P	TDM_BITCLK	B	PB_IDO	A	CLK	F
3	PB_CLK20	B	GND	P	NAC_FCSTB	B	NIC PCI I/O V	F
4	GND	P	TDM_TSCLK	B	PB_ID1	A	RST#	F
5	PB_CLK10	B	GND	P	NIC_DD	B	User Port RXD	F
6	GND	P	TDM_FS	B	NIC_UD0-15	D	User Port DCD	F
7	PB_AD0	B	GND	P	NIC_FC0-15	D	User Port TXD	F
8	PB_AD1	B	TDM_HW1A	B	NAC_UD0-15	D	User Port DSR	F
9	PB_AD2	B	TDM_HW1B	B	NAC_DD0-15	D	User Port RTS	F
10	PB_AD3	B	GND	P	PB_ID2	A	User Port CTS	F
11	GND	P	TDM_HW5A	R	TDM_HW6A	R	User Port DTR	F
12	PB_AD4	B	TDMHW5B	R	TDM_HW6B	R	NAC Present	F
13	PB_AD5	B	GND	P	PB_ID3	A	INTB#	F
14	PB_AD6	B	TDM_HW2A	B	NIC_ID	F	GNTB#	F
15	PB_AD7	B	TDM_HW2B	B	NIC_IDCLK	F	REQB#	F
16	GND	P	GND	P	INTA#	F	-5v	P
17	PB_AD8	B	TDM_HW3A	B	GNTA#	F	REQA#	F
18	PB_AD9	B	TDM_HW3B	B	AD31	F	AD30	F
19	PB_AD10	B	GND	P	AD29	F	AD28	F
20	PB_AD11	B	TDM_HW4A	B	AD27	F	AD26	F
21	GND	P	TDM_HW4B	B	AD25	F	AD24	F
22	PB_AD12	B	GND	P	C_BE3	F	AD23	F
23	PB_AD13	B	BP_TX_TIP1 (GP)	B	AD22	F	AD21	F
24	PB_AD14	B	BP_TX_RING1 (GP)	B	AD20	F	+5V	P
25	PB_AD15	B	BP_TX_TIP2 (GP)	B	AD19	F	+5V	P
26	GND	P	BP_TX_RING2 (GP)	B	AD18	F	+5V	P
27	PB_AD16	B	TDM_HW7A	B	AD17	F	+5V	P
28	PB_AD17	B	TDM_HW7B	B	AD16	F	C_BE2	F
29	PB_AD18	B	TDM_SFSYN	B	FRAME#	F	IRDY#	F
30	PB_AD19	B	GND	P	TRDY#	F	DEVSEL#	F
31	GND	P	PB_START	B	STOP#	F	PERR#	F
32	PB_AD20	B	PB_ACK	B	SERR#	F	PAR#	F
33	PB_AD21	B	TDM_HW8A	B	C_BE1	F	AD15	F
34	PB_AD22	B	TDM_HW8B	B	AD14	F	+12V	P
35	PB_AD23	B	PB_TM0	B	AD13	F	AD12	F
36	GND	P	PB_TM1	B	AD11	F	AD10	F
37	PB_AD24	B	GND	P	AD9	F	AD8	F
38	PB_AD25	B	PB_TM2	B	C_BEO	F	AD7	F
39	PB_AD26	B	PB_TM3	B	AD6	F	-12V	P
40	PB_AD27	B	PB_ARB0	B	AD5	F	BP_TX_TIP1 (GP)	B
41	GND	P	PB_ARB1	B	AD4	F	BP_TX_RING1 (GP)	B
42	PB_AD28	B	PB_ARB2	B	AD3	F	Chassis GND	P
43	PB_AD29	B	PB_ARB3	B	AD2	F	BP_TX_TIP2 (GP)	B
44	PB_AD30	B	PB_NMRQ	B	AD1	F	BP_TX_RING2 (GP)	B
45	PB_AD31		PB_RQST	B	AD0	F	GND	E

Pin Status Legend:

P–Power pins; E–Extended signal ground pins; R–Ring bus; F–Front to back pins; D–Dedicated NMC slot to pins; B–Bussed pins (all slots); A–Hard address lines

System Standards and Specifications The following section describes industry standards implemented by HiPer ARC.

Data Compression Protocols

- Microsoft, STAC and Ascend

Software Specifications The following section lists software standards supported by HiPer ARC.

- Routing Support**
- Transparent on-demand, manual, timed, continuous and bandwidth ondemand routing
 - IP protocol routing
 - IPX protocol routing
 - Inverse multiplexing with programmable load balancing
 - Host, subnet, and network routes supported
 - Selective default routing
 - Continuous connection (automatic retries after connection loss)

- Administration**
- Local FLASH ROM for booting & configuration storage
 - Support for Domain Name Service (DNS)
 - Call activity logging
 - SNMP management - MIB II and additional proprietary MIBs
 - High Performance Access Router Manager GUI
 - TELNET command line interface
 - Tracing to console or SYSLOG host
 - Ping & traceroute utilities
 - Network and port monitoring
 - Dial-in management access
 - Password security for management access - optional
 - RADIUS and TACACS+ accounting and authentication

- Filtering & Security**
- IP, IPX, IPX RIP, IPX SAP, IP RIP, and source/destination filtering
 - Set inbound and outbound Packet Filtering independently
 - Compatible with RADIUS authentication servers
 - IP address pools
 - IP address assignment per router or port

- PPP Specific Features**
- Address and control field compression
 - STAC data compression for PPP payload
 - Protocol field compression
 - PAP and CHAP authentication protocols

- Magic number loopback detection
- Maximum receive unit negotiation
- Async control character map negotiation
- IP Address negotiation and assignment
- IPX Address negotiation and assignment
- RFC 1877 DNS NETBios server configuration
- Van Jacobson (symmetric) compression TCP/IP headers
- IPCP
- Multilink (MLPPP)
- RFC 1331, 1332, 1334 for PPP

Industry Standards Support

- TCP (Transmission Control Protocol)
- IP (Internet Protocol)
- IPX (Internet Packet eXchange)
- RIP (Routing Information Protocol) V1 and V2 with optional authentication
- CIDR (Classless Interdomain Routing)
- SLIP (Serial Line Internet Protocol)
- CSLIP (Compressed SLIP)
- CCP (Compression Control Protocol) with support for STAC algorithms
- ICMP (Internet Control Message Protocol)
- UDP (User Datagram Protocol)
- ARP (Address Resolution Protocol)
- TELNET, Rlogin, ClearTCP
- PPP (Point to Point Protocol)
- RFC 2138, 2030, 1858, 1850, 1742, 1717, 1695, 1659, 1650, 1612, 1611, 1577, 1573, 1483, 1448, 1407, 1406, 1334, 1305, 1220, 1213, 1212, 1058, 1035, 1034, and backward compatible w/ RFC 1171, 1172 and others

Client Dial-up Support

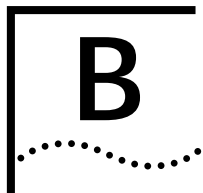
- SLIP, CSLIP, and PPP with automatic PPP detection
- TELNET and Rlogin
- Dynamic address assignment per call
- x2 support

Other Features

- Per-user packet firewall
- Dialout for ISDN/analog with HiPer DSP and Quad Modem cards

SLIP and PPP Client Software Support

We support clients which adhere to PPP, SLIP and IPCP. SLIP dialout is not supported at this time.



ADDRESSING SCHEMES

This appendix contains a brief introduction to the IP addressing schemes for administrators who are new to either one or both.

The following topics are discussed:

- IP addressing basics
- Supernetting

IP Addressing Basics

There are three address classes in IP, ranging with addresses ranges as follows: Class A - 0-127; Class B - 128 - 191; and Class C - 192 - 248.

IP addresses are 32 bits long and generally written in what is called dotted decimal notation: four decimal values separated by periods. For example, 192.77.203.5.

The same 32 bits can be divided in a number of different ways to indicate networks and subnetworks of different sizes. Imagine that the node addresses are no longer the physical addresses of your network interface cards, but arbitrary numbers that are mapped to those physical addresses later. You could then accommodate varying network structures from a small number of network segments with huge numbers of nodes to large numbers of networks with only a few nodes.

In Figure 1 below, notice that the position of this line is determined by the position of the first zero bit in the address.

	0	1	2	3	4	8	16	24	31		
CLASS A	0	NET ID				HOST ID					
CLASS B	1	0	NET ID				HOST ID				
CLASS C	1	1	0	NET ID				HOST ID			

Figure 11-1 Address Class Map

Subnetting

A large IP network can be subdivided into smaller subnetworks. This is done using a device called the subnet mask (in this text, often called netmask), which tells a routing device how to further subdivide the Host ID portion of an IP address.

A subnet mask is a 32 bit value which is written in dotted decimal notation. It contains a number of bits set to 1 (indicating the network portion of an address) followed by a number of bits set to 0 (indicating the host portion of an address).

For example, a netmask of 255.255.255.0 on a Class B network indicates that the network is divided into 254 subnetworks of 254 nodes each (0 and 255 are reserved numbers). 128.5.63.28 is host 28 on subnetwork 63 of that network. The natural network itself is called 128.5.0.0 (Class B network number 5).

Notice that by using subnet masks, you can define a natural hierarchy in which the addresses themselves indicate how a packet is to be routed. But, all routing devices on an IP network must be using the same subnetting scheme.

Also note that a subnet mask for a given network segment is not part of the address and is not transmitted with every packet. It is simply a value which is known to all the routing devices adjacent to that segment.

Subnets of Class C networks

Since Class C networks are by far the most common, subnetting in a Class C network will be examined more closely. The following table is a listing of all possible values for the last octet (byte) in a Class C subnet mask.

Mask	Binary	Subnets	Hosts/Subnet
128	10000000	0	0
192	11000000	2	62
224	11100000	6	30
240	11110000	14	14
248	11111000	30	6
252	11111100	62	2
254	11111110	126	0

Figure 11-2 Class C subnet masks

Two important points about the address divisions created by a subnet mask:

- RFC 950 requires that the first and last subnet created by a mask are reserved. So, the number of usable subnets is always 2 less than the number of divisions created. This makes 128 an unusable netmask because it has no legal subnets!
- The first and last host address in each subnet are also reserved (see *Reserved Addresses* on the next page). This means 254 is also an unusable subnet mask because there are no legal host addresses!

Reserved Addresses

In most IP machines, setting all the bits in the host portion of an IP address to 1 indicates a broadcast to all nodes on the network. In the Class B network described above, an address of 128.5.255.255 is a network broadcast address meaning the packet is destined for all nodes on the entire Class B network. 128.5.63.255 would be a broadcast address indicating that the packet is destined for all nodes on subnet 63.

But, one rare version of TCP/IP instead considers an address in which the host bits are all set to 0 a broadcast address. For HiPer ARC, you configure for this difference as part of basic setup. See the *Chapter 2: HiPer ARC Setup*.

On networks with a "high" broadcast address, setting all bits to 0 simply means "this host" or "this network" and is usually used only when a node does not know its own network or node address (and is probably requesting that information).

One other reserved address is 127.x.x.x. The contents of the last three bytes are not important. This is a loopback address used for troubleshooting. It allows you to verify that a device can send something to itself. A packet with this address should never actually leave the machine that originated it.

Supernetting (Advanced TCP/IP)

Because Class B Internet addresses are in short supply, larger networks are now usually granted a contiguous block of several Class C addresses. Unfortunately, this creates very large routing tables since multiple Class C routes have to be defined for each network containing more than 254 nodes. Larger routing tables mean more work for the routers and, therefore, poorer performance.

With traditional IP, each class C network must have a routing table entry, as shown in Figure 3 below.

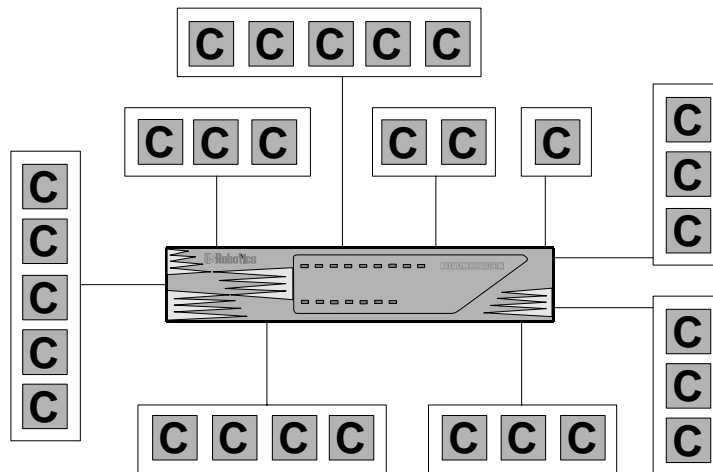


Figure 11-3 Sample Class C Routing topology

Supernetting, or CIDR (Classless InterDomain Routing) is a technique that allows each of these larger networks to be represented by a single routing table entry, as shown in Figure 4 on the next page.

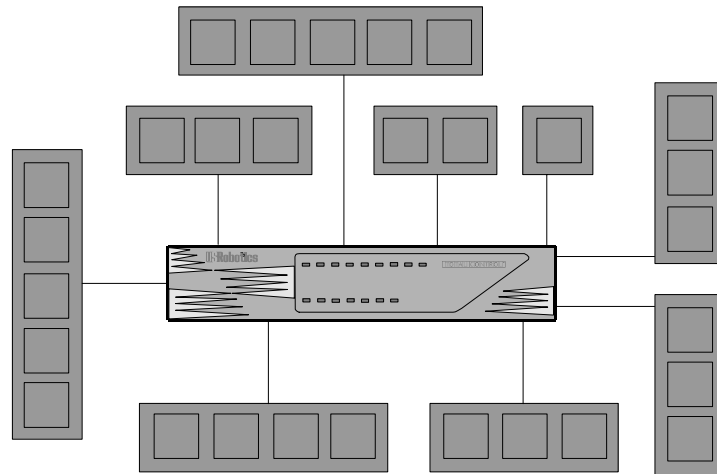


Figure 11-4 Sample Supernetting - CIDR - Topology

To do this, supernet addressing does something very different from traditional TCP/IP routing (which allows only one netmask per network). In supernet routing, each supernet can be assigned its own netmask.

Since supernet addressing is a fairly complex mechanism, the easiest way to understand it is to step through the setup process.

Step 1 - Select a netmask for each supernet

Each supernet must have a netmask assigned to it. The netmask for an individual supernet can be, but does not have to be, the same as the netmask for any other supernet.

As in subnetting, a netmask creates a division between the network portion of an address and the host portion of an address. However, since the network you are defining is *larger* than a Class C network, the division you are creating is not in the fourth octet of the address. This example creates supernets composed of fewer than 254 Class C networks. So, their netmasks are actually splitting up the third octet in their IP addresses. See Figure 5 below.

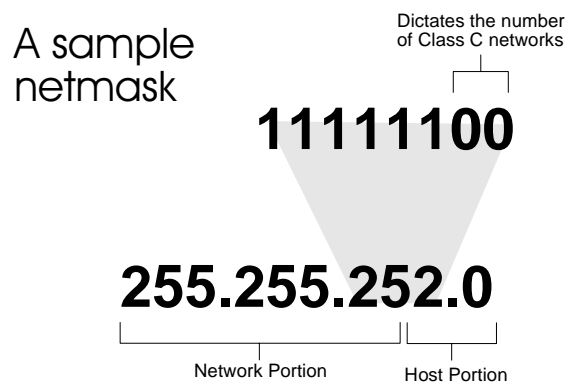


Figure 11-5 Sample CIDR Netmask

Notice that the number of zero bits in the third octet actually dictates the number of Class C networks in the supernet. Each zero bit makes the supernet twice as large. So, a supernet composed of 8 Class C networks would actually have 3 zeroes ($8 = 2^3$).

This would seem very limited since it restricts you to using groups that nicely fit into a power of 2 (1, 2, 4, 8, 16...). However, inconveniently-sized supernets can be accommodated because of a simple fact: a netmask with more 1 bits will override a netmask with fewer 1 bits.

This allows a smaller supernet to share the address space of a larger supernet. If, for example, you had a supernet of size 6 and a supernet of size 2, you could assign the larger supernet an 8 network address space and assign the smaller supernet the portion of that address space that the larger supernet was not using.

Because the smaller supernet's netmask has more 1 bits, packets whose address was part of its address space would be routed to the smaller supernet even though the address is *also* part of the address space dictated by the larger supernet's netmask.

Step 2 - Select a range of addresses for each supernet

The range of addresses in a supernet must fit exactly into a space that can be described by its netmask. This means that the zero bits in the netmask must also appear in the first address of the supernet block. For this to be true, the third octet in the address must be an even multiple of the same power of 2 used to form the netmask. For example, if you had created a block of 8 networks, the third octet in the first address will be an even multiple of 8. See Figure 6 below.

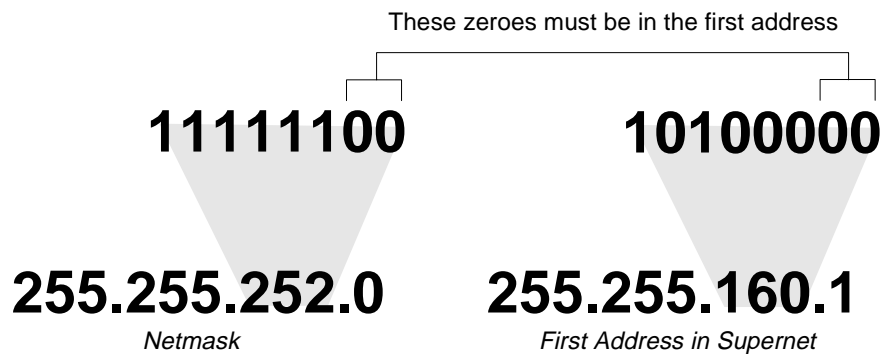


Figure 11-6 Selecting a Range of Addresses

Supernet Example

The four networks in the Figure 7 below are all connected to the same Internet service provider (ISP). The ISP has decided to use supernetting to reduce the size of his routing tables and improve throughput..

	Supernet 1	Supernet 2	Supernet 3	Supernet 4
Network	234.170.160.0	234.170.164.0	234.170.168.0	234.170.175.0
Binary Equivalents	10100000 11111100	10100100 11111100	10101000 11111000	10101111 11111111
Netmask	255.255.252.0	255.255.252.0	255.255.248.0	255.255.255.0
1st Address	234.170.160.1	234.170.164.1	234.170.168.1	234.170.175.1
Last Address	234.170.163.254	234.170.167.254	234.170.174.254	234.170.175.254

Figure 11-7 Sample Supernets

- Supernets 1 and 2 each require four Class C networks, so they require a netmask with 2 zero bits ($4 = 2^2$) in the third octet. This yields a netmask of 255.255.252.0.
- Supernet 3 requires 7 Class C address spaces. Since 7 isn't a power of 2, we have to round it up to eight. This gives it a netmask of 255.255.248.0.
- Supernet 4 is a single Class C network, making its netmask 255.255.255.0

Now, assign ranges of addresses. Assume that the ISP is responsible for the network 234.170.0.0 and that its first free addresses are at 234.170.158.0.

The third octet of Supernet 1 has to be an even multiple of 4, so the ISP grants an address range starting at 234.170.160.0 and hopes that the block between 158 and 160 can be filled in later.

Supernet 2 must also begin on an even multiple of 4. The first available address after Supernet 1 conveniently fits the bill. So, supernet 2 extends from 234.170.164.1 to 234.170.167.254.

Supernet 3 requires an even multiple of 8. It also can begin on the next available address.

Since supernet 4 can fit entirely in a single Class C address space, it can use supernet 3's surplus space. It is therefore given the last Class C address space in Supernet 3's territory, effectively reducing supernet 3 to only the 7 class C networks it needs.

Supernetting and HiPer ARC

In order to define a supernet you must add the network address and its netmask. You have two options. The first option permits you to set the subnet numerically (8-30 bits) . For example:

```
add ip network houston 192.75.202.99/23 ENTER
```

Secondly, you can specify a class designation: A, B or C. You can also leave the subnet value blank and let HiPer ARC choose it for you. In this case, however, HiPer ARC will specify a class setting based on the IP address. For example:

add ip network houston 192.75.202.99/C ENTER



To avoid confusion when configuring an IP address and subnet mask, be aware that a dialup client's subnet class designator is specified as /h (host). This occurs by default with pool addresses and specified addresses, as well as addresses learned from the client. The h designates a mask of all 1 bits (255.255.255.255).

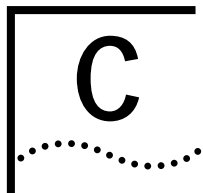
This value can be used only when the station being identified is a host. Networked nodes still require class or numeric (32 bits) subnets. For example:

set network user houston remote_ip_address 234.170.168.1/h ENTER

IP Subnet Mask Address Table

Subnet masking is used to expand the number of networks due to the 32-bit limitation of IP's address field. When assigned an address by the NIC, the address can be further broken down to expand the single net number to many more by using host bits.

Sub-net Bits	Bit Positions	Decimal Mask	HEX Mask	Sub-Nets Available	Hosts Available
Class A	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh	7	FF-00-00-00	126	16777124
Class B	10nnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh	255.255.0.0	FF-FF-00-00	16384	65534
2	10nnnnnnn.nnnnnnnn.sshhhhhh.hhhhhhhh	255.255.192.0	FF-FF-C0-00	2	16382
3	10nnnnnnn.nnnnnnnn.sshhhhhh.hhhhhhhh	255.255.224.0	FF-FF-E0-00	6	8190
4	10nnnnnnn.nnnnnnnn.sssshhhh.hhhhhhhh	255.255.240.0	FF-FF-F0-00	14	4094
5	10nnnnnnn.nnnnnnnn.sssshhhh.hhhhhhhh	255.255.248.0	FF-FF-F8-00	30	2046
6	10nnnnnnn.nnnnnnnn.ssssshhh.hhhhhhhh	255.255.252.0	FF-FF-FC-00	62	1022
7	10nnnnnnn.nnnnnnnn.ssssshhh.hhhhhhhh	255.255.254.0	FF-FF-FE-00	126	510
8	10nnnnnnn.nnnnnnnn.ssssssss.hhhhhhhh	255.255.255.0	FF-FF-FF-00	254	154
9	10nnnnnnn.nnnnnnnn.ssssssss.shhhhhhhh	255.255.255.128	FF-FF-FF-80	510	126
10	10nnnnnnn.nnnnnnnn.ssssssss.sshhhhhh	255.255.255.192	FF-FF-FF-C0	1022	62
11	10nnnnnnn.nnnnnnnn.ssssssss.sshhhhhh	255.255.255.224	FF-FF-FF-E0	2046	30
12	10nnnnnnn.nnnnnnnn.ssssssss.sssshhhh	255.255.255.240	FF-FF-FF-F0	4094	14
13	10nnnnnnn.nnnnnnnn.ssssssss.sssshhhh	255.255.255.248	FF-FF-FF-F8	8190	6
14	10nnnnnnn.nnnnnnnn.ssssssss.sssshhhh	255.255.255.252	FF-FF-FF-FC	16382	2
Class C	110nnnnnn.nnnnnnnn.ssssssss.hhhhhhhh	255.255.255.0	FF-FF-FF-00	2097152	254
2	110nnnnnn.nnnnnnnn.nnnnnnnn.sshhhhhh	255.255.255.192	FF-FF-FF-C0	2	62
3	110nnnnnn.nnnnnnnn.nnnnnnnn.sshhhhhh	255.255.255.224	FF-FF-FF-E0	6	30
4	110nnnnnn.nnnnnnnn.nnnnnnnn.sssshhhh	255.255.255.240	FF-FF-FF-F0	14	14
5	110nnnnnn.nnnnnnnn.nnnnnnnn.sssshhhh	255.255.255.248	FF-FF-FF-F8	30	6
6	110nnnnnn.nnnnnnnn.nnnnnnnn.ssssshhh	255.255.255.252	FF-FF-FF-FC	62	2
Class D	1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx				
Future	11110xxx.xxxxxxxx.xxxxxxxx.xxxxxxxx				
All 1s	11111111.11111111.11111111.11111111				
All 0s	00000000.00000000.00000000.00000000				
0 = binary 0 1 = binary 1 n = network bits h = host bits s = subnet bits x = other					



LEDs AND SWITCHES

This appendix describes the LEDs and DIP switches located on HiPer ARC.

LEDs

There are eight LEDs on HiPer ARC's front panel, as shown in Figure 1 below. The subsections that follow describe each LED function.

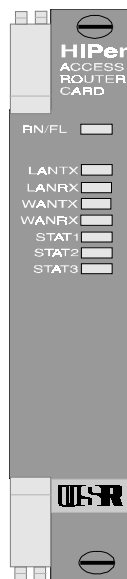


Figure 11-8 HiPer ARC LEDs

Run/Fail LED

The Run/Fail LED lets you know if the card is functioning properly. The following table lists what the Run/Fail LEDs signify except during start-up tests and software downloads (see table on next page).

Color	Meaning
Off	Power off
Green	Power on
Red	Critical failure

During start-up tests and software downloading *only*, this LED cycles through several colors as described in the following table.

Color	Meaning
Red	During start-up POST (Power On Self Test)
Amber (flashing slowly)	Checking for software download (30 seconds)
Green (flashing rapidly)	Loading an application into RAM.
Green (solid)	Normal operation

LAN TX LED Indicates packets are being transmitted through the LAN (Ethernet) interface.

Color	Meaning
Red	Interface failure
Red (flashing)	Collision (1 flash per error)
Green	Transmitting packet
Amber (flashing)	Multiple collisions, network busy
Off	Idle

LAN RX LED Indicates packets are being received from the LAN (Ethernet) interface.

Color	Meaning
Red	Interface failure
Red (flashing)	Collision, error
Green	Receiving packet
Off	Idle

WAN TX LED LED is not supported at this time.

WAN RX LED LED is not supported at this time.

Other LEDs The front panel LEDs labeled STAT1, STAT2 and STAT3 are not used at this time.

DIP Switches

HiPer ARC uses a ten-position DIP switch, as shown in Figure 2.

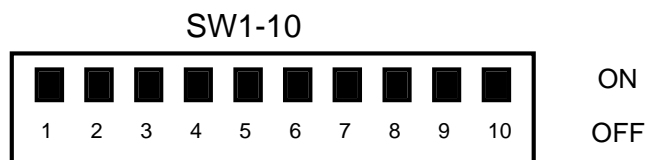


Figure 11-9 HiPer ARC DIP Switches



The factory default for all HiPer ARC DIP switches is the OFF position.

DIP Switches 1 and 2 HiPer ARC DIP switches SW-1 and SW-2 control Console port baud rate speeds as follows:

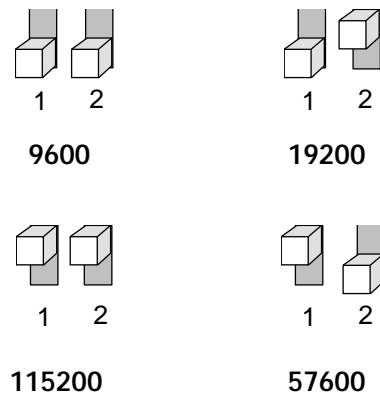


Figure 11-10 SW-1 and SW-2 Console Port Baud Rate Settings

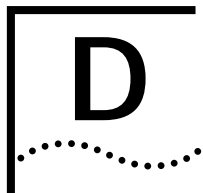
DIP Switch 5 If you plan to connect a modem to the Console port, you must turn DIP Switch 5 to the **ON** position. DIP 5 enables carrier checking for the Console port. The default position of this switch is **OFF**.

DIP Switches, 3,4 and 5 The remaining DIP switches (SW-3, SW-4 and SW-6 through SW-10) are for 3Com internal use only. Do not change these settings.

You can issue the **show board settings** command to view current DIP switch settings and a description of their function. Consult the DIP Switch Settings section of the command's output below.

DIP Switch Settings:

1	2	3	4	5	6	7	8	9	10
ON	ON	OFF	OFF	OFF	OFF	OFF	OFF	XXX	OFF
SW 1-2 UI baud rate:						115200			
SW 3 Engineering Fastboot:						DISABLED			
SW 4 Autoload application:						ENABLED			
SW 5 UI Require Carrier:						ENABLED			
SW 6 L1 Data Cache:						ENABLED			
SW 7 L1 Instruction Cache:						ENABLED			
SW 8 L2 Cache						ENABLED			
SW 9 Eng. Watchdog Disable:						(CANNOT BE READ)			
SW 10 Manufacturing Test:						DISABLED			



EVENT MESSAGES

This appendix includes information about the HiPer ARC event message facility that logs event messages to a SYSLOG host, console, or local flash file. It provides some event message examples that include descriptions of the message and suggested action you can take to correct problems.

Event Logging

The HiPer ARC event logging system logs important information about HiPer ARC processes to a number of logging sinks. Logging sinks are destinations to which event information is sent (for example, a console or SYSLOG host) in the form of event messages. HiPer ARC is capable of logging event data to:

- SYSLOG host(s)
- the Console (local)
- a local FLASH file
- a TELNET session via the **show event** command

SYSLOG Host Event Logging

You can use the SYSLOG daemon to log HiPer ARC events to one or more remote hosts. Event messages are sent to a SYSLOG server via UDP using port # 514 - the standard UDP port for SYSLOG messages.

When ICMP logging is *enabled*, the following ICMP events are logged to SYSLOG:

- Sent Dest Unreachable
- Sent ICMP TimeExceeded
- Rcvd ICMP TimeExceeded
- Sent Parameter Problem
- Rcvd Parameter Problem
- Rcvd Source Quench ICMP
- Rcvd TimeStamp REQ ICMP
- Rcvd Address Mask REQ ICMP
- Rcvd Address Mask Reply ICMP
- Rcvd Router Solicitation ICMP
- Sent Router Advertisement ICMP
- Sent ICMP Redirect (Recv'd ICMP Redirect messages are not logged)

Console Event Logging

Event messages are automatically displayed on a local console. Of all ICMP messages generated, only *Received Destination Unreachable* messages are logged to the console.

Local FLASH File Event Logging

HiPer ARC event logging maintains a file - *log-file.local* - in the FLASH file system that contains a circular buffer of the last 20 event messages generated by HiPer ARC. You can define a threshold for events written to this file. The default is *critical*, meaning only critical events are written to this file.

If HiPer ARC crashes and is rebooted, either manually or automatically, messages generated before the crash may not reach SYSLOG or Console logging facilities. But, the local FLASH file should contain the critical event messages generated just prior to the crash so that you can determine the cause of the error.

TELNET Session

All events normally directed to the Console only can also be echoed to the TELNET or dial-in session you're running by issuing a **show events** command (the **hide events** command disables the function).

Event Logging Levels

HiPer ARC processes are accomplished through a number of facilities, (for example, TELNET, SLIP, or IP routing). Various event messages are generated for each facility, and are sent to any logging sinks that you have defined. For each HiPer ARC facility, you can specify the level of event information sent.

Although the logging level of each event is fixed, you can configure the level of messages that are sent to a specific logging sink. Logging levels are:

- **Critical** - A serious system error that may affect the integrity of the system
- **Unusual** - An event that normally does not happen, but from which the system should recover
- **Common** - A normal event
- **Verbose** - A normal occurrence that happens frequently

You can configure whether event messages are sent to a logging sink according to the level of the message. For example, if you wanted to see only the *unusual* and *critical* events messages generated by the TELNET facility, you would set the event level threshold for TELNET to *unusual*.

Use the following command to list HiPer ARC facilities and their default log levels:

```
list facilities ENTER
```



*Do not confuse **set facility** and **set syslog** commands. **Set facility** determines which messages are generated on the console or to a telnetted PC - depending on the loglevel specified for each facility. The **set syslog** command, on the other hand, determines which messages are saved - depending on the global loglevel you've set for the particular SYSLOG host.*

Event Logging Counters

HiPer ARC keeps a running tab of packets successfully and erroneously generated by various processes. These *counter* commands can be used in addition to the SYSLOG to monitor system-wide performance of HiPer ARC facilities. **Show ICMP counters**, for example, details many input and output counters for ICMP packets. See *Chapter 10: Command Reference* for more information.

Using SYSLOG

This section describes how to configure HiPer ARC to send event messages to the SYSLOG host you define. The first step (below) involves setting up your SYSLOG server to receive data from HiPer ARC.

Configuring SYSLOG on the SYSLOG (UNIX) Server

On the UNIX server running the SYSLOG daemon (syslogd):

- 1 Log messages via SYSLOG to the *auth* facility at node priority *info* (*auth.info*) by editing the */etc/syslog.conf* file (as the user "root") and adding the following line:

```
auth.info /var/log/authlog
```



You can choose from eight UNIX node priorities to log your messages to. They are: alert, critical, debug, emergency, err, info, notice and warning. For example:

```
auth.alert /var/log/authlog
```

- 2 Run the following commands as the user "root". These commands, in succession, create the *authlog* file, change file privileges to execute a search by owner of the file, kill the old SYSLOG process and reload the new process.

```
touch /var/log/authlog
```

```
chmod 700 /var/log/authlog
```

```
kill -HUP `cat /etc/syslog.pid`
```



You do not have to log to a separate file, but it can be convenient.

Configuring SYSLOG Hosts on HiPer ARC

You can define separate SYSLOG hosts to which event messages are logged by the event logging level associated with the message. For example, you can configure a SYSLOG host to log event messages with a Critical logging level only, while another SYSLOG host logs Unusual or Critical event messages.

To configure a SYSLOG host, use the following CLI command:

```
add syslog <ip name or address> facility <facility_node> loglevel <loglevel choice>
```

- *ip name/address* is the network designation of the syslog host to which you want event messages sent.
- *facility* is the syslog node priority to which syslog messages are sent. The choices are:
 - *log_auth*
 - log_local0*
 - log_local1*
 - log_local2* ... and so forth to *log_local7*

For example, to define a SYSLOG host logging common, unusual, and critical events, type:

```
add syslog 191.54.42.115 facility log_auth loglevel common ENTER
```


Setting the Event Log Level

You can set the log level for each HiPer ARC facility. By setting the event log level, you define the level at which you want messages associated with the facility to be displayed on the console port. Messages associated with a selected loglevel are displayed along with any more serious log levels.

For example, if you set the event log level for the IP facility to Critical, HiPer ARC will only send *critical* event messages to the console port.

To set the log level of a facility, use the following command:

```
set facility <facility_name> loglevel <loglevel choice>
```

For example, to set the loglevel of the IP facility to Unusual (only messages that are *unusual* and *critical* are sent to the Console port) type:

```
set facility IP loglevel unusual ENTER
```

To display the list of facilities and their associated log levels, use the following command:

```
list facility ENTER
```

Event Message Examples

HiPer ARC is capable of delivering hundreds of event messages, from common events to critical events. This section describes some representative event messages that are generated by HiPer ARC facilities. Each event message is categorized by the facility by which it is generated.

The message description includes information about the meaning of the message, and if necessary, any corrective action you can take.

IP Messages

"ip_fwd_add_ondemand: ondemand route %lx exists already"

Meaning: The administrator tried to add an ondemand user that has been configured with a remote IP address already being used by another user

Action: Select a different remote IP address for the user being configured

"ip_fwd_get_opt: no more IP address available for dynamic address assignment"

Meaning: There are no more available addresses in the IP address pool

Action: Increase the size of the IP address pool using the **set ip pool** command

"ip_addr_pool_init: attempting to initialize the ip address pool with an illegal value (X), current ip address pool starting address Y. \n"

Meaning: The administrator tried to specify a starting address for the IP address pool which is illegal. The address is either '0' or has a network prefix of '0'

Action: Specify a legal IP address as the start of the pool

"ip_addr_pool_init: bad address pool range (%lx), the value must be between 1 and 254. \n"

- Meaning: The administrator tried to specify the size of the IP address pool using a value that is either too big (greater than 254) or too small
- Action: Specify a pool size that is within this range using the **set ip pool <name> size** command

"ip_send_common: on demand route, X, input queue overflow. One packet dropped\n"

- Meaning: When a call to an on-demand address is being established, IP datagrams for that address are queued. If the queue fills up before a call can be completely established, subsequent datagrams are dropped
- Action: This message is informational. No action is required

"ip_fwd_get_opt: duplicate ip address %lx\n"

- Meaning: A dial-in user tried to use an address already allocated for another dial-in user
- Action: Re-configure the dial-in user to use a different remote IP address

"ipCfmSet_ipRoute: gateway of destination X, mask Y is not reachable. static route not added\n"

- Meaning: The administrator tried to define a static route using a gateway that is not reachable via any of the existing IP routes
- Action: Specify a different gateway that has an IP address that can be reached

"proxy_arp_insert: no common network address found for remote ip address X"

- Meaning: A network user is connecting to the system using an IP address that is not on the same IP subnetwork as the network defined for the system's LAN interface. Therefore, no proxy ARPing will be performed for this user.
- Action: Informational message. No action required

"IP routes created for ondemand users cannot be deleted this way. Disable the user to delete the route."

- Meaning: The administrator tried to delete an IP route that was created for an on-demand user. These routes can only be deleted by disabling the user
- Action: Delete the route using the **disable user** command

"The route destination (X) should not contain more bits than are specified in the route mask (Y)"

- Meaning: The administrator tried to add an IP route where the network prefix of the destination contains more bits than are specified in the network mask

Action: If no netmask is specified, the natural mask of the address is assumed. To specify a host route, you must specify /H as the netmask. For example:

add ip route 204.249.182.199/H

"Failed to delete the route to X. Only routes marked as Static/NetMgt can be deleted."

Meaning: The administrator tried to delete an IP route that cannot be deleted

Action: Informational message. No action required

"Failed to create static or default route. The IP subnet for the specified gateway does not exist or is disabled."

Meaning: The administrator tried to add an IP route over an interface which is disabled or down

Action: Enable the interface before adding the route

"ip_fwd_add_ondemand: ondemand IP network address (X) conflicts with an IP network that already exists.\n"

Meaning: The administrator has defined an on-demand user whose remote IP address is already being used by an existing IP network

Action: Change the on-demand user's remote IP address to one that does not conflict with any existing networks.



Use the ***list ip net*** command to view IP network addresses currently in use.

Call Initiation Process Messages

"CIP: Unable to find an available default host for user %s, %x/n"

Meaning: The user tried to connect to a host from the login host table, but there is no available host

Action: The login host table is probably empty. Add a host to the table and let the user dial in again

"CIP: No available modem is found for modem group, %s/n"

Meaning: There is no available modem in the modem group

Action: If there is no modem available, the user should wait until one becomes available. If the modem group contains a subset of the available modems, you can add modem interfaces to this modem group

"CIP: The port is disabled for login services, %x/n"

Meaning: The user is a login user, but the interface is configured for network users

Action: Set the port_type to login_network or login

"CIP: The modem group %s already exists /n"

Meaning: The administrator tried to configure a modem group, but the modem group already exists

Action: Choose another modem group name

User Manager Messages	"AUTH: Unable to authenticate if both authentication IP's are set to 0"	
	Meaning:	The user may not be defined locally, remote authentication is not enabled, or a remote authentication IP address is not configured
	Action:	Define the user locally or configure a RADIUS server IP address
	"AUTH: Unable to account if both accounting ip's are set to 0"	
	Meaning:	Remote accounting is enabled, but no RADIUS accounting server IP addresses have been configured
	Action:	Either disable remote accounting or configure a RADIUS accounting server IP address
Filter Manager Process Messages	"AUTH - Most likely client/server configuration mismatch"	
	Meaning:	The RADIUS secret configured on HiPer ARC does not match the secret configured on the RADIUS server, or an invalid RADIUS server is trying to contact HiPer ARC
	Action:	Ensure the secret is identical on HiPer ARC and RADIUS server
	"FM: In filter file <name> had no rules for <protocol> protocol"	
	Meaning:	A filter protocol section is defined, but there are no rules associated with it.
	Action:	A protocol section must either contain at least one rule, or be commented out for the syntax to be valid
UDP Messages	"FM: In filter file <name>, previously defined section <protocol section name>"	
	Meaning:	There are two protocol sections that use the same name, for example, you defined two IP protocol sections in the filter file
	Action:	Delete one of the duplicate protocol sections
	"FM: In filter file <name>, ambiguous first line"	
	Meaning:	The filter file does not contain the required file descriptor on the first line
	Action:	Place file descriptor (#filter) on first line of file
Configuration File Manager Messages	"UDP - could not get source IP address"	
	Meaning:	HiPer ARC tried to send a UDP message (for example, an SNMP trap or syslog message) with no IP networks enabled
	Action:	Create an IP network
	"Could not get my own Mailbox Handle."	
	Meaning:	The Configuration File Manager process could not resolve its own mailbox
	Action:	Reboot the system

"Could not resolve @mailbox://MIBRegistrar."

Meaning: The Configuration File Manager could not resolve the MIB Registrar's mailbox

Action: Reboot the system

"The configuration file <filename> is corrupt. Status <error status>."

Meaning: The Configuration file has been corrupted. It will be renamed to <filename>.bad

Action: Keep a copy of the <filename>.bad file. If the file was uploaded to using TFTP, upload the file again making sure the TFTP transfer mode is set to octet

"Could not create a list for CFM Control Structures. Status: <error status>."

Meaning: The Configuration File Manager could not allocate the resources necessary for normal operation

Action: Reboot the system

TELNET Messages**"CIP_GET_SHARED_DEV_REQ failed: no modems available"**

Meaning: A user is attempting to TELNET to HiPer ARC to perform modem sharing, but there are no free modems available for the group defined

Action: Use the **list service** command to see which modem group is configured. Determine why all modems in the modem group are being used

"User X attempted CLI access without dial-out privileges. \n"

Meaning: A user is attempting to TELNET to HiPer ARC to perform modem sharing using a valid username and password, but the user profile does not have dial-out enabled

Action: Use the **set user <name> type dial_out** command to enable dial-out privileges for the user

IP Dial-out Process Messages**"INIT: Could not allocate a private data area. Status: <error status>."**

Meaning: The dial-out process could not allocate enough memory for its data. The dial-out process will not be started

Action: Free some memory, for example, delete some users. Once some memory has been freed, save the configuration and reboot the system

"Could not register socket <socket> with the IP forwarder. Status: <error status>(<error value>)."

Meaning: The dial-out process failed to register its socket with the IP forwarder. The IP dial-out service will not be started

Action: Ensure the IP forwarder process is running by using the **list processes** command. Ensure that there is an IP network defined. Reboot the system and re-enable the dial-out service

"Could not unregister socket <socket> with the IP forwarder. Status: <error status>(<error value>)."

- Meaning: The dial-out process failed to unregister its socket with the IP forwarder. This message is displayed only when disabling the dial-out network service
- Action: When the IP dial-out service reaches this state, it cannot be enabled again without rebooting. Reboot the system

"Could not register the IP Dial-out service with SAP. Status: <error status>(<error value>)."

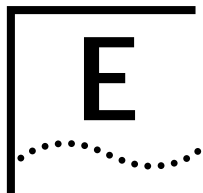
- Meaning: The dial-out process failed to register the IP dial-out service with the SAP process. The IP dial-out service will not be started
- Action: If the dial-out service is enabled, disable the dial-out service and re-enable the dial-out service. If message is displayed again, reboot the system

"Could not set the IP ACS timer. Status: <error status>(<error value>). The IP Dial-out service will be automatically disabled."

- Meaning: The dial-out process could not start its service timer. This timer is required for normal operation. The dial-out network service will not be enabled
- Action: A system error occurred. If re-enabling the dial-out network service fails, reboot the system

"There are no interfaces assigned to the Dial-out process' modem groups."

- Meaning: The dial-out process detected that there were no interfaces contained in the modem group it was assigned to use
- Action: Verify that at least one interface has been assigned to the dial-out service's modem group. If no interface is assigned, add at least one interface to the dial-out service's modem group and re-enable the dial-out service



RADIUS AND TACACS+ SYSTEMS

Remote Authentication Dial In User Service (RADIUS) is a distributed security system that secures remote access to networks and network services against unauthorized access. This chapter describes:

- HiPer ARC RADIUS enhancements
- How RADIUS works
- CHAP Authentication
- Configuring RADIUS authentication and accounting from the CLI
- RADIUS examples by user type
- Chat scripting with RADIUS users
- RADIUS security server user table entries
- TACACS+ authentication, authorization and accounting support
- Configuring TACACS+ AAA service

HiPer ARC RADIUS Enhancements

HiPer ARC provides user authentication and session accounting locally using a user table defined by the administrator. Also, you can use the RADIUS authentication server for centralized authentication services on your network.

HiPer ARC integrates the following enhanced RADIUS features:

- 128 challenge responses up to 128 bytes.
- A filter rule format allowing filter names and rules to be downloaded to the RADIUS client.
- Dynamic RADIUS server changes of a user's filter rules.
- Increased RADIUS security through RADIUS server verification of source IP address and UDP port.
- Configuration of one secret and UDP port per server.

RADIUS Authentication

The RADIUS authentication process consists of two parts: an authentication server and RADIUS client. The authentication server is installed on a machine on your network. HiPer ARC acts as a RADIUS client, sending authentication requests to the authentication server, and acting on responses (with remote authentication enabled) sent back from the authentication server. RADIUS authentication, as well as local authentication, is on by default although RADIUS service must be configured on HiPer ARC.

RADIUS Accounting

The RADIUS accounting server can perform session accounting for the Hub. Session accounting information includes date and time, user information and service type. When RADIUS accounting is enabled, HiPer ARC forwards an accounting record of each session for storage on the accounting server.



The HiPer ARC SYSLOG facility also performs local session accounting. For more information about SYSLOG accounting, refer to Appendix D: Event Messages.

Obtaining RADIUS

HiPer ARC software has built in *client* support for RADIUS authentication and accounting. 3COM also makes available a RADIUS Security and Accounting server in support of the client/server relationship. Since RADIUS is an open standard, there are other RADIUS server implementations on the market but 3Com's platform is optimized for use with HiPer ARC. Contact your 3Com sales representative for more information.

Performing Authentication

You can perform user authentication using HiPer ARC's local authentication facility, RADIUS authentication, or both.

The local authentication facility lets you define a user table stored in HiPer ARC FLASH memory. Local and RADIUS authentication are enabled by default but you can enable or disable each using the CLI. If you enable and configure:

- *Local authentication only* - HiPer ARC grants or denies access based on information in the local user table only.
- *RADIUS authentication only* - HiPer ARC sends a request to the RADIUS server and grants or denies access based on the response.
- *Both local and RADIUS authentication* - HiPer ARC first checks the local user table. If the user is defined in the local user table, HiPer ARC grants or denies the user access based on information in the table. If the user is not defined in the user table, HiPer ARC sends a request to the RADIUS server and grants or denies access based on the response.

RADIUS Authentication Process

When a user dials up HiPer ARC, and local authentication is enabled, HiPer ARC first checks its own user table. If it can not find the user, it then checks with the RADIUS server. If a local entry is found, RADIUS authentication is not tried.

HiPer ARC encrypts the user's password using a key shared by both HiPer ARC and the RADIUS server, and passes the user name and encrypted password on to the RADIUS server. The RADIUS server then checks the user name and password against its users file, determines whether to grant or deny access, and passes this information back to HiPer ARC. If access is denied, HiPer ARC disconnects the user. If access is granted, the RADIUS server will forward the appropriate user configuration information (such as what host or what protocol the user needs) to HiPer ARC.

CHAP Authentication Using RADIUS

If you want HiPer ARC to let RADIUS authenticate a remote device, a user name and password of the remote device can be stored in the users file on the RADIUS server.

The user name of the remote device must be the user ID it will send during CHAP authentication. The password must be in clear text in order for the MD5/MD4 comparison to succeed. The remote device uses the same password. If HiPer ARC does not have a user table entry for the remote device, there must be an entry for the remote device in the RADIUS users file.

Configuring RADIUS from the CLI

This section provides descriptions of CLI commands used to manage the RADIUS security server authentication process. Topics include:

- Configuring RADIUS authentication settings
- Enabling and disabling authentication

Configuring RADIUS Authentication Settings

This section assumes the RADIUS security server is up and running on a PC on your network.

Use the following CLI command to configure RADIUS authentication settings:

```
set authentication
  primary_port <port_number>
  primary_secret <string>
  primary_server <name_or_ip_address>
  secondary_port <port_number>
  secondary_secret <string>
  secondary_server <name_or_ip_address>
  tertiary_port <port_number>
  tertiary_secret <string>
  tertiary_server <name_or_ip_address>
  retransmissions <number>
  timeout <seconds>
```

Configure RADIUS accounting parameters by setting the following values. Each step describes a parameter and step 8 combines them in an example.

- 1 Select the *primary* RADIUS security server. Use the following command:

```
set authentication primary_server <ip_address>
```

- 2 *Optional.* Select the *secondary* RADIUS security server (and tertiary server if required). Use the following command:

If your network has more than one RADIUS server, indicate which one will be considered the secondary server. If for some reason the primary server is unavailable, HiPer ARC will check with the secondary server.

```
set authentication secondary_server <ip_address>
```

- 3 Set the *primary encryption key* or secret. Use the following command:

This is the first key HiPer ARC uses to encrypt passwords and the RADIUS server uses to decrypt them. The RADIUS server(s) must be set to the same secret (encryption) key. The encryption key is entered into the "clients" file for the RADIUS server. The encryption key can be up to 15 characters long. Refer to your RADIUS documentation for more information. Use the following command:

```
set authentication primary_secret <encryption key>
```

- 4 Optional. Set the secondary (and tertiary, if required) secret key. Use the following command:

```
set authentication secondary_secret <encryption key>
```

- 5 Set the number of *retransmissions*. This value is the total number of times HiPer ARC will re-transmit an authentication request to both primary and secondary RADIUS servers. Use the following command:

```
set authentication retransmissions <count>
```

- 6 *Optional.* For additional security, configure *UDP ports* to an unused UDP port number for one or all three servers. This setting vacates the default port of 1645. Use the following command:

```
set authentication primary_port <port_number>
```

or

```
set authentication secondary_port <port_number>
```

- 7 Set the *interval* (in seconds) between retransmissions. Use this command:

```
set authentication timeout <number_seconds>
```

- 8 Configure the accounting server and save the changes. Use these commands:

For example:

```
set authentication primary_server 3.3.3.2 secondary_server 3.3.3.4 primary_secret
nuncio secondary_secret pope use_servers both retransmissions 3 start_time
connection timeout 60 primary_port 5555 secondary_port 5556 <ENTER>
```

```
save all <ENTER>
```

Enabling and Disabling Authentication

You can use CLI commands to enable and disable both RADIUS and local authentication. By default, both local and RADIUS authentication are enabled.

Use the following CLI commands to enable and disable authentication:

```
enable authentication [local | remote]
```

```
disable authentication [local | remote]
```

Configuring RADIUS Accounting Settings

HiPer ARC sends frames to the RADIUS accounting server that enable RADIUS to perform accounting functions. The RADIUS accounting server uses the same basic protocol as the RADIUS security server. Both servers may run on the same host, but you may choose a different host to provide each function. This section describes:

- Configuring RADIUS accounting settings
- Enabling and disabling RADIUS accounting
- RADIUS accounting examples

Configuring RADIUS Accounting Settings

Use the following CLI command to configure RADIUS accounting settings:

```
set accounting
primary_port <port_number>
```

```

primary_secret <string>
primary_server <name_or_ip_address>
retransmissions <count>
secondary_port <port_number>
secondary_secret <string>
secondary_server <name_or_ip_address>
start_time <authentication | connection>
timeout <seconds>
use_servers <one | both>

```

Configure RADIUS accounting parameters by setting the following values. Each step describes a parameter and step 9 combines them in an example.

- 1 Select the *primary* RADIUS accounting *server*. Use this command:

```
set accounting primary_server <ip_address>
```

- 2 *Optional.* Select the *secondary* RADIUS accounting *server*. If your network has more than one RADIUS accounting server, indicate which one will be considered the secondary server. If for some reason the primary server is unavailable, HiPer ARC will check with the secondary server. Type:

```
set accounting secondary_server <ip_address>
```

- 3 Set the primary and secondary secret (encryption) keys.

These are the first and secondary encryption key that HiPer ARC uses to encrypt passwords and the RADIUS server uses to decrypt them. Specify with a string of up to 15 ASCII characters for each server. Use the following commands:

```
set accounting primary_secret <string>
```

```
set accounting secondary_secret <string>
```

- 4 Determine whether accounting information is sent to the primary server only (the secondary server acts as a backup) or whether accounting information is sent to both the primary and secondary servers until a response is received from both servers. Use the following command:

```
set accounting use_servers [one | both]
```

- 5 Set the number of *retransmissions*. *This is the total number of times HiPer ARC will re-transmit an authentication request to both the primary and secondary RADIUS servers.* Type:

```
set accounting retransmissions <count>
```

- 6 Set the time at which HiPer ARC begins accounting, either at the point of authentication or the point of connection. Use this command:

```
set accounting start_time [authentication | connection]
```

- 7 Set the *interval (in seconds) between retransmissions*. Use this command:

```
set accounting timeout <number_seconds>
```

- 8 *Optional.* For additional security, configure UDP ports to an unused port number for one or both servers. This setting overrides the default port of 1646. Use the following command:

```
set accounting primary_port <port_number>
```

```
set accounting secondary_port <port_number>
```

9 Configure the accounting server and save the changes.

For example:

```
set accounting primary_server 2.2.2.2 secondary_server 2.2.2.3 primary_secret bishop
secondary_secret cardinal use_servers both retransmissions 3 start_time connection
timeout 60 primary_port 4444 secondary_port 4445 <ENTER>
```

```
save all <ENTER>
```

Enabling and Disabling RADIUS Accounting

RADIUS accounting is enabled by default, and can be enabled or disabled from the CLI.

Use the following CLI commands to enable and disable authentication:

```
enable accounting <ENTER>
```

```
disable accounting <ENTER>
```



SYSLOG accounting is always enabled as long as a SYSLOG sink is defined. For more information about SYSLOG accounting, refer to Appendix D: Event Messages.

RADIUS Accounting Examples

Here are a few examples of RADIUS accounting output. The first describes a login user who has just begun a session.

```
Thurs Jan 16 22:00:55 1995
Acct-Session-ID="06000003"
User-Name=cindyg
Acct-Status-Type=Start
Acct-Authentic=RADIUS
User-Service-Type=Login-User
Login-Host=NY_Sales
Login-Service=Telnet
```

When the user above ends the session with the host, a record like the one below is sent to the accounting server:

```
Thurs Jan 16 23:15:31 1995
Acct-Session-Id="06000003"
User-Name=cindyg
Acct-Status-Type=Stop
Acct-Authentic=RADIUS
Acct-Session-Time=4476
User-Service-Type=Login-User
Login-Host=NY_Sales
Login-Service=Telnet
Acct-Delay-Time=0
```

If a PPP or SLIP (framed) user begins a session with the network, a record like the one below is sent to the accounting server:

```
Thurs Jan 16 16:15:53 1995
Acct-Session-Id="06000004"
User-Name=harryk
Client-Id=201.123.234.79
Client-Id-Port=5
Acct-Status-Type=Start
Acct-Authentic=Local
User-Service-Type=Framed-User
Framed-Protocol=PPP
```

```
Framed-Address=122.132.124.152
Framed-Netmask=255.255.124.0
```

When the framed user ends the session, a record like the one below is sent to the accounting server:

```
Thurs Jan 16 16:25:57 1995"
Acct-Session-Id="06000004"
User-Name=harryk
Client-Id=201.123.234.79
Client-Id-Port=5
Acct-Status-Type=Stop
Acct-Session-Time=664
Acct-Authentic=Local
User-Service-Type=Framed-User
Framed-Protocol=PPP
Framed-Address=122.132.124.152
Framed-Netmask=255.255.124.0
Acct-Delay-Time=0
```

RADIUS Examples by User Type

The tables below describe examples of RADIUS configurations by user type. RADIUS *packet types* are listed as well as the *Vendor Specific Attribute* (VSA) number, the *Attribute ID*, and the *Attribute Name*. User types displayed are:

- Terminal user with incorrect password
- Terminal user with correct password (TELNET, Rlogin, ClearTCP)
- Administrative user
- Terminal user with port tapping enabled
- Framed user with port tapping enabled
- L2TP framed user/PPP-SLIP framed user
- Terminal login-callback user
- Framed user with multilink PPP enabled
- Dialback user

Terminal user with incorrect password

The access reject packet is exactly the same no matter what the condition.

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
Access Reject		12	Reply Message

Terminal user with correct password (TELNET, Rlogin, ClearTCP)

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
Access Response	429	9843	Interface-Index
		06	Service-Type
		3D	NAS-Port-Type
		0E	Login-IP-Host
		0F	Login-Service
		10	Login-Port
		13	Callback-Number
		1C	Idle-Timeout
		1B	Session-Timeout
Accounting Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect_Speed
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
Accounting Stop		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic

		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets

Administrative Terminal User

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
Access Response		06	Service-Type
	429	9843	Interface-Index
		3D	NAS-Port-Type
		0E	Login-IP-Host
		0F	Login-Service
		10	Login-Port
		1C	Idle-Timeout
		1B	Session-Timeout
Accounting Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		3D	NAS-Port-Type
		06	Service-Type
		05	NAS-IP-Port

	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
Accounting Stop		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets

Terminal User with Port Tapping Enabled

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
Access Response		06	Service-Type

		3D	NAS-Port-Type
	429	9843	Interface-Index
		0E	Login-IP-Host
		0F	Login-Service
		10	Login-Port
		1C	Idle-Timeout
		1B	Session-Timeout
	429	9845	Port-Tap
	429	9846	Port-Tap-Format
	429	9847	Port-Tap-Output
	429	9848	Port-Tap-Facility
	429	9849	Port-Tap-Priority
	429	984A	Port-Tap-Address
Accounting Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	9023	Initial-Connect-Rate
	429	00C7	Compression-Type
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
Accounting Stop		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type

	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets

Framed User with Port Tapping Enabled

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
Access Response		06	Service-Type
		0E	Login-IP-Host
		0F	Login-Service
		10	Login-Port
		1C	Idle-Timeout
		1B	Session-Timeout
	429	9845	Port-Tap
	429	9846	Port-Tap-Format
	429	9847	Port-Tap-Output
	429	9848	Port-Tap-Facility
	429	9849	Port-Tap-Priority
	429	984A	Port-Tap-Address
Accounting Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id

	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
Accounting Stop		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets

L2TP Framed User/PPP-SLIP Framed User

Attribute Name	VSA ID (if any)	Attribute ID	Attribute Name
User-Name		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
Access Response		06	Service-Type
		07	Framed-Protocol
		40	Tunnel-Type
		09	Framed-IP-Netmask
		0C	Framed-MTU
		08	Framed-IP-Address
	429	43	Tunnel-Server-Endpoint
		65	Tunnel-Medium-Type
Accounting Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	Port-Limit
		40	Tunnel-Type
		41	Tunnel-Medium-Type
		43	Tunnel-Server-Endpoint
		05	NAS-IP-Port
		44	Acct-Tunnel-Connection-Id
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		07	Framed-Protocol
		08	Framed-IP-Address
	429	9842	Modem-Training-Time
	429	982F	Multilink-PPP-Receive-Unit
		33	Acct-Link-Count
		32	Acct-Multi-Session-Id
Accounting Stop		01	User-Name

		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		40	Tunnel-Type
		41	Tunnel-Medium-Type
		43	Tunnel-Server-Endpoint
		44	Acct-Tunnel-Connection-Id
		05	Acct-Tunnel-Connection-Id
		3D	Port-Limit
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		07	Framed-Protocol
		08	Framed-IP-Address
	429	9842	Modem-Training-Time
	429	982F	Multilink-PPP-Receive-Unit
		33	Acct-Link-Count
		32	Acct-Multi-Session-Id
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets
		2F	Acct-Input-Packets
		30	Acct-Output-Packets

Terminal Login-Callback User

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
Access Response		06	Service-Type
		0E	Login-IP-Host
		0F	Login-Service
		10	Login-Port
		13	Login-Callback-Number

		1C	Idle-Timeout
		1B	Session-Timeout
Accounting Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	Port-Limit
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
Accounting Stop		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	Port-Limit
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Calling-Station-Id
		1E	Called-Station-Id
		006C	Modulation-Type
		0099	Error-Control
		00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets

Framed User with Multilink PPP Enabled

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface Index
		06	Service-Type
		07	Framed-Protocol
	429	9841	MP-EDO-HIPER
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
Access Response	429	9843	Interface-Index
	429	9841	MP-EDO-HIPER
		3D	NAS-Port-Type
		06	Service-Type
		07	Framed-Protocol
		09	Framed-IP-Netmask
		0C	Framed-MTU
		0A	Framed-Routing
		08	Framed-IP-Address
	429	900F	Primary-DNS-Server
	429	9010	Secondary-DNS-Server
		1C	Idle-Timeout
		1B	Session-Timeout
	429	9802	Max-Channels
	429	9803	Channel-Expansion
	429	9804	Channel-Decrement
	429	9805	Expansion-Algorithm
	429	9806	Compression-Algorithm
	429	9807	Receive-Acc-Map
	429	9808	Transmit-Acc-Map
	429	9809	Compression-Reset-Mode
	429	980A	Min-Compression-Size
Accounting Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	NAS-Port-Type
		05	NAS-IP-Port
		9842	Modem-Training-Time
		9843	Interface Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Caller-Id

		1E	Client-Port-DNIS
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		07	Framed-Protocol
		08	Framed-IP-Address
	429	9842	Modem-Training-Time
	429	982F	MP-MRRU
	429	9841	MP-EDO-HIPER
		33	Acct-Multi-Session-Id
		32	Acct-Link-Count
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets
		30	Acct-Output-Packets
Accounting Stop		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	Port-Limit
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Caller-Id
		1E	Client-Port-DNIS
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
	429	9842	Modem-Training-Time
	429	982F	MP-MRRU
	429	9841	MP-EDO-HIPER
		32	Acct-Link-Count
		33	Acct-Multi-Session-Id
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets
		2F	Acct-Input-Packets
		30	Acct-Output-Packets
		DE	User-ID
		20	NAS-Identifier

Dialback User

Type of Packet	VSA ID (if any)	Attribute ID	Attribute Name
Access Request		01	User-Name
		02	User-Password
		04	NAS-IP-Address
		05	NAS-IP-Port
		2C	Acct-Session-Id
	429	9843	Interface-Index
		06	Service-Type
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
		1E	Called-Station-Id
		1F	Calling-Station-Id
		3D	NAS-Port-Type
		06	Service-Type
Access Response		0E	Login-IP-Host
		0F	Login-Service
		10	Login-Port
		1C	Idle-Timeout
		1B	Session-Timeout
	429	9817	Send-Script1
	429	9818	Reply-Script1
	429	9819	Send-Script2
	429	981A	Reply-Script2
	429	981B	Send-Script3
	429	981C	Reply-Script3
	429	981D	Send-Script4
	429	981E	Reply-Script4
	429	981F	Send-Script5
	429	9820	Reply-Script5
	429	9821	Send-Script6
Access Start		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	Port-Limit
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Caller-Id
		1E	Client-Port-DNIS
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port

		0E	Login-IP-Host
Accounting Stop		01	User-Name
		04	NAS-IP-Address
		28	Acct-Status-Type
		2C	Acct-Session-Id
		29	Acct-Delay-Time
		2D	Acct-Authentic
		06	Service-Type
		3D	Port-Limit
		05	NAS-IP-Port
	429	9842	Modem-Training-Time
	429	9843	Interface-Index
	429	9019	Chassis-Call-Slot
	429	901A	Chassis-Call-Span
	429	901B	Chassis-Call-Channel
	429	901D	Unauthenticated-time
		1F	Caller-Id
		1E	Client-Port-DNIS
	429	006C	Modulation-Type
	429	0099	Error-Control
	429	00C7	Compression-Type
	429	9023	Initial-Connect-Rate
		0F	Login-Service
		10	Login-Port
		0E	Login-IP-Host
	429	9842	Modem-Training-Time
	429	982F	MP-MRRU
	429	9841	MP-EDO-HIPER
		32	Acct-Link-Count
		33	Acct-Multi-Session-Id
		2E	Acct-Session-Time
		31	Acct-Terminate-Cause
		2A	Acct-Input-Octets
		2B	Acct-Output-Octets

Chat Scripting with the RADIUS User

Two new VSA attributes have been created to permit the use of Chat Scripting for RADIUS users. Chat-style scripting is designed to support interaction with HiPer ARC after a user dials in, including setting up a TELNET session, echoing IP addresses, and runtime errors, setting timeouts, and disconnecting the call.

The *Chat_Script_Name* attribute (0x9865) refers to a file stored locally in HiPer ARC FLASH memory which contains all chat interactions in ASCII-formatted text. After successful authentication, if a user is found to have this attribute and if the corresponding script file exists in FLASH, script processing will begin for the user and the commands in the script file will be executed. Any user login-service or service-type attributes are ignored when chat scripting occurs and normal HiPer ARC processing is ignored when this attribute is configured.

Another means of building a chat script permits the explicit insertion of chat rules in the RADIUS user's attribute list. The *Chat_Script_Rules* attribute (0x9866) can be multi-valued (reflecting any parameters spelled out in the RADIUS user profile). Chat script values are concatenated and executed upon successful authentication. Again, when configured, a user's normal processing by HiPer

ARC is replaced by processing of the rules obtained from the Chat-Script-Rules attribute. If the script attribute is absent for a user, regular processing is done by HiPer ARC.

Chat scripting allows backwards compatibility with existing users. Those users on earlier-supported platforms can be converted by simply adding the VSA attribute to the RADIUS/Local database and TFTP'ing the script file to HiPerARC (if necessary).

Chat scripting can also be done locally from the HiPer ARC CLI. See *Chapter 10: Administrative Tools* and *Chapter 11: CLI Reference*, for more information.

Syntax The chat script consists of *SEND*, *EXPECT* and *conditional* constructs. Commands such as TELNET are also available. Variables can be implicitly declared, assigned and used in the script. The following rules apply:

- Value - *string*
- Comparison allowed - ***equal*** (=) and ***not-equal*** (!=)
- Variables are considered **case-sensitive** when making comparisons
- Statements must end with a ***semi-colon*** (;)
- Lines can be commented out with the usual C syntax */* ... */* which spans multiple lines. The *'''* syntax comments out the rest of the line.

For example:

```
SEND 'Hello';
EXPECT %login_host;
SEND "Telnetting to " $login_host "\n";
//Invoke a telnet session
TELNET $login_host;
HANGUP
```

- Conditional checking and jump statements are provided
- Multiple conditional values must be checked by inserting multiple *IF* statements.

For example:

```
IF ($login_host == "ash.alien.usr.com") GOTO ash;
IF ($login_host == "bishop.alien.usr.com") GOTO bishop;
```

- Labels must be present in the script, otherwise a compilation error will occur.

SEND construct The *SEND* construct outputs strings and values of variables to a user. String portions must be enclosed within matching single (') or double (") quotes, but variables need not. Use the sequence *"\n"* to output a new-line.

For example:

```
SEND "Hello" "Welcome to HiPerARC";
SEND "\n";
SEND "Your IP address is " $ip_address "\n";
SEND "Your Gateway is '$ip_gateway '\n";
```

Timeout A timeout value can be specified when expecting input from a user. It is expressed in seconds.

If a timeout occurs before a user's input is completed (the input must be followed by a new-line character) OR, if whatever was entered does not match the expected input, the system variable *\$NO_MATCH* gets set to "TRUE". The usage for *\$NO_MATCH* is explained below.

The timeout construct is independent of the *IDLE_TIMEOUT* and *SESSION_TIMEOUT* user attributes also supported by HiPerARC and can run concurrently with this construct.

A timeout example:

```
TIMEOUT 60;
```

Timeout value is reset during each execution of an *EXPECT* statement. In the code fragment below, the timer is reset each time the *EXPECT* statement is run:

For example:

```
TIMEOUT 30;
start:
EXPECT %host_name;
SEND $host_name;
GOTO start;
```

EXPECT construct The *EXPECT* statement reads input from a user and an exact pattern match is performed on the strings. One or more variable names can be specified in the *EXPECT* statement (each variable is preceded by the percentage (%) sign). Any name can be used for these variables (e.g. %one %ip_addr, etc.) The user's input is assigned to these variables using *white* space as the separator (blank, tab characters).

For example:

```
EXPECT "Hello";
EXPECT "Telnet" %ip_addr %port_number;
```

If there are fewer variables in the expect statement than what the user inputs, the assignment is made from left to right and additional inputs are discarded.

For example:

```
EXPECT "Telnet" %ip_addr %port_number;
```

In the previous example, if a user types: *Telnet 149.112.213.1*, then the *port_number* will be a NULL string (""). Also, if the user types more than the expected number of variables, additional inputs are discarded.

For example, if the user types: *Telnet 149.112.213.1 23 1024*, the last token (1024) is discarded.

If input does not match the expected string, then the system variable *\$NO_MATCH* is set to "TRUE". This variable is also set if a timeout occurred while in the expect statement. Usage for *\$NO_MATCH* is detailed below.

Conditional constructs

An *IF* construct is supported to check for values of variables. The *IF* statement is followed by an expression and a *GOTO* construct. The only possible expressions are '=' which checks for equality, and '!=' which checks for non-equality. The goto statement refers to a label which must be present somewhere in the script.

If the script has a TIMEOUT construct, then the timeout value applies for each expect statement. If the timeout expires before the user completes input, the system variable *\$NO_MATCH* is set to "TRUE". This value must be compared after the expect statement as follows:

```
IF ($NO_MATCH == "TRUE") GOTO match_fail;
GOTO match_success;
match_fail:
SEND "Time out occurred or User Input did not match; Please try again. \n";
GOTO input_again;
match_success:
SEND "Match succeeded! \n";
```

Examples of IF usage:

```
TIMEOUT 30;
start:
EXPECT %ip_addr %port_number
IF ($NO_MATCH == "TRUE") GOTO start;
IF ($ip_addr == "149.112.213.1") GOTO do_telnet;
GOTO start;
do_telnet:
TELNET $ip_addr $port_number;
```

Action Statements

The *ACTION* statement currently supported are TELNET, RLOGIN and PPP.

TELNET

This takes the login host name or IP address as the first argument and a port number as the second argument. Port number is optional.

For example:

```
TELNET '149.112.213.3';
TELNET $login_host $tcp_port;
```

The *\$login_host* in the example above can be a host name (DNS lookup is performed on this value) or an IP address.

RLOGIN

This action statement allows a user to rlogin from the chat-script. You can provide the user-name for this command as follows:

```
RLOGIN login-host-name or ip-address [user-name]
```

For example:

```
RLOGIN "149.112.213.3";
RLOGIN $login_host $user_name;
RLOGIN "149.112.213.1" "john";
```

PPP

This action statement starts PPP from the chat-script. PPP supplies authentication of the user via PAP/CHAP.

For example:

```
PPP;
```

Disconnecting the call

A chat script can issue a *HANGUP* command at any time during processing. The following construct is used without any arguments:

```
HANGUP
```

The call is automatically hung up after completion of a TELNET session to a remote host.

Miscellaneous constructs

By default, input received from the user is case-sensitive. The *UPCASE* construct converts the variable into uppercase before performing the comparison.

For example:

```
IF (UPCASE($host_name) == "ASH.ALIEN.USR.COM") GOTO telnet_ash;
```

Run time errors

HiPer ARC detect *tight-loops* and drops the connection in such cases. A tight-loop is defined as one where no expect statement is executed, and a *GOTO* statement carries execution back to an original point. The loop is executed 100 times before a run-time error is detected, an error message is sent to the user and the connection is dropped.

For example:

```
EXPECT %host_name;
begin:
SEND "Host name is " $host_name;
IF ($host_name != "ash.alien.usr.com") GOTO begin;
TELNET $host_name;
```

Script Examples**Example A**

Use this script to TELNET to either of two fixed hostnames (*abc.com* or *def.com*) depending upon user's input.

```
TIMEOUT 60;
begin:
SEND "Enter Remote Host Name:";
EXPECT %login_host;
IF ($login_host == "abc.com") GOTO do_telnet;
IF ($login_host == "def.com") GOTO do_telnet;
IF ($login_host == "logout") GOTO exit;
SEND "Invalid choice";
GOTO begin;
do_telnet:
TELNET $login_host;
exit:
HANGUP
```

Example B

Use the following script to offer the user multiple choices.

```

TIMEOUT 60;
start:
SEND "Enter a number from one of the choices below:";
// SEND "1. PING";
SEND "2. TELNET";
SEND "3. HANGUP";
EXPECT %number;
// IF ($number == "1") GOTO ping;
IF ($number == "2") GOTO do_telnet;
IF ($number == "3") GOTO exit;
SEND "Invalid choice.";
GOTO start;
// ping:
// SEND "Enter Ping destination:";
// EXPECT %login_host_ip_address;
// PING $login_host_ip_address;
// GOTO exit;
do_telnet:
SEND "Enter Telnet destination IP address and port:";
EXPECT %login_host_ip_address %tcp_port;
TELNET $login_host_ip_address $tcp_port;
exit:
HANGUP

```



Note that PING is not currently supported.

Example C

This script supports a Sprint-style script.

/* This sample script can specify the user input as either **lightship.airborn.dialnet.net** or **TerminalDownload** or **Terminal Download**". In the first case the user TELNETs to the host directly. In the latter two cases, some abbreviations of Terminal download are allowed. Another prompt ">" is then sent to the user who is expected to type in the remote host name and an optional port number. */

```

start:

TIMEOUT 10;
SEND "sdn-ts>" ;
EXPECT %one %two;
IF($one == "lightship.airborn.dialnet.net") GOTO send_Menu;
IF(UPCASE($one) == "TERMINALDOWNLOAD") GOTO see_second;
IF(UPCASE($one) == "TERM") GOTO see_second;

next:
IF(UPCASE($one) != "TERMINAL") GOTO error_message;
IF(UPCASE($two) == "DOWNLOAD") GOTO other_two;
GOTO error_message;

see_second:
send "INPUT == " $one "\n";
IF($two == "") GOTO other_two;
IF(UPCASE($two) != "DOWNLOAD") GOTO error_message;

other_two:
SEND ">";
EXPECT %host_name %port_number;
SEND $host_name "*" $port_number "*" "\n";

```



```

IF($host_name == "") GOTO other_two;
// SEND "Telneting to " $host_name " " $port_number "\n";
TELNET $host_name $port_number;
GOTO exit;

send_Menu:
// SEND "Telneting to " $host_name "\n";
TELNET $host_name $two;
GOTO exit;

error_message:
IF($one == "") GOTO start;
SEND 'Incorrect syntax please type "Terminal Download"\n';
GOTO start;

exit:
//SEND "Telneting to " $host_name " " $port_number "\n";
TELNET $host_name $port_number;
SEND "DONE\nDONE\n";
HANGUP;

```

RADIUS Security Server User Table Entries

RADIUS user table entries are stored in the RADIUS security server database. A user table entry must contain the required parameters user's name but you may enter optional parameters such as protocol, address, and session.

This section briefly describes how to format the entries commonly used with HiPer ARC in the RADIUS database. For more detailed instructions on setting up a user table entry in the version of the RADIUS security server that you decide to use, refer to your RADIUS documentation. RADIUS user table entries consist of:

- Required parameters
- Optional parameters
- HiPer ARC-specific parameters



Most RADIUS user table parameters have a corresponding parameter in HiPer ARC's local user table. Most RADIUS parameters described in this chapter include corresponding CLI commands to set the value locally. Be aware that any parameter set via RADIUS exists only for the duration of the session.

Required Parameters

At a minimum, a RADIUS User Table entry *must* contain the following data:

- User-Name - name of the user

1 User-Name

The name the user must enter when logging onto the network via HiPer ARC.

Values:	ASCII character string up to 247 characters
User Types:	All
Packet Types:	Access-Request, Accounting-Request-Start, Accounting-Request-Stop
Default:	None

Use the CLI command below to set this parameter locally (password optional).

```
add user <name> password <password>
```

Optional Parameters

The following sections describe optional user parameters that you can define in the RADIUS authentication server database. Most parameter descriptions include the corresponding command you can use to define the same information in the local HiPer ARC User Table.



For detailed information about local user parameters and commands, refer to the appropriate chapter in this manual for the type of user you are configuring. Also see Chapter 11: Command Reference.

2 User-Password

The password the user may enter when logging onto the network via HiPer ARC. If your RADIUS server supports UNIX, the password can also be a quoted value of UNIX. This forces the RADIUS server to use the etc/passwd on the RADIUS host or query the NIS name server for password authentication if the network has NIS.

On transmission, the password is hidden. The password is first padded at the end with nulls to a multiple of 16 octets. A one-way MD5 hash is calculated over a stream of octets consisting of the shared secret followed by the Request Authenticator. This value is XORed with the first 16-octet segment of the password and placed in the first 16 octets of the string field of the this attribute. If the password is longer than 16 characters, a second one-way MD5 hash is calculated over a stream of octets consisting of the shared secret followed by the result of the first xor. That hash is XORed with the second 16-octet segment of the password and placed in the second 16 octets of the string field of this attribute.

If necessary, this operation is repeated, with each xor result being used along with the shared secret to generate the next hash to xor the next segment of the password, to no more than 128 characters.

Values:	ASCII character string up to 128 characters
User Types:	All except PPP CHAP
Packet Types:	Access-Request
Default:	None

The CLI uses 128-character challenge responses which are entered by the user and placed in this User-Password field. Use the following CLI command to set this parameter locally.

```
add user <name> password <string>
```

3 CHAP-Password

The Chap password is the response received from a PPP client responding to a CHAP challenge. The first octet is the Chap ID while the final 16 octets are the MD5 challenge response.

Values:	ASCII string of 17 characters
User Types:	PPP CHAP users: Framed, Callback and Dialout
Packet Types:	Access-Request
Default:	None

4 NAS-IP-Address

Specifies the HiPer ARC IP address. If more than one LAN interface is configured on the system, one will be declared the default and used for this purpose.

Values: IP address
 User Types: All
 Packet Types: Access-Request, Accounting-Request-Start, Accounting-Request-Stop
 Default: None

Use the following CLI command to set this parameter locally:

```
set ip network <name> address <IP_address>
```

5 NAS-Port

Specifies the physical slot and port the user logs in on HiPer ARC. This attribute is used to correlate dynamic filter change requests with users.

Values: 32-bit integer. For example: 0x00000907 (slot 9, port 7)
 User Types: All connecting to a WAN port
 Packet Types: Access-Request, Accounting-Request-Start, Accounting-Request-Stop, Change-Filter-Req
 Default: None

6 Service-Type

Indicates the type of link the user has requested, or a change in the type of link to be configured.

The RADIUS Service-Type parameter corresponds to the CLI *user type* parameter. The following table shows RADIUS service types and the corresponding user types you can define using the CLI:

RADIUS Service-Type	HiPer ARC Command
Login-User	set user <name> type login
Dialback-Login-User	set user <name> type callback,login
Framed-User (default)	set user <name> type network
Dialback-Framed-User	set user <name> type callback,network
Outbound-User	set user <name> type dial_out
Administrative-User	set user <name> type manage



*You can also specify the user type when you first add the user locally using the **add user** command*

Values: ASCII string: Login, Framed, Callback, DialOut, Manage. Although a local bitmap with the values above is kept, these standard RADIUS values are supported: Login, Framed, Callback Login, Callback Framed, Outbound and Administrative.



NAS_prompt, Authenticate_Only and Callback-NAS-Prompt values are not currently supported.

User Types: All
 Packet Types: Access-Response
 Default: Framed

Login-User The CLI also terms this a Login user. Once the user name and password are authenticated, this user is connected via a login service to the host or network specified in RADIUS or in the local user table.

At a minimum, a Login-User entry must contain:

- User-Name
- User-Password
- Service-Type

For example:

```
annab User-Password="dkt902d"
      Service-Type=Login-User
```

Dialback-Login-User The CLI defines this user type as two separate user types: *Login* and *Callback*. When a user ID and password are authenticated by RADIUS, HiPer ARC disconnects and dials users back, using a pre-defined telephone number. Once this connection is made, users are connected via a login service to the host or network specified in their profile. A Dialback-Login-User entry must contain:

- User-Name
- User-Password
- Service-Type
- Dialback-No

For example:

```
cindyg User-Password="billthecat",
        Service-Type=Dialback-Login-User,
        Dialback-No="19195551234"
```

Framed-User The CLI terms this a *Network* user. Once the user ID and password are authenticated, users are connected to the network using the network service (PPP or SLIP) specified in RADIUS or in the local user table.

A Framed-User entry must contain:

- User-Name
- User-Password
- Service-Type
- Framed-Protocol (not necessary if the user wants the default user setting)

For example:

```
daver User-Password="antietem",
       Service-type=Framed-User,
       Framed-Protocol=PPP
```

Dialback-Framed-User The CLI defines this as two separate user types: *Network* and *Callback*. When a user ID and password are authenticated by RADIUS, HiPer ARC disconnects and dials the user back, using a pre-defined telephone number. Once this connection is made, users are linked via a framed protocol service to the host or network specified in RADIUS or the local user table.

A Dialback-Framed-User entry must contain:

- User-Name
- User-Password
- Service-Type
- Framed-Protocol (not necessary if the user wants the default user setting)
- Dialback-No

For example:

```
harryk Password="flipper",
        Service-type=Framed-User,
        Framed-Protocol=PPP
        Dialback-No="15088470203"
```

Outbound-User HiPer ARC defines this user type as a *Dial-Out* user. An outbound user is a LAN user utilizing the shared modems to dial out.

A Outbound-User entry must contain:

- User-Name
- User-Password
- Service-Type

For example:

```
joek Password="vienna",
      Service-type=Outbound-User
```

Administrative-User HiPer ARC defines this user type as a *Manage* user. The administrative user has management access capabilities on HiPer ARC.

At a minimum, a Administrative-User entry must contain:

- User-Name
- User-Password
- Service-Type

For example:

```
frankr User-Password="rizzo55"
        Service-Type=Administrative-User
```

7 Framed-Protocol

Identifies which protocol the user is using to make the connection, indicating the type of framing for framed access.

Values:	ASCII string: PPP (default), SLIP (ARAP and RFC1490 not supported in this release).
User Types:	Network/Framed users - Framed, Callback and Dialout
Packet Types:	Access-Request, Accounting-Request-Start, Accounting-Request-Stop, Access-Response
Default:	PPP

Use the following CLI command to set this parameter locally:

```
set network user <name> network_service [PPP | SLIP]
```

8 Framed-IP-Address

Specifies the IP address (destination) that is assigned to the user for the duration of the connection. If HiPer ARC is configured to use assigned addresses, this field is not applicable. HiPer ARC assigns the user a temporary IP address from the Assigned Address pool for the duration of the connection.

Values:	IP address
User Types:	Framed, Callback, Dialout
Packet Types:	Accounting-Request-Start, Accounting-Request-Stop, Access-Response
Default:	0.0.0.0

The address 255.255.255.255 causes the address to be negotiated, while the addresses 0.0.0.0 (from RADIUS) or 255.255.255.254 will cause the server to locally choose an IP address from the IP address pool.

Use the following CLI command to set whether a user's client IP address is *negotiated*, *assigned* from the configured IP pool, or *specified* by administrator:

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



If you set the user's address selection to specified, you must also enter the remote IP address.

9 Framed-IP-Netmask

Specifies the user's (destination) remote IP address netmask. When the destination is a host, the value *must* be 255.255.255.255. This attribute indicates the IP netmask to be configured for the user when the user is a router to a network.

Values:	IP address
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response
Default:	255.255.255.255

Use the following CLI command to set the user's netmask locally:

```
set network user <name> remote_ip_address <ip_add>/<mask>
```



If you do not enter a mask value following the IP address, HiPer ARC automatically sets the netmask to 255.255.255.255.

10 Framed-Routing

Determines whether HiPer ARC lets Routing Information Protocol (RIP) packets be sent to or from the remote user, indicating the user's routing method when the user is a router to a network. Values: are pertinent to IP RIPv1 only. RIP policy defaults are initially set dependent upon this attribute's values.



This value applies only to IP RIP v1 in RADIUS. HiPer ARC supports both IP RIP v1 and IP RIP v2.

Values: *Listen* - HiPer ARC accepts RIP packets across the serial interface
 Broadcast - HiPer ARC broadcasts RIP packets across the serial interface
 Broadcast-Listen - HiPer ARC broadcasts and accepts RIP packets across the serial interface
 None - HiPer ARC discards RIP packets received from remote site or sent by local host

User Types: Framed, Callback and Dialout
 Packet Types: Access-Response
 Default: None

Use the following CLI command to set this parameter locally:

```
set network user <name> ip_routing [both | listen | none | send]
```

11 Filter-Id

Identifies the packet filter that controls the user's access to the host by specifying a filter file stored in the HiPer ARC FLASH file system. Locally, the CLI places the input filter in this attribute and the output filter in the vendor-specific *filter_id_output* attribute. For backwards compatibility, if a filter name is specified *filter*, HiPer ARC places *filter.in* in this attribute and *filter.out* in the *filter_id_output* attribute.

Values: ASCII character string up to 253 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Request
 Default: Null

The RADIUS syntax for specifying incoming and/or outgoing packets is:

```
Filter_ID= input filter filename / output filter filename
```

For example, if you want to specify a filter that is applied to incoming packets only (input filter), place a comma after the input file name:

```
Filter_ID=pktfilter.fil,
```

To specify a filter that is applied outbound packets only (output filter), place a comma (,) before the output filter filename. For example:

```
Filter_ID=,my_filter.fil
```

To specify an input *and* output filter in the same entry, enter both filter filenames separated by a comma. For example:

```
Filter_ID=pktfilter.fil,my_filter.fil
```

Use the following CLI commands to set this parameter locally. If the filter is a *user*, type:

```
add filter <name>
verify filter <name>
set user <name> input_filter <filter_name> output_filter <filter_name>
set interface <slot:x/mod:y> filter_access on
```

If the filter is an *interface* filter, issue the commands below:

```
add filter <name>
verify filter <name>
set interface <slot:x/mod:y> input_filter <filter_name> output_filter <filter_name>
```

For more detailed information, see *Chapter 9: Packet Filters*.

12 Framed-MTU

The Maximum Transmission Unit (MTU) specifies the largest packet that will be sent from HiPer ARC to a *network* user. IP packets larger than this value are fragmented prior to transmission.

Values:	32-bit integer
User Types:	Framed, Callback, Dialout
Packet Types:	Access-Response
Default:	1514

Use the following CLI command to set this parameter locally:

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

13 Framed-Compression

Specifies whether to use default TCP/IP compression (Van Jacobsen) for the link. HiPer ARC is responsible for applying the proper compression protocol to the appropriate link traffic.

Values:	ASCII string: None, VJ TCP/IP header compression
User Types:	Framed, Callback, Dialout
Packet Types:	Access-Response
Default:	VJ TCP/IP header compression

Use the following CLI command to set this parameter locally:

```
set network user <name> header_compression [none | tcpip]
```

14 Login-IP-Host

This is the name or IP address of the host to which a login user will log on and connect.

Values:	IP address
---------	------------

User Types: Login, Callback
 Packet Types: Access-Request, Accounting-Request-Start,
 Accounting-Request-Stop
 Default: 0.0.0.0

The address 255.255.255.255 causes the user to be prompted and the address 0.0.0.0 causes the server to pick a connection host from the default host table.

Use the following CLI command to set whether a user's client IP address is negotiated, assigned, or specified by the user:

```
set login user <name> host_type [prompt | select | specified]
```



If you set the user's host type to specified, you must also specify the host IP address.

15 Login-Service

Defines the type of connection the user makes with the host.

Values: ASCII string: TELNET, Rlogin, ClearTCP
 User Types: Login, Callback
 Packet Types: Access-Response
 Default: TELNET

Use the following CLI command to set this parameter locally:

```
set login user <name> login_service <cleartcp | rlogin | telnet>
```

16 Login-Port

Specifies that the user connect with a specific TCP port (such as 23, the default TELNET port). This attribute specifies the TCP port to which the user is automatically connected, when the *Login-Service* attribute is also present.

Values: 32-bit integer
 User Types: Login, Callback
 Packet Types: Access-Request, Accounting-Request-Start,
 Accounting-Request-Stop
 Default: 23



If this field isn't set, the value of the Login_Service attribute will set the default .

Use the following CLI command to set this parameter locally:

```
set login user <name> tcp_port <number>
```

17 Old-Password (NMC Only)

This attribute not supported in the current release.

18 Reply-Message

Indicates text which *may* be displayed to the user. When used in an *Access-Accept*, it is a success message. When used in an *Access-Reject*, it is a

failure message. It *may* indicate a dialog message to prompt the user before another Access-Request attempt. When used in an Access-Challenge, it *may* indicate a dialog message to prompt the user for a response.

Values: ASCII string of less than 254 characters
 User Types: Login, Framed, Callback
 Packet Types: Access-Response, Challenge-Response
 Default: Null

Use the following CLI command to set this parameter locally:

```
set user <name> message <"message text">
```

19 Callback-Number-One

Specifies the first phone number HiPer ARC uses to call back a user or dial out. If there are multiple login callback numbers in the RADIUS packet, the second number will be placed in the Login-Callback-Number-Two attribute.

Values: ASCII string of less than 254 characters
 User Types: Login, Framed, Callback
 Packet Types: Access-Response, Challenge-Response
 Default: Null

Use the following CLI command to set this parameter locally:

```
set user <user_name> phone_number [number] type [callback]
```

20 Callback-ID

This attribute not supported in the current release.

21 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.

22 Framed-Route

Specifies the static route, or a specific set of routers that the connection must take. HiPer ARC allows multiple framed routes in a RADIUS packet. The RADIUS format for this parameter is:

```
framed-route=<destination>/<bit count> <gateway> <metric>
```

- *Destination* - name or IP address of the host or network to which the user will connect
- *Bit Count* - optional bit count for netmask
- *Gateway* - router that provides the route to the host or network
- *Metric* - number of routers between the destination and the gateway; also known as hop count.

For example:

```
192.168.1.0/24 192.168.1.1 1
```



If the connection is configured to use the assigned addresses, or if the address is negotiated, and you set the destination to 0.0.0.0 (default host route), HiPer ARC will “learn” the gateway to reach the host or network. HiPer ARC allows multiple framed routes in a RADIUS packet.

Values: ASCII string of less than 254 characters
 User Types: Login, Framed, Dialback
 Packet Types: Access-Response
 Default: Null

Use the following CLI command to set this parameter locally:

```
add framed_route user <user>
    ip_route <ip_name or address>
    gateway <ip_name or address>
    metric <number>
```

23 Framed-IPX-Network

Indicates the IPX network number configured for the user.

Values 4-byte hexadecimal value
 User Types: Framed, Dialback
 Packet Types: Accounting-Stop, Account-Start, Access-Response
 Default 00000000

The default value of 0 or 0xFFFFFFFF causes the server to choose an address from the pool of available IPX addresses.

You can use the following CLI command to set this parameter locally:

```
set network user <name> ipx_address <ipx_addr>
```



You can enter '0' in the ipx_addr field to cause HiPer ARC to choose an IPX address from a pool of available addresses. The value '0xFFFFFFFF' is not valid.

24 State

This attribute may be sent in a Challenge-Response packet. The ensuing Access-Accept packet must contain this name attribute as it appeared in the Challenge-Response packet. Used primarily by the RADIUS server to keep track of Challenge states.

Values: ASCII string of less than 254 characters
 User Types: Login, Framed, Dialback
 Packet Types: Challenge-Response, Access-Request
 Default: None

25 Class

This attribute may be included in an Access-Response packet. It is forwarded exactly as it appears in the ensuing Accounting-Request_Start and Stop packets.

Values: ASCII string of less than 254 characters
 User Types: All

Packet Types: Access-Request, Accounting-Request-Start,
Accounting-Request-Stop

Default: None

26 Vendor-Specific

This is the vendor-specific space. Any attributes defined by 3Com and not defined by the standard are included here. See a description of HiPer ARC-specific attributes on page E-438.

Values: Dependent on vendor-specific variable

User Types: All

Packet Types: All

Default: None

27 Session-Timeout

Sets the maximum time (in seconds) of service provided to the user before the session is automatically terminated. Value can be sent by the server to the client in an *Access-Accept*. A value of 0 indicates no session timeout.

Values: 32-bit integer

User Types: All

Packet Types: Access-Response

Default: 0

Use the following CLI command to set this parameter locally:

```
set user <name> session_timeout <seconds>
```

28 Idle-Timeout

Sets the maximum time (in seconds) that a connection can be idle before the user session is automatically terminated. Value can be sent by the server to the client in an *Access-Accept*.

Values: 32-bit integer

User Types: All

Packet Types: Access-Response

Default: 0 (not activated)

Use the following CLI command to set this parameter locally:

```
set user <name> idle_timeout <1-86400 seconds>
```

29 Termination-Action

This attribute not supported in the current release.

30 Called-Station-ID

Specifies the phone number that was dialed to connect with HiPer ARC.

Values: ASCII string of less than 254 characters.

User Types: Framed, Login, Callback

Packet Types: Access-Request, Accounting-Request-Start,
Accounting-Request-Stop

Default: None

31 Calling-Station-ID

Specifies the phone number that was dialed from to connect with HiPer ARC.

Values: ASCII string of less than 254 characters.

User Types: Framed, Login, Callback

Packet Types: Access-Request, Accounting-Request-Start,
Accounting-Request-Stop

Default: None

32 NAS-Identifier

This attribute is not supported in the current release.

33 Proxy-State

This attribute is not supported in the current release.

34 Login-LAT-Service

This attribute is not supported in the current release.

35 Login-LAT-Node

This attribute is not supported in the current release.

36 Login-LAT-Group

This attribute is not supported in the current release.

37 Framed-AppleTalk-Link

This attribute is not supported in the current release.

38 Framed-AppleTalk-Network

This attribute is not supported in the current release.

39 Framed-AppleTalk-Zone

This attribute is not supported in the current release.

40 Acc(oun)t-Status-Type

Indicates whether the Accounting-Request packet describes the beginning or the end of a user session. HiPer ARC does not support *Accounting-On* and *Accounting-Off*.

Values: ASCII string: Start, Stop

User Types: All

Packet Types: Accounting-Request-Start, Accounting-Request-Stop

Default: None

41 Acc(oun)t-Delay-Time

Indicates the interval between when the original packet was transmitted and when this particular packet was transmitted. It is primarily used for retransmissions.

Values: 32-bit integer
User Types: All
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: None

42 Acc(oun)t-Input-Octets

Indicates the number of inbound bytes received during this user session.

Values: 32-bit integer
User Types: All
Packet Types: Accounting-Request-Stop
Default: None

43 Acc(oun)t-Output-Octets

Specifies the number of outbound bytes transmitted during this user session.

Values: 32-bit integer
User Types: All
Packet Types: Accounting-Request-Stop
Default: None

44 Acc(oun)t-Session-ID

Specifies a unique ID to facilitate matching start and stop records in a log file for this session. Start and stop records must have the same AccountAccount-Session-ID.

Values: ASCII string of less than 254 characters
User Types: All
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: None

45 Acc(oun)t-Authentic

Specifies whether the Accounting-Request packet describes how the user is authenticated - by RADIUS or HiPer ARC. The *Remote* option is not currently supported.

Values: ASCII string: RADIUS, Local
User Types: All
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: None

46 Acc(oun)t-Session-Time

Specifies the period in seconds the user was connected. The counter begins when the user is authenticated or connected.

Values: 32-bit integer
User Types: All
Packet Types: Accounting-Request-Stop
Default: None

47 Acc(oun)t-Input-Packets

Specifies the number of inbound packets received during this user session.

Values: 32-bit integer
User Types: Framed, Callback
Packet Types: Accounting-Request-Stop
Default: None

48 Acc(oun)t-Output-Packets

Specifies the number of outbound packets transmitted during this user session.

Values: 32-bit integer
User Types: Framed, Callback
Packet Types: Accounting-Request-Stop
Default: None

49 Acc(oun)t-Terminate-Cause

Specifies the reason for terminating this user session. See RFC 2139 for more information.

Values: ASCII string: User Request, Lost Carrier, Lost Service, Idle Time-out, Session Time-out, Admin reset, Admin reboot, Port Error, NAS Error, NAS Request, NAS Reboot, Port Unneeded, Port Preempted, Port Suspended, Service Unavailable, Callback, User Error, Host Request
User Types: Framed, Callback
Packet Types: Accounting-Request-Stop
Default: None

50 Acc(oun)t-Multi-Session-ID

Specifies a unique Accounting ID to make it easy to link multiple related sessions in a log file. Each linked session has a unique Acc(oun)t-Session-Id but the same Acc(oun)t-Multi-Session-Id. It is strongly recommended that the Acc(oun)t-Multi-Session-Id be a printable ASCII string. The attribute will match the Session ID (44) across Multilink calls.

Values: ASCII string of less than 254 characters
User Types: All user types
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: None

51 Acc(oun)t-Link-Count

Provides the number of links known to have been in a given multilink session at the time the accounting record is generated. HiPer ARC may include the Acc(oun)t-Link-Count attribute in any Accounting-Request which might have multiple links. For example:

Multi-Session-Id	Session-Id	Status-Type	Link-Count
10	10	Start	1
10	11	Start	2
10	11	Stop	2
10	12	Start	3
10	13	Start	4
10	12	Stop	4
10	13	Stop	4
10	10	Stop	4

Values: 32-bit integer

User Types: All user types

Packet Types: Accounting-Request-Stop, Accounting-Request-Start

Default: None

60 CHAP-Challenge

This attribute not supported in the current release.

61 NAS-Port-Type

Indicates the type of physical port on the NAS authenticating the user. It can be used instead of or in addition to the NAS-Port (5) attribute. Either NAS-Port (5) or NAS-Port-Type or both *should* be present in an Access-Request packet, if the NAS differentiates among its ports. X.75 is also signaled as ISDN sync.

Values: ASCII string: Async, ISDN Sync, ISDN Async V.120, ISDN Async V.110, Virtual

User Types: All user types

Packet Types: Access-Request

Default: None

62 Port-Limit

Indicates the maximum number of dialin ports a user can concurrently employ.

63 Login-LAT-Port

This attribute is not supported in the current release.

64 Tunnel-Type

Indicates the tunneling protocol to be used. It may be included in Access-Request, Access-Accept and Accounting-Request packets. If the Tunnel-Type Attribute is present in an Access-Request packet, it should be taken as a hint to the RADIUS server as to the tunnelling protocols supported by the tunnel initiator; the RADIUS server may ignore the hint, however. A tunnel initiator is not required to implement any of these tunnel types; if a tunnel initiator receives an Access-Accept packet which contains only unknown or

unsupported Tunnel-Types, the tunnel initiator MUST behave as though an Access-Reject had been received instead.

Values: Integer: Point-to-Point Tunneling Protocol (PPTP) [1], Layer Two Tunneling Protocol (L2TP) [3]
 User Types: Tunnel
 Packet Types: Access-Request, Access-Accept, Accounting-Request
 Default: PPTP

Use the following CLI command to set this parameter locally:

```
set tunnel user <name> type <none | pptp | l2tp>
```

65 Tunnel-Medium-Type

Indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. It may be included in both Access-Request and Access-Accept packets; if it is present in an Access-Request packet, it SHOULD be taken as a hint to the RADIUS server as to the tunnel mediums supported by the tunnel initiator. The RADIUS server may ignore the hint, however.

Values: Integer: IP (IP version 4) [1]
 User Types: Tunnel
 Packet Types: Access-Request, Access-Accept, Accounting-Request-Stop, Accounting-Request-Start
 Default: IP

Use the following CLI command to set this parameter locally:

```
set tunnel user <name> medium_type ipv4
```

66 Tunnel-Client-Endpoint

Contains the address of the initiator end of the tunnel. It may be included in both Access-Request and Access-Accept packets to indicate the address from which a new tunnel is to be initiated. If the Tunnel-Client-Endpoint Attribute is included in an Access-Request packet, the RADIUS server should take the value as a hint; the server is not obligated to honor the hint, however. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop, in which case it indicates the address from which the tunnel was initiated. This attribute, along with the Tunnel-Server-Endpoint and Acct-Tunnel-Connection-ID attributes, may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.

Values: Less than 64-character ASCII string: Either the fully qualified domain name of the tunnel client, or a "dotted-decimal IP address".
 User Types: Tunnel
 Packet Types: Access-Request, Access-Accept, Accounting-Request-Stop, Accounting-Request-Start
 Default: None

Use the following CLI command to set this parameter locally:

```
set tunnel user <name> client_endpoint <ip_address>
```

67 Tunnel-Server-Endpoint

Indicates the address of the server end of the tunnel. This attribute may be included (as a hint to the RADIUS server) in the Access-Request packet and must be included in the Access-Accept packet if the initiation of a tunnel is desired. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session. This attribute, along with the Tunnel-Client-Endpoint and Acct-Tunnel-Connection-ID Attributes, may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.

Values:	Less than 64-character ASCII string: Either the fully qualified domain name of the tunnel client, or a "dotted-decimal IP address".
User Types:	Tunnel
Packet Types:	Access-Request, Access-Accept, Accounting-Request-Stop, Accounting-Request-Start
Default:	None

Use the following CLI command to set this parameter locally:

```
set tunnel user <name> server_endpoint <ip_address>
```

68 Acc(ount)-Tunnel_Connection-Id

This attribute, along with the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint, may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.

69 Tunnel-Password

Contains a key or password for tunneled users.

Values:	String: Less than 256 ASCII characters
User Types:	Tunnel
Packet Types:	Access-Accept
Default:	None

Use the following CLI command to set this parameter locally:

```
set tunnel user <name> password <string>
```

76 Prompt

Indicates whether or not the challenge response by the user should be echoed.

Values:	If attribute sent via RADIUS, CLI does not echo the response.
User Types:	All
Packet Types:	Challenge-Response
Default:	None

81 Tunnel-Private-Group_ID

Attribute not supported at this time.

250 Char-NoEcho

Attribute previously supported in the 3.x (NETServer) code

Indicates whether or not the challenge response by the user should be echoed.

Values:	If attribute sent via RADIUS, CLI does not echo the response.
User Types:	All
Packet Types:	Challenge-Response
Default:	None

HiPer ARC-Specific Parameters

This section describes HiPer ARC-specific authentication parameters you can enter for a user in the RADIUS database. These parameters directly correspond to parameters supported by HiPer ARC software. Indicators are expressed beside the name of the attribute.



Since RADIUS is an open standard, many RADIUS server implementations are available. The values described below may not be available depending on your RADIUS server implementation.

Format

The format below describes all of the following vendor-specific attributes. Only bit length and indicator values change for each attribute. Indicators are expressed beside the name of the attribute.

Type:	26 (Vendor Specific)
Length:	Variable but always greater than 10 bytes
Org. ID:	429 (3Com)
Indicator:	3Com-specific, sub-attribute hexadecimal ID displayed in attribute header (1-62)
Data:	Like any standard RADIUS attribute, the data can be string, IP address, integer or date type. Each of these data types have the same meaning as standard RADIUS data types.

0x006C Mod(ulation)-Type

Contains the modulation type for this user session. Attribute previously supported in the 3.x (NETServer) code.

Values:	ASCII string: 0 - Unknown, 1 - HST, 2 - V32, 3 - V22BIS, 4 - BELL103, 5 - V21, 6 - V22_BELL212, 7 - V32 BIS, 8 - V23, 9 - BELL208, 10 - V21_CLASS_1_FAX, 11 - V27_CLASS_1_FAX, 12 - V29_CLASS_1_FAX, 13 - V17_CLASS_1_FAX, 14 - V21_CLASS_2_FAX, 15 - V27_CLASS_2_FAX, 16 - V21_CLASS_2_FAX, 17 - V17_CLASS_2_FAX, 18 - V32TER, 19 - V34, 20 - VFC, 21 - V34_PLUS, 22 - X2_SERVER, 23 - ISDN_V110, 24 - ISDN_V120, 25 - ISDN_X75, 26 - ISDN_ASYNC_SYNC, 27 - ISDN_CLEAR_CHANNEL, 28 - X2_CLIENT,
---------	--

29 - X2_SYMMETRIC, 30 - PIAFS, 31 - X2-V2, 32 - Analog V.PCM, 33 - Digital V.PCM, 34 - All Digital

User Types: All
 Packet Types: Accounting-Request-Start, Accounting-Request-Stop
 Default: None

0x007C Compression-Type

Specifies the compression type for this user session. Attribute previously supported in the 3.x (NETServer) code.

Values: Unknown, None, V42BIS, MNP5
 User Types: All
 Packet Types: Accounting-Request-Start, Accounting-Request-Stop
 Default: None

0x0099 Error-Control

Contains the error control for this user session. Attribute previously supported in the 3.x (NETServer) code

Values: ASCII string: 0 - UNKNOWN, 1 - NON_ARQ, 2 - MNP3, 3 - MNP4, 4 - V42, 5 - HST, 6 - SYNCHRONOUS, 7 - MNP2, 8 - MNP10 (Cellular), 9 - V42ETC, 10 - MNP10EC, 11 - LAPMEC, 12 - V42ETC2, 13 - V42SREJ, 14 - PIAFS, 15 - V120, 16 - X75
 User Types: All Packet Types: Accounting-Request-Start, Accounting-Request-Stop
 Default: None

0x9000 IP-Input-Filter

The various filter attributes (0x9000 - 0x9005) are all string types. They provide a means to specify filters on the RADIUS server in the standard HiPer ARC format on a per-user basis. Attribute previously supported in the 3.x (NETServer) code.

Values: ASCII string of less than 254 characters
 User Types: Login, Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: None

Filter Rule (e.g.): " 1 ACCEPT src-adr>146.115.121.213/255.255.255.252"
 " 2 REJECT dst-addr=146.115.122.75/255.255.255.252"
 " 3 ACCEPT tcp-one-way=4554"
 " 4 ACCEPT udp-src-port=4556"
 " 5 ACCEPT udp-src-port=4557"
 " 6 ACCEPT icmp-type=246"
 " 7 REJECT protocol=udp"
 " 8 ACCEPT tcp-src-port=4561"
 " 9 ACCEPT tcp-dst-port=4562"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9001 IPX-Input-Filter

Filter string supported by HiPer ARC and previously supported in the 3.x (NETServer) code.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: None
 Filter Rule (e.g.): " 1 ACCEPT src-net=00-01-10-00"
 " 2 REJECT dst-net=00-01-11-10"
 " 3 ACCEPT src-host=01-11-00-00-10-01"
 " 4 ACCEPT dst-host=01-00-00-10-00"
 " 5 REJECT src-socket=010101"
 " 6 ACCEPT dst-socket=010111"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9002 IPX-SAP-Input-Filter

Filter string supported by HiPer ARC and previously supported in the 3.x (NETServer) code.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: None
 Filter Rule (e.g.): " 1 ACCEPT network=01-11-00-00-10-01"
 " 2 REJECT node=01-11-00-00-10-11"
 " 3 ACCEPT server=boston"
 " 4 ACCEPT service-type=0x011"
 " 5 REJECT socket=1x001"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9003 IP-Output-Filter

Filter string supported by HiPer ARC and previously supported in the 3.x (NETServer) code.

Values: ASCII string of less than 254 characters
 User Types: Login, Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: None

Filter Rule (e.g.): " 1 ACCEPT src-adr=146.115.121.213/255.255.255.252"
 " 2 REJECT dst-addr=146.115.122.75/255.255.255.252"
 " 3 ACCEPT tcp-one-way=5345"
 " 4 ACCEPT udp-src-port=5346"
 " 5 REJECT udp-dst-port=5347"
 " 6 ACCEPT icmp-type=220"
 " 7 REJECT protocol!=tcp"
 " 8 ACCEPT tcp-src-port=5350"
 " 9 REJECT tcp-dst-port=5351"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9004 IPX-Output-Filter

Filter string supported by HiPer ARC and previously supported in the 3.x (NETServer) code.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: None
 Filter Rule (e.g.): " 1 ACCEPT src-net=00-01-10-00"
 " 2 REJECT dst-net=00-01-11-10"
 " 3 ACCEPT src-host=01-11-00-00-10-01"
 " 4 ACCEPT dst-host=01-00-00-10-00"
 " 5 REJECT src-socket=0x011;"
 " 6 ACCEPT dst-socket=1x001"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9005 IPX-SAP-Output-Filter

Filter string supported by HiPer ARC and previously supported in the 3.x (NETServer) code.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: None
 Filter Rule (e.g.): " 1 ACCEPT network=01-11-00-00-10-01"
 " 2 REJECT node=01-11-00-00-10-11"
 " 3 ACCEPT server =boston;"
 " 4 REJECT service-type=0x011;"
 " 5 REJECT socket=1x001"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9006 VPN-ID

This attribute is not supported in the current release.

0x9007 VPN-Name

This attribute is not supported in the current release.

0x9008 VPN-Neighbor

This attribute is not supported in the current release.

0x9009 Framed Routing-V2

This attribute is not supported in the current release.

0x900A VPN-Gateway

This attribute is not supported in the current release.

0x900B Tunnel-Authenticator

This attribute is not supported in the current release.

0x900C Packet-Index

This attribute is not supported in the current release.

0x900D Cutoff

This attribute is obsolete.

0x900E Access-Accept-Packet

This attribute is obsolete.

0x900F Primary-DNS

Server attributes 0x900F - 0x9012 are all IP address types. They provide the means to assign DNS and NBNS server IP address information to PPP clients. Attribute previously supported in the 3.x (NETServer) code.

Values:	32-bit integer: IP address
User Types:	All
Packet Types:	Access-Response
Default:	None
Length:	14

0x9010 Secondary DNS

IP address of the secondary DNS server. Attribute previously supported in the 3.x (NETServer) code.

Values:	32-bit integer: IP address
User Types:	All
Packet Types:	Access-Response
Default:	None

0x9011 Primary-NBNS

IP address of the primary NBNS server. Attribute previously supported in the 3.x (NETServer) code.

Values: 32-bit integer: IP address
User Types: All
Packet Types: Access-Response
Default: None

Use the following global command to set this parameter locally:

```
set ppp nbns_primary <ip address>
```

0x9012 Secondary NBNS

IP address of the secondary NBNS server. Attribute previously supported in the 3.x (NETServer) code.

Values: 32-bit integer: IP address
User Types: All
Packet Types: Access-Response
Default: None

Use the following global command to set this parameter locally:

```
set ppp nbns_secondary <ip address>
```

0x9013 Syslog-Tap

This attribute is not supported in the current release but was previously supported in the 3.x (NETServer) code.

0x9014 MIC

Identifies the message integrity code for an enhanced standard RADIUS packet. Attribute previously supported in the 3.x (NETServer) code.

Values: ASCII string
User Types: All
Packet Types: Change-Filter-Request, Change-Filter-Ack, Change-Filter-Nack
Default: None

0x9015 Log-Filter-Packet

This attribute is not supported in the current release but was previously supported in the 3.x (NETServer) code.

The following undefined attribute is not supported in this release:

0x9017 Call-Tracking-ID**0x9019 Chassis-Call-Slot**

Contains the slot within the chassis where the T1 or PRI card resides. Attribute previously supported in the 3.x (NETServer) code.

Chassis-Call-Slot is the slot within the chassis where T1 or PRI cards resides.

Values: 32-bit integer: 1-16
User Types: All
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: None

0x901A Chassis-Call-Span

Contains the T1 or ISDN-PRI (physical) span line the call comes in on. This value is passed to HiPer ARC directly from the PRI card. Attribute previously supported in the 3.x (NETServer) code.

Values: Integer: 0 or 1
User Types: All
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: Base 1

Use the following global command to set this parameter locally:

```
set pbus reported_base 1
```

0x901B Chassis-Call-Channel

Contains the DSO or B_CHAN (physical) the call came in on. This value is passed to HiPer ARC directly from the PRI card. Attribute previously supported in the 3.x (NETServer) code.

Values: Integer: 0-31
User Types: All
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: None

0x901C Keypress-Timeout

Specifies the number of seconds before HiPer ARC should assume a carriage return while waiting for a Challenge-Response from the user. Attribute previously supported in the 3.x (NETServer) code.

Values: 32-bit integer
User Types: All
Packet Types: Challenge-Response
Default: None

0x901D Unauthenticated-Time

Tracks the interval between the user being connected and authenticated. Attribute previously supported in the 3.x (NETServer) code.

Values: 32-bit integer
User Types: All
Packet Types: Accounting-Request-Start, Accounting-Request-Stop
Default: None

0x901E VPN-Encrypter

This attribute is not supported in the current release.

0x901F Acct-VPN-Gateway

This attribute is not supported in the current release.

0x9020 Re-CHAP-Timeout

This attribute is not supported in the current release.

0x9021 CCP-Algorithm

This attribute is not supported in the current release.

0x9022 ACCM-Type

This attribute is not supported in the current release.

0x9023 Connect-Speed

Specifies the initial speed of the modem connection.

Values:	32-bit integer
User Types:	Login, Framed
Packet Types:	Accounting-Request-Stop, Accounting-Request-Start
Default:	None

0x9024 IP-Address-Pool

Sets the name of the IP address pool for Framed PPP/SLIP users.

Values:	ASCII string. Limit: 16 bytes
User Types:	Framed
Packet Types:	Access-Accept
Default:	None

Use the following global command to set this parameter locally:

```
add ip pool <pool_name>
```

0x9026 Local-Framed-IP-Address

This attribute not supported in the current release.

0x9800 Bearer Capabilities

This attribute is obsolete.

0x9801 Speed-of-Connection

This attribute not supported in the current release.

0x9802 Max-Channels

Specifies the maximum number of channels that can be used for a LAN-to-LAN connection. Specifying one channel disables multilink PPP. HDM cards support up to 16 channels, QUAD cards support 2.

Values:	Integer: 1 or 2
---------	-----------------

User Types: Framed, Callback and Dialout
Packet Types: Access-Response
Default: 2

Use the following CLI command to set this parameter locally:

```
set network user <name> ppp max_channels <number>
```

0x9803 Channel-Expansion

Indicates the channel expansion percentage for a LAN-to-LAN connection. When usage of the first channel exceeds this percentage, PPP adds a second channel.

Values: Integer: Percentage ranging from 0-100
User Types: Framed, Callback and Dialout
Packet Types: Access-Response
Default: 0

Use the following CLI command to set this parameter locally:

```
set network user <name> ppp channel_expansion <percent>
```

0x9804 Channel-Decrement

Indicates the channel decrement percentage for a LAN-to-LAN connection. When usage of the second channel drops below this percentage, PPP will drop the second channel and use the first channel only.

Values: Integer: Percentage ranging from 0-100
User Types: Framed, Callback and Dialout
Packet Types: Access-Response
Default: 0
Length 14 bytes

Use the following CLI command to set this parameter locally:

```
set network user <name> ppp channel_decrement <percent>
```

0x9805 Expansion-Algorithm

Specifies which type of expansion algorithm should be used to handle bandwidth allocation. Each algorithm measures traffic bandwidth over 60 second intervals. The *constant* value takes a conservative approach to bandwidth allocation and does not react to short-term bandwidth changes. The *linear* value measures more current, higher weight traffic when allocating bandwidth.

Values: Integer: Constant (1), Linear (2)
User Types: Framed, Callback and Dialout
Packet Types: Access-Response
Default: Constant

Use the following CLI command to set this parameter locally:

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

0x9806 Compression-Algorithm

Specifies which proprietary compression algorithm PPP should use.

Values:	Integer: None (0), Stac (1), Ascend (2), Microsoft (3), Auto (4)
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response
Default:	Auto

Use the following CLI command to set this parameter locally:

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

0x9807 Receive-Acc-Map

Determines whether HiPer ARC uses the asynchronous control character map to filter incoming data.

Values:	Hexadecimal value
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response
Default:	0xffffffff
Length	14 bytes

Use the following CLI command to set this parameter locally:

```
set network user <name> ppp receive_acc_map <hex_number>
```

0x9808 Transmit-Acc-Map

Determines whether HiPer ARC uses the asynchronous control character map to filter outgoing data.

Values:	Hexadecimal value
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response
Default:	0xffffffff
Length	14 bytes

Use the following CLI command to set this parameter locally:

```
set network user <name> ppp transmit_acc_map <hex_number>
```

0x980A Compression-Reset-Mode

Determines how often PPP should examine packets to decide when to re-negotiate the optimum compression algorithm.

Values:	Integer: Auto (0), Reset every packet (1), Reset on error (2)
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response
Default:	Auto

Length 14 bytes

Use the following CLI command to set this parameter locally:

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

0x980B Min-Compression-Size

Specifies the minimum size at which PPP compresses a packet. Smaller data packets are not compressed.

Values: 32-bit integer: Decimal value (Range: 128-1514 bytes)

User Types: Framed, Callback and Dialout

Packet Types: Access-Response

Default: 256 bytes

Length 14 bytes

Use the following CLI command to set this parameter locally:

```
set network user <name> ppp min_size_compression <number>
```

0x980C IP

Indicates whether IP is enabled for the user. Attribute previously supported in the 3.x (NETServer) code.

Values: Integer: Enabled (1), Disabled (2)

User Types: Framed, Callback and Dialout

Packet Types: Access-Response

Default: Enabled

Use the following CLI command to set this parameter locally:

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

0x980D IPX

Indicates whether IPX is enabled for the user. Attribute previously supported in the 3.x (NETServer) code.

Values: Integer: Enabled (1), Disabled (2)

User Types: Framed, Callback and Dialout

Packet Types: Access-Response

Default: Enabled

Use the following CLI command to set this parameter locally:

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

0x980E Filter-Zones

This attribute is not supported in the current release.

0x980F AppleTalk

This attribute is not supported in the current release.

0x9810 Bridging

This attribute is not supported in the current release.

0x9811 Spoofing

Indicates whether protocol spoofing is enabled for the user. Spoofing reduces WAN traffic between routers by intercepting queries from a server to a client and replying to that server.

Values:	Integer: Enabled (1), Disabled (2)
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response
Default:	Disabled

Use the following CLI command to set this parameter locally:

```
set network user <name> spoofing [enable | disable]
```

0x9812 Host-Type

This attribute is obsolete.

0x9813 Send-Name

This attribute is obsolete

0x9814 Send-Password

Indicates the password to be sent when logging into and being authenticated by a remote location. This is needed for a two-way, LAN-to-LAN routing connection.

Values:	ASCII string of less than 254 characters
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response
Default:	Null
Length	14 bytes

Use the following CLI command to set this parameter locally:

```
set network user <name> send_password <string>
```

0x9815 Start-Time

This attribute not supported in the current release.

0x9816 End-Time

This attribute not supported in the current release.

0x9817 Send-Script1

An AT command script to transmit remotely for dial-out purposes.

Values:	ASCII string of less than 254 characters
User Types:	Framed, Callback and Dialout
Packet Types:	Access-Response

Default: Null

Use the following CLI command to set this parameter locally:

```
set dial_out user <user_name> send1_script <"string">
```

0x9818 Reply-Script1

An AT command script to receive from a remote site for dial-out purposes.

Values: ASCII string of less than 254 characters

User Types: Framed, Callback and Dialout

Packet Types: Access-Response

Default: Null

Use the following CLI command to set this parameter locally:

```
set dial_out user <user_name> reply1_script <"string">
```

The following undefined attributes are supported with the same format as described earlier:

0x9819 Send-Script2

0x981A Reply-Script2

0x981B Send-Script3

0x981C Reply-Script3

0x981D Send-Script4

0x981E Reply-Script4

0x981F Send-Script5

0x9820 Reply-Script5

0x9821 Send-Script6

0x9822 Reply-Script6

0x9823 Terminal-Type

Indicates the terminal type defined for the user.

Values: ASCII string of less than 254 characters

User Types: Login and Callback

Packet Types: Access-Response

Default: vt100

Use the following CLI command to set this parameter locally:

```
set login user <user name> terminal_type [string]
```

The following undefined attribute is not supported in this release:

0x9824 AppleTalk-Network-Range

0x9825 Local-IP-Address

Used for dedicated circuits specifying the local IP address of the user.

Values: IP Address

User Types: Framed, Callback and Dialout

Packet Types: Access-Response
 Default: 0.0.0.0

Use the following CLI command to set this parameter locally:

```
set dial_out user <user_name> local_IP_address [ip_net_address]
```

0x9826 Routing-Protocol

Indicates which routing protocol to use.

Values: Integer: RIP1 (1), RIP2 (2)
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response
 Default: 1-RIP1

Use the following CLI command to set this parameter locally:

```
set ip network <name> [none | ripv1 | ripv2]
```

0x9827 Modem-Group

Indicates the modem group configured for the user.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response
 Default: all, slot:1, slot:2, slot:3, etc.

Use the following CLI command to set this parameter locally:

```
add modem_group <group_name> interfaces <interface_name>
```

0x9828 IPX-Routing

Indicates the routing procedure for IPX to take.

Values: Integer: None (0), Send (1), Listen (2), Respond (3), All (4)
 User Types: Framed, Callback, Dialout
 Packet Types: Access-Response
 Default: 0-None

Use the following CLI command to set this parameter locally:

```
set network user <name> ipx_routing [all | listen | none | respond | send]
```

0x9829 IPX-WAN

Indicates whether IPX WAN is enabled or disabled.

Values: Enabled or Disabled
 User Types: Framed, Callback, Dialout
 Packet Types: Access-Response
 Default: Disabled

Use the following CLI command to set this parameter locally:

```
set network user <name> ipx_wan [enable | disable]
```

0x982A IP-RIP-Policies

Indicates the RIP policy flags for a connection. This attribute need only be specified if the user wants to deviate from the defaults set by the *Framed-Routing* attribute.

Values: ASCII string of less than 254 characters: SendDefault (1), SendRoutes (2), SendSubnets (4), AcceptDefault (8), SplitHorizon (0x10), PoisonReverse (0x20), FlashUpdate (0x40), SimpleAuth (0x80), V1Send (0x100), V1Receive (0x200), V2 Receive (0x400), Silent (0x800)

User Types: Framed, Callback and Dialout

Packet Types: Access-Response

Default: Dependent upon value in Framed_Routing attribute

Use the following CLI command to set this parameter locally:

```
set ip network <name> rip_policies_update <rip_policies>
```

0x982B IP-RIP-Simple-Auth-Password

Contains the string value of the simple authentication password used when the simple authentication bit is set by IP RIP policy flags

Values: ASCII string of less than 254 characters

User Types: Framed, Callback and Dialout

Packet Types: Access-Response

Default: Null

Use the following CLI command to set this parameter locally:

```
set network user <name> rip_authentication_key
```

0x982C IP-RIP-Input-Filter

Filter string supported by HiPer ARC.

Values: ASCII string of less than 254 characters

User Types: Login, Framed, Callback and Dialout

Packet Types: Access-Response, Change-Filter-Req

Default: None

Filter Rule (e.g.): "1 ACCEPT network=146.115.121.213/255.255.255.252"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x982D IP-Call-Input-Filter

Filter string supported by HiPer ARC.

Values: ASCII string of less than 254 characters

User Types: Login, Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: None
 Filter Rule (e.g.): " 1 ACCEPT tcp-src-port=6609"
 " 2 REJECT tcp-dst-port=6610
 " 3 ACCEPT tcp-one-way=6611"
 " 4 ACCEPT udp-src-port=6612"
 " 5 REJECT udp-src-port=6613"
 " 6 ACCEPT icmp-type=211"
 " 7 REJECT network=udp"
 " 8 ACCEPT src-addr<=147.122.139.123/255.255.255.243"
 " 9 REJECT dest-addr>=147.122.138.123/255/255/255/244"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x982E IPX-Call-Input-Filter

Filter string supported by HiPer ARC.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Request
 Default: Null
 Filter Rule (e.g.): " 1 ACCEPT src-net=01-00-01-00"
 " 2 REJECT dst-net=01-00-01-01
 " 3 ACCEPT src-host=01-11-10-01-00-01"
 " 4 ACCEPT dst-host=01-11-10-01-00-00"
 " 5 REJECT src-socket=1x001"
 " 6 ACCEPT dst-socket=1x011"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9831 AT-Input-Filter

This attribute is not supported in the current release.

0x9832 AT-RTMP-Input-Filter

This attribute is not supported in the current release.

0x9833 AT-ZIP-Input-Filter

This attribute is not supported in the current release.

0x9834 AT-Call-Input-Filter

This attribute is not supported in the current release.

0x9835 ET-Bridge-Input-Filter

This attribute is not supported in the current release.

0x9838 IPX-RIP-Output-Filter

Filter string supported by HiPer ARC.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: Null
 Filter Rule (e.g.): " 1 ACCEPT network=01-11-00-01"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9839 IPX-Call-Output-Filter

Filter string supported by HiPer ARC.

Values: ASCII string of less than 254 characters
 User Types: Framed, Callback and Dialout
 Packet Types: Access-Response, Change-Filter-Req
 Default: Null
 Filter Rule (e.g.): " 1 ACCEPT src-net=01-00-01-00"
 " 2 REJECT dst-net=01-00-01-01"
 " 3 ACCEPT src-host=01-11-10-01-00-01"
 " 4 ACCEPT dst-host=01-11-10-01-00-00"
 " 5 REJECT src-socket=1x001"
 " 6 ACCEPT dst-socket=1x001"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x983A AT-Output-Filter

This attribute is not supported in the current release.

0x983B AT-RTMP-Output-Filter

This attribute is not supported in the current release.

0x983C AT-ZIP-Output-Filter

This attribute is not supported in the current release.

0x983D AT-Call-Output-Filter

This attribute is not supported in the current release.

0x983E ET-Bridge-Output-Filter

This attribute is not supported in the current release.

0x983F ET-Bridge-Call-Output-Filter

This attribute is not supported in the current release.

0x982F MP-MRRU (Multilink PPP Receive Unit)

Specifies the maximum reconstructed receive unit for Multilink PPP.

User Types: Framed, Callback and Dialout

Packet Types: Accounting-Request-Start, Accounting-Request-Stop

0x9836 IP-RIP-Output-Filter

Filter string supported by HiPer ARC.

Values: ASCII string of less than 254 characters

User Types: Login, Framed, Callback and Dialout

Packet Types: Access-Response, Change-Filter-Req

Filter Rule (e.g.): " 1 ACCEPT network=146.115.121.213/255.255.255.252"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9837 IP-Call-Output-Filter

Filter string supported by HiPer ARC.

Values: ASCII string of less than 254 characters

User Types: Login, Framed, Callback and Dialout

Packet Types: Access-Response, Change-Filter-Req

Filter Rule (e.g.): " 1 ACCEPT tcp-src-port=7700"

" 2 REJECT tcp-dst-port=7701"

" 3 ACCEPT tcp-one-way=7701"

" 4 ACCEPT udp-src-port=7703"

" 5 REJECT udp-src-port=7704"

" 6 ACCEPT icmp-type=204"

" 7 REJECT protocol=udp"



Note: The rule syntax for filters is the same as HiPer ARC filter syntax except that the first line need not contain #filter and doesn't require a section name such IP:. NETServer 3.x filter syntax is also supported in HiPer ARC.

0x9840 IP-Default-Route-Option

Indicates whether the destination IP address should become the default route.

Values: Integer: Enabled (1), Disabled (2)

User Types: Framed, Callback and Dialout

Packet Types: Access-Response

Default: Disabled

Use the following CLI command to set this parameter locally:

```
set network user <name> default_route_option [ENABLE | DISABLE]
```

0x9841 MP-EDO (Multilink PPP Endpoint Discriminator Option)

Specifies the endpoint descriptor for Multilink PPP. The EDO identifies the system transmitting a packet. It advises a system that the peer on this link could be the same as the peer on another existing link.

Values: ASCII string
 User Types: Framed, Callback and Dialout
 Packet Types: Accounting-Request-Start, Accounting-Request-Stop

0x9842 Modem-Training-Time

Modem Training Time is the delay in seconds between the time when a call arrives and is actually connected. When a call arrives the modem notifies HiPer ARC with a PacketBus message. HiPerARC answers the call and when the call is connected the modem again notifies this event. The interval between these notifications is the modem training time.

Values: Integer
 User Types: Always sent
 Default: None
 Packet Types: Accounting-Request-Start, Accounting-Request-Stop, Accounting-Request-Interim-Update

0x9843 Interface-Index

Describes the interface index value of the interface the call is established on. The least significant byte is the physical port number of the card in the chassis. The second least significant byte is the slot number of the card in the chassis. For instance, 0x00000503 indicates the call has been processed on port 3/slot 5.

Values: Integer greater than 1
 Default: None
 Packet Types: Access-Request, Accounting-Request-Start, Accounting-Request-Stop, Accounting-Request-Interim-Update

0x9844 Tunnel-Security

Defines the security level of the tunnel. The value is sent if the user defined in the RADIUS server has this attribute set.

Values: None (0), Control only (1), Data only (2), Data and Control (3)
 User Types: Sometimes sent
 Default: 0-None
 Packet Types: Access-Request

Use the following CLI command to set this parameter locally:

```
set tunnel user <name> security <none | control_only | data_only | both_data_and_control>
```

0x9845 Port-Tap

Enables/disables tapping of the HiPer ARC data stream.

Values: Disabled (0)/Enabled (1)
User Types: Sometimes sent
Default: 0-Disabled
Packet Types: Access-Accept

0x9846 Port-Tap-Format

Specifies the outputted format of packets tapped on HiPer ARC.

Values: ASCII (0), Hexadecimal (1), Clear text (2)
User Types: Sometimes sent
Default: 0-ASCII
Packet Types: Access-Accept

0x9847 Port-Tap-Output

Specifies where tapped HiPer ARC data packets are sent.

Values: Integer: 0-Syslog
User Types: Sometimes sent
Default: 0-Syslog
Packet Types: Access-Accept

0x9848 Port-Tap-Facility

Specifies the facility identified to store HiPer ARC packets.

Values: Integer: Log_Auth (1), Log_Level0 (2) - Log_Level7 (9)
User Types: Sometimes sent
Default: 1-Log_Auth
Packet Types: Access-Response

0x9849 Port-Tap-Loglevel

Specifies the level of HiPer ARC packet traffic to log.

Values: Integer: Critical (0), Unusual (1), Common (2), Verbose (3)
User Types: Sometimes sent
Default: 0-Critical
Packet Types: Access-Accept

0x984A Port-Tap-Address

Specifies where tapped output of the SYSLOG daemon running on the specified IP address is sent to.

Values: IP Address
User Types: Sometimes sent
Default: None
Packet Types: Access-Accept

0x984B MobileIP-Home-Agent-Address

This attribute not supported in the current release.

The following undefined attribute is not supported in this release:

0x984C Tunneled-MLPP

0x984D Multicast-Proxy

Indicates which Ethernet interface to proxy multicast groups that have been learned or joined on this WAN interface.

Values: Integer: any valid interface number
User Types: Callback
Default: 0
Packet Types: Access-Accept

The following undefined attribute is not supported in this release:

0x984E Multicast-Receive

0x9850 Multicast-Forwarding

Indicates the state of multicast forwarding on this network.

Values: Integer: Enabled (1), Disabled (2)
User Types: Callback
Default: Disabled
Packet Types: Access-Accept

0x9851 IGMP-Query-Interval

Indicates the period in seconds between IGMP query transmissions.

Values: Integer: 5-65535
User Types: Callback
Default: 125
Packet Types: Access-Accept

0x9852 IGMP-Maximum-Response-Time

Indicates the greatest allowable response time in seconds advertised in IGMPv2 queries on this interface

Values: Integer: 1-10
User Types: Callback
Default: 10
Packet Types: Access-Accept

0x9853 IGMP-Robustness

Sets tuning of this interface for the expected packet loss on a subnet.

Values: Integer: 1-5)
User Types: Callback
Default: 2

Packet Types: Access-Accept

0x9854 IGMP-Version

Indicates the version of IGMP running on this interface.

Values: Integer: 1 or 2

User Types: Callback

Default: 2

Packet Types: Access-Accept

0x9855 IGMP-Routing

Indicates the state of IGMP routing on this interface.

Values: Integer: Enabled (1), Disabled (2)

User Types: Callback

Default: Disabled

Packet Types: Access-Accept

0x9865 Chat-Script-Name

Refers to a file stored locally in HiPer ARC FLASH memory which contains all Chat Script instructions in ASCII-formatted text. After successful authentication, if a user has configured this attribute and the corresponding script file exists in FLASH, script processing will begin and commands contained in the script file will be executed. If both the attribute and normal HiPer ARC processing are configured, chat script values take precedence. If both Chat-Script-Name and Rules attributes are configured, the Name attribute takes precedence.

Values: String

User Types: Login

Default: None

Packet Types: Access-Accept

0x9866 Chat-Script-Rules

Specifies any Chat Script rules stored in the RADIUS user's profile. This attribute can accept as many values as expressed in the user profile. These values are concatenated and executed after successful authentication. When this attribute is used in conjunction with the RADIUS user's profile, normal processing by HiPer ARC is bypassed. But, if this attribute is missing for a user, normal processing (the specified remote IP address will be consulted by HiPer ARC) continues. Also, if both the attribute and normal HiPer ARC processing are configured, chat script values take precedence. If both Chat-Script-Name and Rules attributes are configured, the Name attribute takes precedence.

Values: String - explicit Chat Script rules. For example:
 chat_script_rules = "TIMEOUT 30;"
 chat_script_rules = "start:"
 chat_script_rules = "EXPECT %ip_addr %port_number;"

User Types: Login

Default: None

Packet Types: Access-Accept

HiPer ARC-Supported Local Attributes Not Set Via RADIUS

Expiration

Specifies the date when the password expires. Value must be enclosed in quotes (e.g.: "June 15, 1999").

Values: 32-bit integer
User Types: All
Default: No expiration

Use the following CLI command to set this parameter locally:

```
set user <user_name> expiration <mm:dd:yy>
```

Location_Type

Indicates the location type for the user. *Timed*, *continuous* and *ondemand* users are used locally but not set by RADIUS.

Values: ASCII string: Continuous, Ondemand, Manual, Timed
User Types: Framed, Dialout
Default: None

Use the following CLI command to set this parameter locally:

```
set dial_out user <user name> site type [ondemand | timed | continuous | manual]
```

Filter_ID_Output

Indicates the output filter defined for the user. The filter name specified after the comma in the FILTER_ID_INPUT field is placed in this value.

Values: ASCII string of less than 254 characters.
User Types: Framed, Dialout, Callback
Default: Null

Use the following CLI command to set this parameter locally:

```
add filter <filter_name>
```

Start_Time

Indicates the time a timed location user should start each day. *Timed*, *continuous* and *ondemand* users are used locally but not set by RADIUS.

Values: 32-bit integer
User Types: Framed, Dialout
Default: None

Use the following CLI command to set this parameter locally:

```
set dial_out user <user name> site start_time <time>
```

End_Time

Indicates the time a timed location user should finish each day. *Timed*, *continuous* and *ondemand* users are used locally but not set by RADIUS.

Values: 32-bit integer

User Types: Framed, Dialout
 Default: None

Use the following CLI command to set this parameter locally:

```
set dial_out user <user name> site start_time <time>
```

Login_Callback_Number_Two

Indicates the alternate phone number HiPer ARC uses to call back or dialout to a user.

Values: ASCII string of less than 254 characters.
 User Types: Dialout, Callback
 Default: Null

Use the following CLI command to set this parameter locally:

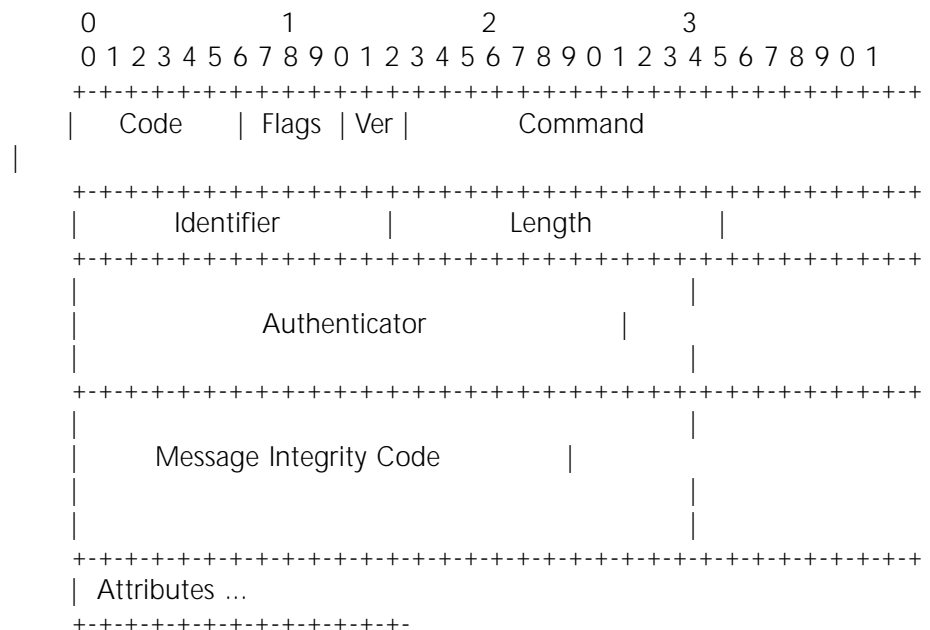
```
set user <user_name> alternate_phone_number [number] type callback]
```

Enhanced RADIUS Support

The Enhanced RADIUS protocol is supported by HiPer ARC. Enhanced RADIUS is an extension of the existing RADIUS specification. Since RADIUS Version 1 has a very limited number of available commands and attributes, the intent of the Enhanced RADIUS protocol is to allow for future protocol enhancements. This document describes the packet headers for the Enhanced RADIUS protocol as well as any commands and attributes which **must** be supported.

Enhanced Packet Formats

Exactly one RADIUS packet is encapsulated in the UDP Data field, where the UDP Destination Port field indicates 1645. When a reply is generated, source and destination ports are reversed. A summary of the Enhanced RADIUS data format is shown below. Fields are transmitted from left to right.



Code The Code field is one octet in length, and identifies the type of RADIUS packet. When a valid code is received, the packet format to use is as defined in the RADIUS V1 specification. When a packet is received with an invalid Code field, it is silently discarded. When a code of 0xFE (254) is received, it identifies an Enhanced RADIUS packet as shown above, in which case the Command field is to be checked. In this case, the RADIUS Codes which follow (with the exception of 254) are passed in the Command field instead.

RADIUS Codes (decimal) are assigned as follows:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server (experimental)
- 13 Status-Client (experimental)
- 254 Enhanced RADIUS packet

Flags The Flags field is five bits in length, and is used in order to identify any options. This field **must** be set to zero unless any options are used. The following flags are defined globally for all commands:

0x1 - (Bit 12) TimeStamp is included in the Authenticator Field.



Additional options in the Flag field may be defined per Command (see individual commands).

Version The Version field is three bits in length, and indicates the version number which is associated with the packet received. This field **must** be set to 2.

Command The Command field is two octets in length, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, a Command-Unrecognized message should be returned. RADIUS Commands (decimal), in addition to those shown above, are assigned as follows:

- 256 - Command-Unrecognized
- 267 - NAS-Reboot-Indication
- 268 - NAS-Reboot-Ack
- 304 - Radius-Change-Filter-Request
- 305 - Radius-Change-Filter-Request-Ack
- 306 - Radius-Change-Filter-Request-Nak

Identifier The Identifier field is two octets in length, and aids in matching requests and replies.

Length The Length field is two octets in length. It indicates the length of the packet including the header fields. Octets outside the range of the Length field should be treated as padding and should be ignored on reception.

Authenticator The Authenticator field is a random 16-octet value. This field adds randomness to the packets and makes the guessing of the shared secret much more difficult to the malicious user.

If the Timestamp option is supported, the first four octets contain a timestamp of when the packet was sent from the peer. This allows the protocol to detect replay attacks. The Timestamp value is the current time relative to a base of 0:0:0 GMT January 1, 1900.

Message Integrity Code This field contains an MD5 hash of the following:
MD5 (packet | Shared Secret)

When creating a message, the Message Integrity Code (MIC) must be set to all zeros before calculating the MD5 hash. When receiving a message, the receiver must save the MIC, set the field to all zeroes and perform the hash function. The resulting value **MUST** be identical to the value which was in the message.

Attributes RADIUS attributes carry the specific authentication, authorization, information and configuration details for the request and reply. Some attributes may be listed more than once. The effect of this is attribute specific, and is specified by each such attribute description.

The end of the list of attributes is indicated by the length of the RADIUS packet. A summary of the attribute format is shown below. The fields are transmitted from left to right.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Attribute Type   |   Length   |
+-----+-----+-----+-----+-----+-----+-----+
|   Flags   |   Vendor ID (optional)   |
+-----+-----+-----+-----+-----+-----+-----+
|Vendor ID (opt)| Value ... |
+-----+-----+-----+-----+-----+-----+

```

Type The Type field is two octets in length. RADIUS Version 1 reserves the lowest 256 attribute numbers. Up-to-date values of the RADIUS Type field are specified in the most recent "Assigned Numbers" . Enhanced RADIUS Versions will use attribute numbers 257 and above. Vendor Specific attributes reside within this space when the Vendor Specific bit is set (see flags). This will allow up to 65535 trouble-free vendor specific attributes (per vendor).

Length The Length field is two octets in length, and indicates the length of this Attribute including the Type, Length, Flag, Vendor ID is present and Value fields. If a packet is received with an Invalid length, the packet should be rejected.

Flags The Flags field indicates how the NAS or RADIUS Server **must** react to the attribute. The following values are currently supported:

- 1 - The Device must support this attribute. If the attribute is NOT supported, the device must reject the Command. If this flag is not set, then the device

may accept the command regardless of whether or not the particular attribute is recognized.

- 128 - If this bit is set, the optional Vendor ID field will be present. When set, the attribute is a vendor specific attribute.

Value The Value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field is determined by the Type and Length fields. The format of the value field is one of five data types:

- string - 0-65535 octets.
- address - 32-bit value, most significant octet first.
- extended address - Address Length is determined from the Length field, most significant octet first. This is required in order to support protocols which require an address length greater than 32 bits (i.e. IPNG). Note that this type is differentiated from the previous type by the value of length.
- integer - 32-bit value, most significant octet first.
- time - 32-bit value, most significant octet first -- seconds since 00:00:00 GMT, January 1, 1900

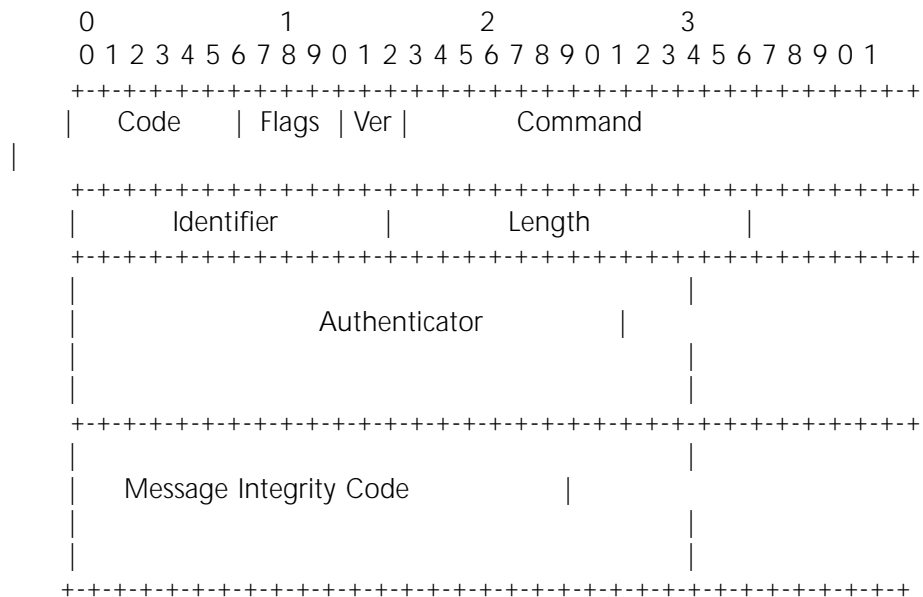
Enhanced Command Codes

256 Command-Unrecognized

Command-Unrecognized packets are sent by the NAS or the RADIUS server to inform its peer that a previous packet received is unrecognized.

Since there certainly will exist a case where an existing device does not support a new extension to the Enhanced RADIUS protocol, a device which receives a packet with an unrecognized Command code should return a Command-Unrecognized packet.

For backward compatibility with RADIUS Version 1, a device must support the fact that its peer may silently discard the packet. A summary of the Command-Unrecognized packet format is shown below. The fields are transmitted from left to right.



Code 254 for Enhanced RADIUS.

Flags The Flag field is used as described above.

Version Must be set to 2

Command 256 for Command-Unrecognized.

Identifier The Identifier field is a copy of the Identifier field of the packet which caused this event.

Length The total length of the message, including this header.

Authenticator The Authenticator field is a random 16-octet value. If the Timestamp option is supported, the first four octets contains a timestamp of when the packet was sent from the peer.

Message Integrity Code This field contains an MD5 hash of the following:
MD5 (packet | Shared Secret)

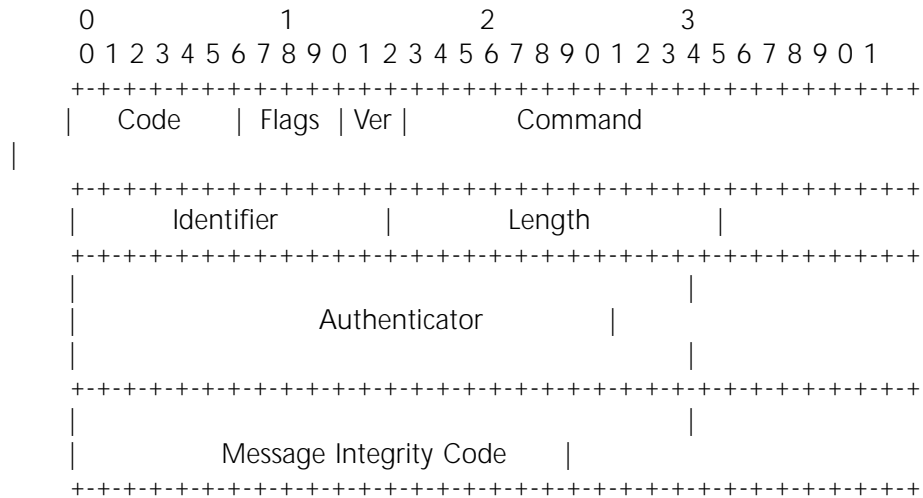
267 NAS-Reboot-Indication

The NAS-Reboot-Indication message is sent from the NAS to the RADIUS Server in order for the NAS to inform the local server that it has rebooted. The server must respond to the message with a successful acknowledge, indicating its version. This message is used by both the NAS and the RADIUS Server in order to exchange protocol version numbers which it supports. The NAS must insert the highest version number which it supports. The RADIUS Server must respond with the highest version which it supports, but may not be higher than the version number requested by the NAS.

In the case of a proxy server, the proxy is responsible for inserting the highest version number which it supports in the version field before sending the proxy request to the remote RADIUS server. The proxy server may then retain the version number of the remote server as received in the response, and must insert its highest version number (with the limitations described above) in the response to the NAS.

The Server may discard this information if it wishes to do so. It is envisioned that the Server would retain the NAS' and remote RADIUS server's version numbers to retain backward and forward protocol compatibility. A HiPer ARC must support the fact that it may not receive an acknowledge to this message if the RADIUS Server does not support this version of the protocol. In this case, and no acknowledge was received, it would default to version 1 messages.

If a HiPer ARC is configured to communicate with more than one RADIUS server it MUST issue NAS-Reboot-Indications to each server. The format for this attribute is as follows:



Code 254 for Enhanced RADIUS

Flags The Flag field is used as described above.

Version The version field is used by the NAS to indicate the highest supported version of the RADIUS protocol. this will allow HiPer ARC and RADIUS Server to be able to negotiate a version of the protocol to use between both peers.

Command 267 for NAS-Reboot-Indication.

Identifier The Identifier field **must** be changed whenever the content of the attributes field changes, and whenever a valid reply has been received for a previous request. For re-transmissions, the Identifier may remain unchanged.

Length The total length of the message, including this header.

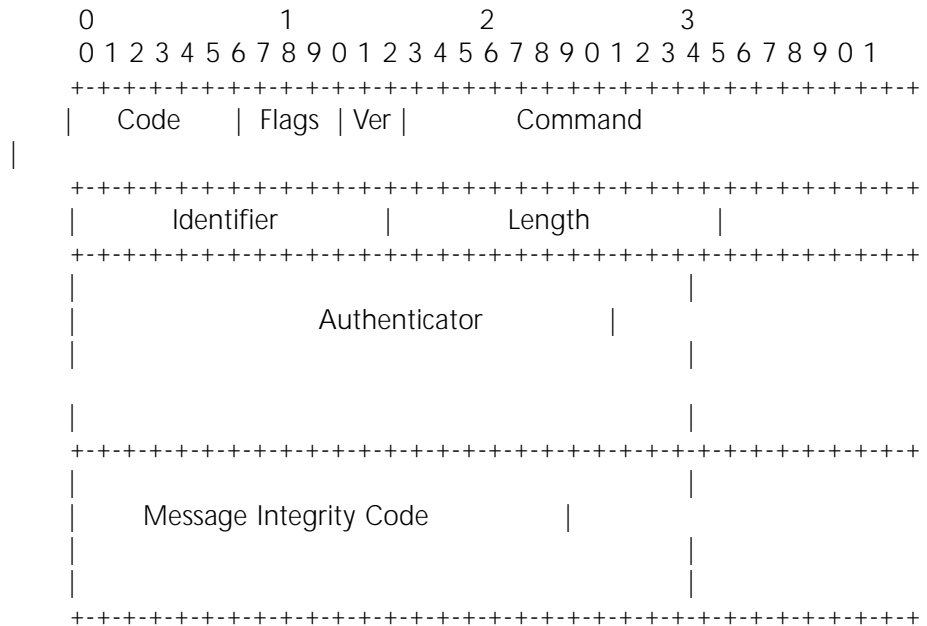
Authenticator The Authenticator field is a random 16-octet value. If the Timestamp option is supported, the first four octets contain a timestamp of when the packet was sent from the peer.

Message Integrity Code This field contains an MD5 hash of the following:
MD5 (packet | Shared Secret)

268 NAS-Reboot-Ack

The NAS-Reboot-Ack message is sent from the RADIUS Server to HiPer ARC to acknowledge the receipt of the NAS-Reboot message. The Server **MUST** replace the version value in the version field with the highest version number which it supports, up to and including the version which was included in the NAS-Reboot's version field.

HiPer ARC may wish to ignore the version number contained in the Flag field. It is envisioned that the NAS would retain this information to remove any backward compatibility problems with any future versions of the protocol. The format for this attribute is as follows:



Code 254 for Enhanced RADIUS.

Flags The Flag field is used as described above.

Version The Version field is used by the RADIUS Server to inform the NAS the highest version which it supports. The Server must not insert a version which is higher than requested by the NAS. The client must use the version which is reported by the Server. If the NAS does not support the version returned by the Server, it should default to RADIUS V1.

Command 268 for NAS-Reboot-Ack.

Identifier The Identifier field is a copy of the Identifier field of the packet which caused this event.

Length The total length of the message, including this header.

Authenticator The Authenticator field is a random 16-octet value. If the Timestamp option is supported, the first four octets contain a timestamp of when the packet was sent from the peer.

Message Integrity Code This field contains an MD5 hash of the following: MD5 (packet | Shared Secret)

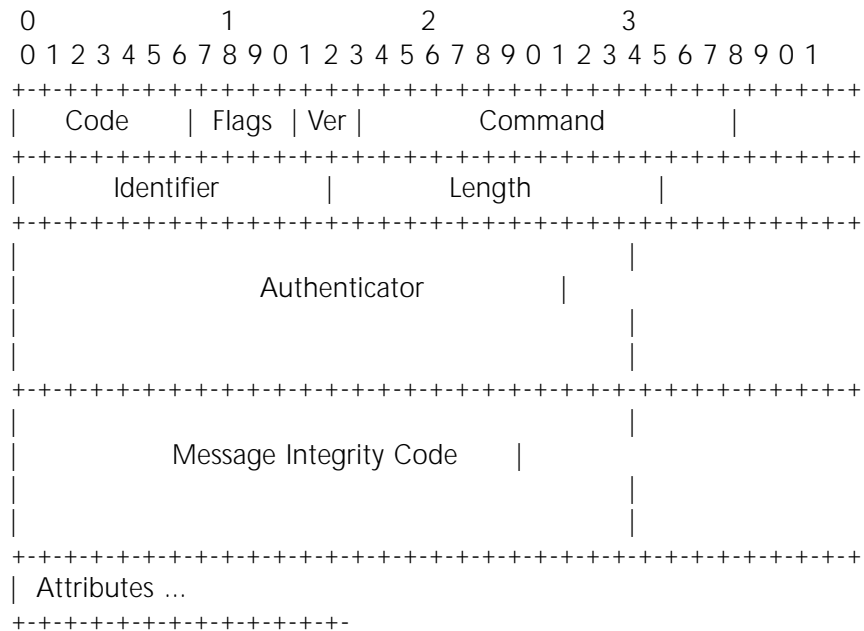
Dynamic Filter Change

As ISP service offerings expand, the need exists for a user to request a new set of filters to be applied to his session on HiPer ARC. The existing method offers two distinct accounts for the user, each with a different set of filters. A more graceful method allows a user to request, with an out-of-band message to the RADIUS server, a change of the user's filters.

304 RADIUS-Change-Filter-Request

RADIUS-Change-Filter-Request packets are initiated by the RADIUS Server to the NAS when a change to the users' filters is required. A NAS which does not

support this feature *may* return a Command-Unrecognized message. The format for this attribute follows:



Code 254 for Enhanced RADIUS.

Command 304 for RADIUS-Change-Filter-Request

Identifier The Identifier field must be changed whenever the content of the attributes field changes, and whenever a valid reply has been received for a previous request. For retransmissions, the Identifier may remain unchanged.

Length The total length of the message, including this header.

Authenticator The Authenticator field is a random 16-octet value. If the Timestamp option is supported, the first four octets contain a timestamp of when the packet was sent from the peer.

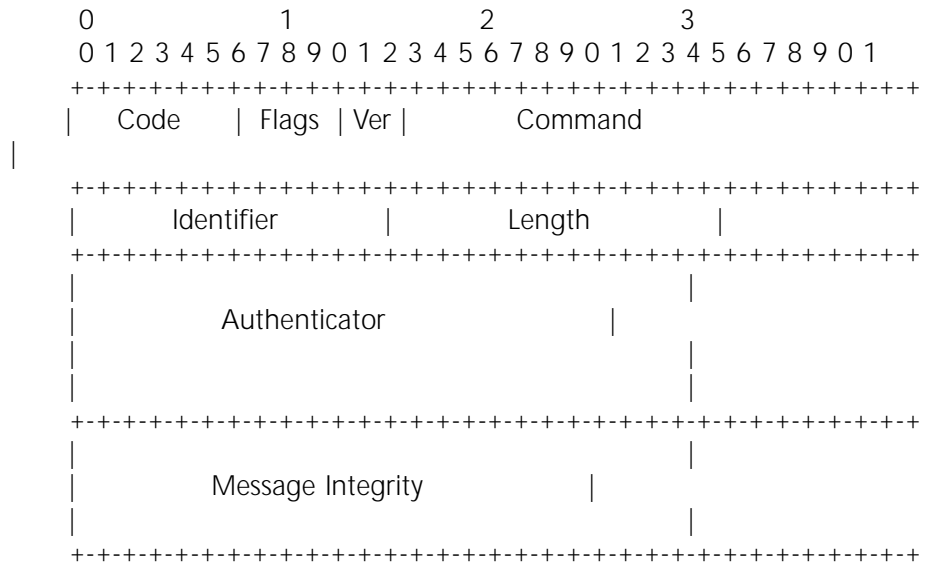
Message Integrity Code This field contains an MD5 hash of the following: MD5 (packet | Shared Secret)

Attributes The Attribute field is variable in length. The following RADIUS attributes are included in the message:

- *NAS-IP-Address* - This attribute **must** contain the IP Address of the NAS.
- *NAS-Port* - This attribute **must** contain the port number of the user.
- *Filter-Id* - This attribute may be present if the NAS uses filter naming. A vendor specific filter rule may be sent in its place. The absence of a filter attribute removes all filters currently assigned to user's port.

305 RADIUS-Change-Filter-Request-Ack

RADIUS-Change-Filter-Request-Ack packets is sent from the NAS to the RADIUS Server if the filter was successfully changed. The format is as follows:



Code 254 for Enhanced RADIUS.

Version MUST be set to 2

Command 305 for RADIUS-Change-Filter-Request-Ack

Identifier The Identifier field is a copy of the Identifier field of the RADIUS-Change-Filter-Request which caused this RADIUS-Change-Filter-Request-Ack to be sent.

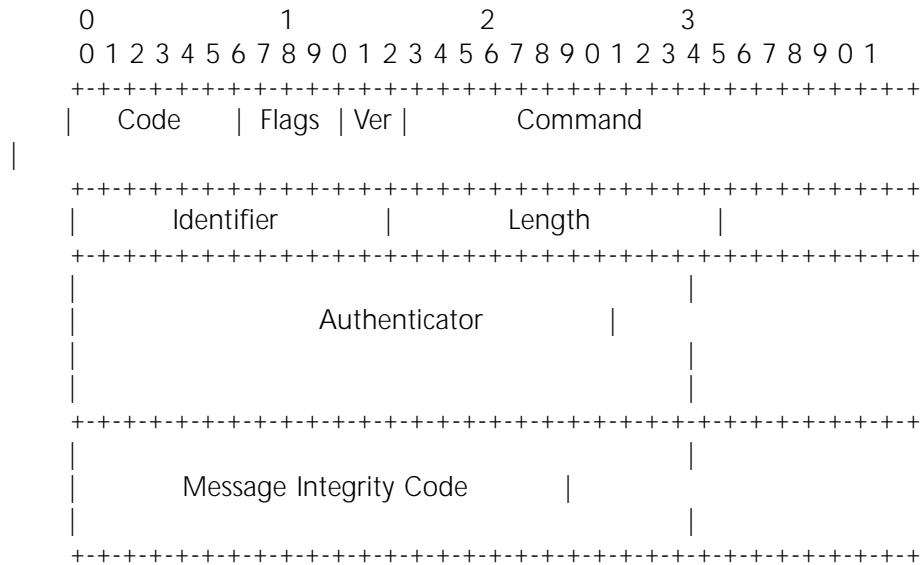
Length The total length of the message, including this header.

Authenticator The Authenticator field is a random 16-octet value. If Timestamp option is supported, the first 4 octets contain a timestamp for when the packet was sent from the peer.

Message Integrity Code This field contains an MD5 hash of the following:
MD5 (packet | Shared Secret)

306 RADIUS-Change-Filter-Request-Nak

RADIUS-Change-Filter-Request-Nak packets are sent from HiPer ARC to the RADIUS Server if the filter was not successfully changed. The message should be sent as follows:



Code 254 for Enhanced RADIUS.

Version MUST be set to 2

Command 306 for RADIUS-Change-Filter-Request-Nak

Identifier The Identifier field is a copy of the Identifier field of the RADIUS-Change-Filter-Request which caused this RADIUS-Change-Filter-Request-Nak to be sent.

Length The total length of the message, including this header.

Authenticator The Authenticator field is a random 16-octet value. If the Timestamp option is supported, the first four octets contain a timestamp of when the packet was sent from the peer.

Message Integrity Code This field contains an MD5 hash of the following:
MD5 (packet | Shared Secret)

The rationale for this protocol extension is to allow RADIUS servers to download filters dynamically. In the past, a user would have needed two separate user accounts, or if some dynamic filter mechanism on the RADIUS server had existed, the user would have had to logoff and log back in.

This extension provides the service provider the capability of adding new services to existing infrastructure. It is envisioned that the client would have access to an application which would send an out-of-band request to the service provider's RADIUS server, which would in turn send a new set of filters to the NAS for the user's port.

Upon receipt of a RADIUS-Change-Filter-Request, the NAS **must** ensure that the NAS port is still active. If so, the NAS must replace any filters which are currently applied to the port with the new set of filters received in the message.

If the Filter-Id attribute is included in the message, then the NAS must use it in the traditional RADIUS method, however the message may also support vendor

specific filter rules instead. The absence of any filters in the message will remove any such filters currently applied to the user's port.

Enhanced RADIUS Reference Information

The documents listed below are available on the Internet, at the address listed in the front of this manual. These documents serve as an excellent source of additional information for Enhanced RADIUS.

- draft-calhoun-enh-radius-00.txt
- draft-calhoun-enh-radius-eap-00.txt
- draft-calhoun-enh-radius-filter-00.txt
- draft-calhoun-enh-radius-res-mgmt-00.txt

Internet-Drafts are valid for a maximum of six months and may be updated, replaced, or rendered obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as works in progress.

RADIUS Attributes

RADIUS uses specific attributes in authentication requests and responses, as well as for specific accounting functions. These "standard" and vendor-specific attributes are detailed in the table below. This section lists RADIUS attributes used by HiPer ARC.



In table, the term NAS (Network Application Server) refers to HiPer ARC.

RADIUS Attributes

RADIUS attributes are defined using these terms:

- Req - *Request* message to RADIUS server;
- Acpt - *Accept* response from RADIUS server
- Rej - *Reject* response from RADIUS server
- Chal - *Challenge* response from RADIUS server
- NS - *Not Supported* in the current release
- X - Security message *Always* sent
- O - Security message *Optionally* sent
- F - *Framed* User Only
- L - *Login* User Only
- M - *Modem* User Only

[illegible]

[illegible]

3Com Specific Extensions <i>Not</i> Used by HiPer ARC (224 - 240)		
224	User-Group-Name	NS
225	Dial-In-Sec-Mode	NS
226	Req-Db-Mdm-Sel	NS
227	Req-Db-Login-Valid	NS
228	Dialback-Group-Names	NS
229	Dial-In-Call-Rest	NS
230	Dial-Out-Call-Rest	NS
231	Logins-Before-Blacklist	NS
232	Failed-Logins	NS
233	Allowed-DB-Modems	NS

3Com Vendor Specific Extensions (9000-9FFF)								
Id	Name	Length	Req	Acc	Rej	Chal	Start	End
0x9000	IP-Input-Filter	>10 bits		F,o				
0x9001	IPX-Input-Filter							
0x9002	IPX-SAP							
0x9003	IP-Output-Filter	>10 bits		F,o				
0x9004	IPX-Output-Filter							
0x9005	SAP-Output-Filter	>10 bits		F,o				
0x9006	VPN-ID							
0x9007	VPN-Name							
0x9008	VPN-Neighbor							
0x900A	VPN-Gateway							
0x900B	Tunnel-Authenticator							
0x900C	Packet-Index		NS					
0x900D	Cutoff		NS					
0x900E	Access-Accept-Packet							
0x900F	Primary-DNS-Server	32 bits		o				
0x9010	Secondary-DNS-Server	32 bits		o				
0x9011	Primary-NBNS-Server	32 bits		o				
0x9012	Scndry-NBNS-Server	32 bits		o				
0x9013	Syslog-Tap		NS					
0x9014	MIC		F,L,o					
0x9015	Call-Tracking-ID		NS					
0x9017	Log-Filter-Packet			L,F,o				
0x9019	Chassis-Call-Slot	14 byte	x				m	m
0x901A	Chassis-Call-Span	14 byte	x				m	m
0x901B	Chassis-Call-Channel	14 byte	x				m	m
0x901C	Keypress-Timeout	14 byte				o		
0x901D	Unauthenticated-Time		NS				m	m
0x901E	VPN-Encrypter							
0x9020	Re-CHAP-Timeout		NS					
0x9801	Speed-of-Connection		Not supported locally					
0x9802	Max-Channels			F,o				
0x9803	Channel-Expansion			F,o				
0x9804	Channel-Decrement			F,o				
0x9805	Expansion-Algorithm			F,o				
0x9806	Compression-Algorithm			F,o				
0x9807	Receive-ACC-Map			F,o				
0x9808	Transmit-ACC-Map			F,o				
0x980A	Compression-Reset-Mode			F,o				
0x980B	Min-Compression-Size			F,o				
0	Location-Type		NS					
0x980C	IP			F,o				
0x980D	IPX							
0x980E	Filter-Zones		NS					
0	Filter-ID-Output							
0x980F	AppleTalk		NS					
0x9810	Bridging		NS					
0x9811	Spoofing			F,o				
0x9814	Send-Password			F,o				
0x9817	Send-Script-1			o				
0x9818	Reply-Script-1			o				
0x9819	Send-Script-2			o				
0x981A	Reply-Script-2			o				
0x981B	Send-Script-3			o				

0x981C	Reply-Script-3		o				
0x981D	Send-Script-4		o				
0x981E	Reply-Script-4		o				
0x981F	Send-Script-5		o				
0x9820	Reply-Script-5		o				
0x9821	Send-Script-6		o				
0x9822	Reply-Script-6		o				
0x9823	Terminal-Type		L,o				
0x9824	AppleTalk-Network-Range		NS				
0x9825	Local-IP-Address		F,o				
0x9826	Routing-Protocol		F,o				
0x9827	Modem-Group		L,F,o				
0x9828	IPX-Routing						
0x9829	IPX-WAN						
0x982A	IP-RIP-Policies		F,o				
0x982B	IP-RIP-Simple-Auth-Password		F,o				
0x982C	IP-RIP-Input-Filter		F,L,o				
0x982D	IP-Call-Input-Filter		F,L,o				
0x982E	IPX-Call-Input-Filter						
0x9831	AT- Input-Filter						
0x9832	AT-RTMP-Input-Filter						
0x9833	AT-ZIP-Input-Filter						
0x9834	AT-Call-Input-Filter						
0x9835	ET-Bridge-Input-Filter	NS					
0x9838	IPX-RIP-Output-Filter						
0x9839	IPX-Call-Output-Filter						
0x983A	AT-Output-Filter						
0x983B	ET-RTMP-Output-Filter						
0x983C	AT-ZIP-Output-Filter						
0x983D	AT-Call-Output-Filter						
0x983E	ET-Bridge-Output-Filter	NS					
0x983F	ET-Bridge-Call-Output-Filter	NS					
0x9836	IP-RIP-Output-Filter		F,L,o				
0x9837	IP-Call-Output-Filter		F,L,o				
0x9840	Default:-Route-Option		F,o				
0x9845	Port-Tap						
0x9846	Port-Tap-Format						
0x9847	Port-Tap-Output						
0x9848	Port-Tap-Facility						
0x9849	Port-Tap-Loglevel						
0x984A	Port-Tap-Address						

RADIUS Accounting Attributes

This table shows attributes used in HiPer ARC for RADIUS Accounting.

		HiPer ARC	
Attribute		Call Start	Call End
Id	Name	.rad	.rad
Standard RADIUS Attributes			
1	User-Name	x	x
2	Password	Never	
3	CHAP-Password	Never	
4	NAS-IP-Address	x	x
5	NAS-Port	x	x*
6	Service-Type	x	x
7	Framed-Protocol	F	F
8	Framed-IP-Address	F	F
9	Framed-IP-Netmask	NS	
10	Framed-Routing	NS	
11	Filter-Id	NS	
12	Framed-MTU	NS	
13	Framed-Compression	NS	
14	Login-IP-Host	L	L
15	Login-Service	L	L
16	Login-Port	L	L
17	Old-Password (NMC Only)	NS	
18	Reply-Message	NS	
19	Callback-Number	NS	
20	Callback-Id	NS	
21	Expiration (deprecated)		
22	Framed-Route	NS	
23	Framed-IPX-Network	NS	
24	State	NS	
25	Class	o	o
26	Vendor-Specific		
27	Session-Time-out	NS	
28	Idle-Time-out	NS	
29	Termination-Action	NS	
30	Called-Station-ID	F,L	F,L
31	Calling-Station-ID	F,L	F,L
32	NAS-Identifier	NS	
33	Proxy-State	NS	
34	Login-LAT-Service	NS	
35	Login-LAT-Node	NS	
36	Login-LAT-Group	NS	
37	Framed-AppleTalk-Link	NS	
38	Framed-AppleTalk-Network	NS	
39	Framed-AppleTalk-Zone	NS	
40	Account-Status-Type	" 1 "	" 2 "

41	Account-Delay-Time	x	x
42	Account-Input-Octets		x
43	Account-Output-Octets		x
44	Account-Session-ID	x	x
45	Account-Authentic	x	x
46	Account-Session-Time		x
47	Account-Input-Packets		F
48	Account-Output-Packets		F
49	Account-Terminate-Cause		F
50	Account-Multi-Session-ID	F,ML	F,ML
51	Account-Link-Count	F,ML	F,ML
60	CHAP-Challenge	NS	
61	NAS-Port-Type	F	F
62	Port-Limit		
63	Login-LAT-Port	NS	
USR Vendor Specific Extensions			
0x6C	Modulation-Type	x	x
0x99	Error-Control	F,L	F,L
0xC7	Compression	x	x
0x9015	Call-Tracking-ID	NS	
0x9014	Unauthenticated-Time	x	x
0x9019	Chassis-Call-Slot	x	x
0x9023	Connect-Speed	F,L,o	F,L,o
0x901A	Chassis-Call-Span	x	x
0x901B	Chassis-Call-Channel	x	x
0x901D	Unauthenticated-Time	x	x
0x982F	MP-MRRU	F	F
0x9841	MP-EDO	F	F
Server Specific			
0x9006	VPN-ID	NS	
0x901F	VPN-Gateway-Location-Id	NS	

* Except for LAN users who do not use a modem

Key: x - Always sent; o - optionally sent; F - Framed User only; L - Login User only; NS - Not Supported in the current release; ML - MultiLink

TACACS+

TACACS+ is a simple TCP-based protocol providing access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

TACACS+ improves on TACACS and XTACACS by separating the functions of Authentication, Authorization and Accounting and by encrypting all traffic between the NAS and the daemon. It allows for arbitrary length and content authentication exchanges which will allow any authentication mechanism to be utilized with TACACS+ clients. It is extensible to provide for site customization and future development features, and it uses TCP to ensure reliable delivery.

The protocol allows the TACACS+ client to request very fine grained access control and allows the daemon to respond to each component of that request.

The separation of authentication, authorization and accounting is a fundamental component of the design of TACACS+. The protocol provides for all three, but configuration is not required to use them all. Each component serves a unique purpose that alone is useful, and together can be powerful. An important benefit to separating authentication from authorization is that authorization (and per-user profiles) can be a dynamic process. Instead of a one-shot user profile, TACACS+ can be integrated with other negotiations, such as a PPP negotiation, for far greater flexibility. The accounting portion can provide security auditing or accounting/billing services.

TACACS+ uses TCP for its transport. The daemon listens at port 49 - the "LOGIN" port assigned for the TACACS protocol. This port is reserved in the assigned numbers RFC for both UDP and TCP. Current TACACS and extended TACACS implementations both use port 49.

Authentication

Authentication determines *who a user* (or entity) *is*. It can take many forms. Traditional authentication utilizes a name and a fixed password. Most computers work this way, and TACACS+ can also work this way. But, fixed passwords have limitations, mainly in the area of security. Many modern authentication mechanisms utilize "one-time" passwords or a challenge-response query. TACACS+ supports all of these. Authentication generally takes place when the user first logs in to a machine or requests a service of it.

Authentication is not mandatory, it is a site-configured option. Some sites do not require it. Others require it only for certain services (see authorization below). Authentication may also take place when a user attempts to gain extra privileges, and must identify himself as someone who possesses the required information (passwords, etc.) for those privileges.

Authorization

Authorization determines what a user is allowed to do. Generally, authentication precedes authorization, but, this is not required. An authorization request may indicate that the user is not authenticated (HiPer ARC doesn't know who they are). In this case the authorization agent must determine if an unauthenticated user is allowed the services in question. In TACACS+, authorization does not merely provide yes or no answers, but it may also customize the service for a particular user.

Examples of when authorization would be performed are: When a user first logs in and wants to start a shell, or when a user starts PPP and wants to use IP over PPP with a particular IP address. The TACACS+ daemon might respond to these requests by allowing the service, but placing a time restriction on the login shell, or by requiring IP access lists on the PPP connection.

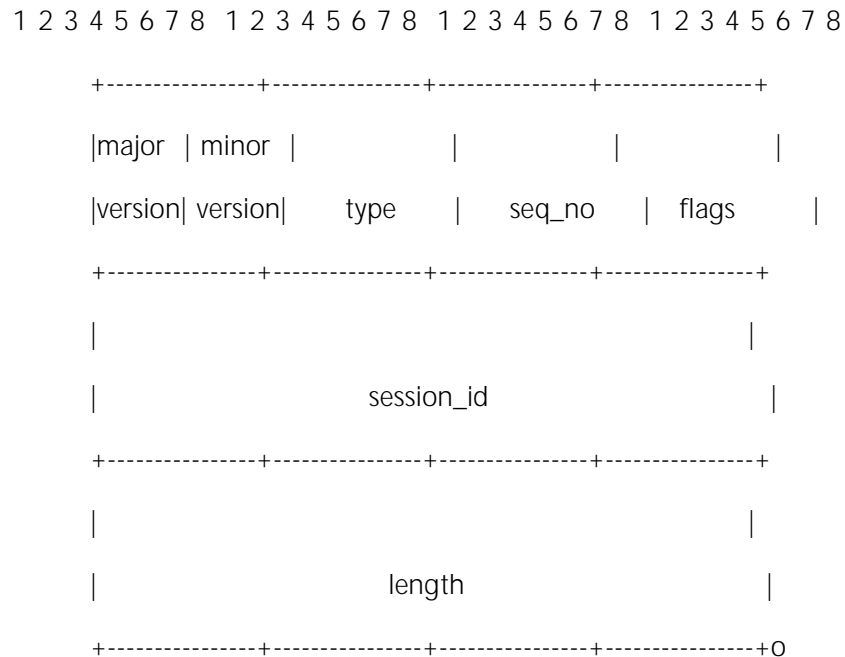
Accounting

Accounting typically follows authentication and authorization. But neither authentication nor authorization are required. Accounting records what a user is doing, and/or has done. TACACS+ accounting accounts for services used, such as billing data, and can be used as an auditing tool for security services. To this end, TACACS+ supports these accounting records:

- *Start* records indicate that a service is about to begin.
- *Stop* records indicate that a service has just terminated.
- TACACS+ accounting records contain all the information used in the authorization records, and also contain accounting specific information such as start and stop times (when appropriate) and resource usage information.

TACACS+ packet header

All TACACS+ packets always begin with the following 12-byte header. The header is always cleartext and describes the remainder of the packet:

**TACACS+ commands**

Commands to enable/disable TACACS+ functionality on HiPer ARC are described in *Chapter 11: Command Reference* of this manual.

TACACS+ Accounting Attributes

The table below itemizes attributes used in the NAS for TACACS+ accounting. Attributes associated with the three formats outlined - All, Simple, Sprint - can be specified using the CLI **set acct_format <all | simple | sprint>** command. The *All* parameter encompasses all accounting attributes provided by the NAS, *Simple* covers attributes conforming to the TACACS+ standard and *Sprint* selects attributes based on a sample provided by the Sprint lab.

Accounting Information	Attributes Format		
	ALL	SIMPLE	SPRINT
Time Connection Started	x	x	
Time Connection Updated	x	x	
Time Connection Finished	x	x	
Elapsed Time	x	x	x
# Packets and # Bytes input/output	x	x	x
NAS IP Address	x	x	x
User Name	x	x	x

User Service	x	x	x
User Protocol	x	x	x
Absolute Time-out	x	x	
Inactivity Time-out	x	x	
Date and Time	x	x	x
Task ID	x	x	x
Status (Disconnected Reasons)	x	x	
Port (Channel and Slot)	x	x	x
Host IP Address	x	x	x
Acct-Status-Type(start/stop/updated)	x	x	x
User where is authenticated	x		
Tunnel Type	x		
Tunnel Medium Type	x		
Tunnel Client Endpoint	x		
Tunnel Server Endpoint	x		
Tunnel Private Group ID	x		
Chassis Call Span	x		
Unauthenticated time	x		
Calling Station ID	x		
Called Station ID	x		
Modulation Type	x		
Error Control	x		
Compression Type	x		
Initial Connect Speed	x		
Login TCP Port	x		
Framed IPX network address	x		
Modem Training Time	x		
Multilink PPP MRRU	x		
Multilink PPP endpoint	x		
Multilink PPP link count	x		
Multilink PPP session ID	x		

TACACS+ Authorization Attributes

Each TACACS+ attribute value pair (AVP) is represented as: attribute=value. For example:

address_pool=test_pool

But, the syntax may vary with the supporting server used. HiPer ARC support for TACACS+ is detailed below in a table of describing RADIUS and 3Com VSAs and their associated values. For more information on these attributes, see their individual descriptions described earlier in this chapter. Attributes are case insensitive and any hyphen is treated as an underscore. For example, address-pool is similar to address_pool.

Attribute	Value
address_pool	string

filter_id_input	string
filter_id_output	string
framed_compression	(0)none, (1)VJ TCP header compression default:1
framed_ip_address	ip address
framed_ip_netmask	ip address
framed_ipx_network	integer default:0
framed_mtu	<ul style="list-style-type: none"> • ppp between 100 and 1514 • slip between 100 and 1006 • default:1514
framed_protocol	(1)ppp, (2)slip, (3)arap, (4)RFC1490 default:1
framed_route	string "destination gateway metric"
framed_routing	(0)None, (1)Broadcast, (2)Listen, (3)Broadcast-Listen default:0
idle_timeout	integer (seconds) default:0
login_callback_number_one	string
login_callback_number_two	string
login_host_name	string
login_ip_host	ip address
login_port	integer Default:23
login_service	(0)Telnet, (1)Rlogin, (2)Clear-TCP. (1000)Ping default:0
reply_message	string
service_type	(1>Login, (2)Framed, (3)Callback Login, (4) Callback Framed, (5)Outbound, (6)Administrative
session_timeout	integer (seconds)default:0
user_name	string
ip_input_filter	string
ip_rip_input_filter	string
ip_call_input_filter	string
ipx_input_filter	string
ipx_rip_input_filter	string
ipx_sap_input_filter	string
ipx_call_input_filter	string
ip_output_filter	string
ip_rip_output_filter	string
ip_call_output_filter	string
ipx_output_filter	string
ipx_rip_output_filter	string
ipx_sap_output_filter	string
ipx_call_output_filter	string
log_filter_packet	(0)Disabled,(1)Enabled default:0
speed_of_connection	(0)Auto, (1)56, (2)64, (3)Voice default:0
max_channels	integer default:2
channel_expansion	integer (0-100) default:0
channel_decrement	integer (0-100) default:0
expansion_algorithm	(1)constant, (2)linear default:1

compression_algorithm	(0)none, (1)Stac, (2)Ascend, (3)Microsoft, (4)Auto default:4
receive_acc_map	integer Default: 0xffffffff
transmit_acc_map	integer Default: 0xffffffff
primary_dns	ip address
secondary_dns	ip address
primary_nbns	ip address
secondary_nbns	ip adress
compression_reset_mode	(0)Auto, (1)Reset every packet, (2) Reset on error Default:0
min_compression_size	integer (1128-1514) Default:256
ipx	(1)enabled, (2)disabled default:1
ip	(1)enabled, (2)disable default:1
filter_zones	(1)enabled, (2)disable default:1
appletalk	(1)enabled, (2)disable default:1
bridging	(1)enabled, (2)disable default:1
spoofing	(1)enabled, (2)disable default:2
send_password	string
send_script1	string
reply_script1	string
send_script2	string
reply_script2	string
send_script3	string
reply_script3	string
send_script4	string
reply_script4	string
send_script5	string
reply_script5	string
send_script6	string
reply_script6	string
terminal_type	string
routing_protocol	(1)rip1, (2)rip2 default:1
modem_group	string
ipx_routing	(0)none, (1)send, (2)listen, (3)response, (4)all default:1
ipx_wan	(1)enabled, (2)disable default:2
multicast_proxy	(1)enabled, (2)disabled default:0
tunnel_type	(0)none,(1)pptp, (3)l2tp default:0
tunnel_medium	(1)ipv4 default:0
tunnel_server_endpoint	string
tunnel_private_group_id	string
tunnel_password	string
tunnel_security	(0)none, (1)control only, (2)data only, (3)data and control, default:0
tunnel_client_endpoint	string
port_tap_address	ip address

port_tap_facility	(1)Log_Auth, (2)Log_Level0, (3)Log_Level1, (4)Log_Level2, (5)Log_Level3, (6)Log_Level4, (7)Log_Level5, (8)Log_Level6, (9)Log_Level7 default:1
port_tap_format	(0)ascii, (1)hex, (2)clear default:0
port_tap_loglevel	(0)critical, (1)unusual, (2)common, (3)verbose default:0
port_tap_output	(0)syslog, (1)screen default:0
port_tap	(0)disabled, (1)enabled default:0
igmp_max_response_time	integer(1-10), default:0
igmp_multicast_forwarding	(1)enabled, (2)disabled default:0
igmp_query_interval	integer(5-65535), default:0
igmp_robustness	integer(1-5), default:0
igmp_routing	(1)enabled, (2)disabled default:0
igmp_version	(1)v1, (2)v2, default:0

In addition to the RADIUS and 3Com VSAs described above, the following table displays TACACS+ attributes supported by HiPer ARC.

TACACS+ Attributes	Corresponding NAS Attribute	Description
service	n/a	only exec and ppp supported
protocol	n/a	only ip supported
cmd	n/a	command authorization not implemented
cmd-arg	n/a	command authorization not implemented
acl	n/a	connection access list not implemented
inacl	FILTER_ID_IN	input filter name
outacl	FILTER_ID_OUT	output filter name
zonelist	n/a	AppleTalk zonelist not implemented
addr	FRAMED_IP_ADDRESS	ip address to be assigned
addr-pool	RAD_ADDRESS_POOL	name of address pool
routing	FRAMED_ROUTING	routing flag
route	FRAME_ROUTE	routing information
timeou	SESSION_TIMEOUT	in minutes
idletime	IDLE_TIMEOUT	in minutes
autocmd	n/a	auto-command not implemented
noescape	n/a	no escape character not implemented
nohangup	n/a	no hang up not implemented
priv_lvl	n/a	privilege level not implemented
remote_user	USER_NAME	user name to connect to remote host
remote_host	LOGIN_IP_HOST	ip address of connecting host
callback-dialstring	SEND_SCRIPT1	callback dialing script
callback-line	n/a	callback line not implemented
callback-rotary	n/a	callback rotary number not implemented
nocallback-verify	n/a	callback no authentication not implemented



INDEX

A

- Accounting records, keeping 115, 120
- Accounting server
 - RADIUS 398
 - Settings 398
- Add command 180
- Address pools
 - How to configure 59
- Addressing Schemes, IP Subnet Mask
 - Address Table 379
- Administrative Tools
 - Communicating with remote, local sites 165
- Administrative tools
 - Adding network services 167
 - Command values 149
 - Dial & connect commands 165
 - Discarding, renaming files 156
 - Displaying system information 176
 - Enabling, disabling & deleting network services 169
 - Ending an active process 171
 - Exiting the CLI 167
 - How to do a software download 155
 - How to reconfigure your system parameters 149
 - Resolving addresses with arp 171
 - Resolving host names 171
 - Running script files 150
 - Show connection attributes 177
 - Show memory attributes 177
 - Using network services 167
 - Using Rlogin, TELNET 169
 - Using TELNET access port 155
 - Using TELNET control characters 170
 - Using TFTP 169
 - Using the Boot Configuration Menu 152
 - Viewing facility errors 171
 - Viewing interface status, settings 175
 - Viewing system settings 175
 - Viewing TELNET status 170
- Administrative Utilities 9
- ARAP
 - Not supported by RADIUS 424
- Arp
 - arp command 200
 - How to use 171
 - list ip arp 233
- Ascend
 - Setting for compression algorithm 65, 101
- Asynchronous Control Map
 - Transmit and receive maps 101
- Authentication
 - Passwords 421
 - RADIUS
 - encryption key 396
 - framed user 423

- outbound user 424

B

- Backplane pinouts 370
- Boot Configuration Menu 22
 - Crash upload 154
 - Deleting boot configuration 154
 - Deleting router configuration 154
 - How to use 152
 - Selecting boot IP default gateway 154
 - Selecting boot IP interface 153
 - Selecting boot IP network mask 154
 - Selecting boot mode 153
 - Selecting IP configuration source 153
 - Selecting TFTP boot server IP address 154
 - Selecting TFTP image on startup 154
 - Specifying crash upload 154
 - Specifying crash upload dump file 154

C

- Callback user 182
- Case studies
 - Callback user 66
 - Dialin user 66
 - IP terminal user 53
 - LAN-to-LAN user 103
 - Login user 53
 - Manage user 62
- Channel decrement
 - Setting for LAN-to-LAN users 65, 101
- Channel expansion
 - Setting for LAN-to-LAN users 65, 101
- CHAP authentication 396
- Chassis commands
 - Configuration
 - enable nmc
 - chassis_awareness 219
 - disable nmc chassis_awareness 211
 - list chassis 227
 - list pbus datagrams 242
 - list pbus sessions 242
 - list pbus traps 242
 - set pbus trap 287
- CIDR 373
 - CIDR and the HiPer ARC 378
 - Example 378
 - How to select a netmask 376
 - How to select a range 377
 - Supernetting 375
- ClearTCP
 - Setting port number for login user 50
 - Setting service for login user 51
- CLI help 180
- CLI, abbreviation 180
- Command abbreviation
 - How to use 180
- Command abort
 - How to use 180
- Command completion
 - How to use 180
- Command help
 - How to use 180
- Command line editing
 - How to use 180
- Command Line Interface
 - Abbreviations 17
 - Case-sensitive commands 17
 - Comma separation 18
 - Command completion 18
 - Command reprint 18
 - Command retrieval 18
 - Conventions 17
 - Disabling, then deleting 19
 - Do & Kill commands 19
 - Editing 18
 - Help 19
 - Keywords 17
 - Paused output 18
 - Quick Setup program 16
 - Quotations 17
 - Rebooting 20
 - Saving changes 19
 - Syntax 17
 - Using Add & Set commands 20
 - Using List & Show commands 20
 - Using network services 19
 - Vertical line 18
- Command retrieval
 - How to use 180
- Compression algorithm
 - Ascend, Microsoft and Stac settings 101
- Configuration 36, 181
- Configuration interface
 - How to access 16
- Console baud rate
 - setting 383
- Constant
 - Setting for expansion algorithm 101
- Control characters
 - How to use 180
- conventions
 - notice icons, About This Guide xvii
 - text, About This Guide xvii
- Critical events
 - How to display 176

D

- Debugging IP connections 9
- Default Route
 - delete ip defaultroute 203
- Default User 182
- Diagnostics
 - delete traceroute 206
 - hide events 223

- list critical events 228
- PING 260
- Dial
 - dial command 206
- Dial command 166
- Dial in connections
 - How to view settings 177
- Dialout Service
 - Installing NCSI Client software 78
- Dialout service
 - Configuring NCSIPort for 95 80
 - Configuring Telnet dialout service 74
 - Configuring users 74
 - Editing network services 78
 - Example of an AT call 77
 - Examples using AT commands 77
 - How to configure 73
 - How to setup NCSI dialout service 82
 - NCSI dialout case study 87
 - NCSI's Windows options 87
 - Setting global dial-out values 74
 - Specifying a NCSI name and password 81
 - Telnet case study 89
 - Using NCSI to select a port 81
- Dialout services
 - Case studies 87
- Digital Quad Modem 12
- DIP Switches 382
 - How to set baud rates 383
 - How to view settings 383
- DNS
 - Configuration
 - add DNS host 186
 - add DNS server 186
 - delete DNS host 202
 - delete DNS server preference 203
 - list DNS hosts 229
 - list DNS servers 230
 - set DNS 272
 - set DNS server preference 273
 - set ppp system_dns_usage 288
 - show dns settings 318
 - Diagnostics
 - resolve name 224, 263
 - Statistics
 - show dns counters 319
- Do command 214
- Domain Name Service (DNS) 181

E

- E1 Card 12
- Event messages 385
 - CIP message examples 390
 - Configuration file manager message examples 391
 - Console event logging 385
 - Examples 388
 - Filter Manager message examples 391
 - How to configure syslog hosts 387
 - How to display logging levels 386
 - How to set the event log level 388
 - IP dial-out message examples 392
 - IP message examples 388
 - Local Flash file logging 385
 - Logging 385
 - Logging levels 385, 386

- SYSLOG host logging 385
- TELNET message examples 392
- Telnet session 386
- UDP message examples 391
- User Manager message examples 391
- Using syslog 387
- Exit commands 167
- Expansion algorithm
 - Constant or linear settings 101

F

- FCC
 - Part 15 Compliance 367
- Filters
 - add filter 187
 - Adding filters to the managed list 138
 - Advertisement filters 130
 - Call filters 130
 - Capabilities 129
 - Configuring filters 135
 - Data filters 130
 - delete filter 203
 - Deleting a packet filter 139
 - Displaying managed filter list 135
 - Filter file components 131
 - Filter types 130
 - Filtering overview 129
 - Generating SYSLOG messages for filtered packets 139
 - Generic filter rules 132
 - Generic filters 131
 - Global filtering 146
 - How to assign filters 136
 - How to create filters 131
 - ICMP filtering 144
 - Interface, input, output, call filters 136
 - IP call filtering 145
 - IP packet filter rule examples 141
 - IP RIP filtering 143
 - Keywords 147
 - list filters 232
 - Managing filters 137
 - Masks 142
 - Protocol rules 132
 - Protocol sections 131
 - Removing filters from a user profile 138
 - Removing filters from an interface 138
 - Setting filter access 135
 - Source & destination address filtering 141
 - Specifying the filtering action 133
 - Standard port numbers 143
 - Steps to create filter files 133
 - TCP/UDP filtering 142
 - User filters 136
 - Verifying filter file contents 139
 - Verifying filter file syntax 139
 - Viewing filter files 139
- FLASH ROM 181
- Frame Relay
 - Managing
 - disable user 213

G

- Global timeout (dialout) parameters
 - How to configure 74

H

- Hardware setup 20
- HiPer ARC application
 - network dial-in access 7
- HiPer ARC Applications
 - IP terminal service 6
- HiPer ARC applications
 - Applications overview 6
 - LAN-to-LAN routing 9
- HiPer ARC features 1
- HiPer ARM Setup Wizard 16

I

- ICMP commands
 - disable icmp_logging 208
 - disable icmp_router_advertise 208
 - enable icmp_logging 216
 - enable icmp_router_advertise 216
 - show icmp counters 322
 - show icmp settings 322
- Interface 17, 179, 181
- Interface format 182
- Interfaces
 - assign interfaces 201
 - disable interface 209
 - disable link_traps interface 210
 - enable interface 217
 - list active interfaces 225
 - list interfaces 233
 - list lan interfaces 239
- Internet, viewing Web resources 100
- IP
 - ClearTCP
 - set cleartcp
 - connect_message 270
 - show cleartcp 314
 - Configuration
 - add ip network 188
 - add ip pool 189
 - delete ip network 203
 - delete ip pool 203
 - disable ip network 209
 - disable network service 211
 - enable ip network 217
 - list ip addresses 233
 - list ip networks 235
 - show ip network settings 328
 - Diagnostics
 - ARP command 200
 - list ip ARP 233
 - Routing
 - add ip defaultroute gateway 188, 275
 - add ip route 189
 - delete ip route 203
 - disable ip forwarding 209
 - disable ip rip 209
 - disable ip routing 209
 - disable ip
 - static_remote_routes 210
 - enable ip forwarding 217
 - enable ip rip 217

- enable ip routing 217
- enable ip static routes 218
- list ip routes 236
- Services
 - add network service 193
 - delete network service 205
 - enable network service 219
 - list available servers 226
 - list services 241
 - set network service 286
- Statistics
 - list ip interface_blocks 235
 - list networks 241
 - list tcp connections 249
 - list udp listeners 252
 - show ip settings 326
 - show tcp counters 355
 - show tcp settings 355
- TFTP
 - add tftp client 199
 - delete tftp client 206
 - list tftp clients 250
- IP network user
 - Adding the user 61
 - Case Study A 66
 - Case Study B 67, 69
 - Configuring PPP parameters 63
 - Setting channel decrement 64
 - Setting channel expansion 64
 - Setting idle and session timeouts 66
 - Setting maximum channels 64
 - Setting minimum compression size 64
 - Setting mtu 64
 - Setting PAP/CHAP 64
 - Setting phone and alternate phone numbers 66
 - Setting reset compression mode 64
 - Setting the address selection method 63
 - Setting the compression algorithm 64
 - Setting the expansion algorithm 64
 - Setting the receive ACC map 64
 - Setting transmit ACC map 64
 - Specifying a remote address 62
- IP terminal server setup
 - Case study 53
 - Configuring login hosts 50
 - Configuring login users 51
 - Configuring the remote computer 49
- IPX
 - Configuration
 - add ipx network 190
 - delete ipx network 204
 - disable ipx network 210
 - enable ipx network 218
 - set ipx network 280
 - show ipx network settings 331
 - show ipx settings 330
 - ROUTING
 - enable ipx rip network 218
 - show ipx RIP settings 332
 - Routing
 - add ipx route 190
 - delete ipx route 204
 - disable ipx rip network 210
 - list ipx routes 237
 - list ipx static routes 238
 - SAP
 - disable ipx sap network 210
 - enable ipx sap network 218

- list ipx services 237
- Statistics
 - list ipx networks 236
 - show ipx counters 331
 - show ipx network counters 332

L

- L2TP Access Concentrator (LAC) 114, 120
- LAN RX LED 382
- LAN TX LED 382
- LAN-to-LAN routing 91
 - Adding the user 95
 - Case study 103
 - Configuration 95
 - Configuring dialing scripts 100
 - Configuring dial-out parameters 98
 - Configuring modem groups 99
 - Configuring network parameters 95
 - Configuring PPP values 100
 - Configuring routing parameters 99
 - Connection types 92
 - Connections to remote gateways 94
 - Dialout scripts 92
 - Dynamic routes 93
 - Dynamic routing settings 92
 - IP routing 93
 - PAP and CHAP authentication 94, 95
 - Setting internal networks for unnumbered links 94
 - Setting PAP/CHAP authentication 102
 - Setting RIP 99
 - Setting the remote device phone number 98
 - Setting timeouts 99
 - Specifying a remote address 96
 - Spoofing 94
- Lan-to-LAN routing
 - Bandwidth allocation 92
 - Dialout scripts 92
- Layer Two Tunneling Protocol (L2TP) 113
- LEDs
 - LAN RX LED 382
 - LAN TX 382
 - Overview 381
 - Run/fail 381
 - STAT1 382
 - STAT2 382
 - STAT3 382
 - WAN RX LED 382
 - WAN TX LED 382
- Linear
 - Setting for expansion algorithm 101
- List command 180, 181
- Login banner
 - How to configure 75
- Login Hosts
 - add login host 192
 - delete login_host preference 204
 - list login_hosts 239
 - set login_host preference 282
 - set modem group 283
- Login hosts
 - How to configure 50
- Login prompt
 - How to configure 75
- Login user
 - RADIUS setup 423
- Login users

- Adding the user 51
- Case Study A 53
- Case Study B 55

M

- Manage user
 - How to configure 35
- Management bus 11
- Manual Setup
 - DNS configuration 33
 - SNMP configuration 33
- Manual setup
 - Default gateway configuration 30
 - IP Configuration 30
 - Power on 28
 - System basic setup 28
- Memory
 - How to view usage 177
- Messages
 - add syslog 197
 - list critical events 228
 - list syslog 248
- Microsoft
 - Setting for compression algorithm 65, 101
- Midplane, chassis 11
- MLPPP
 - Bandwidth allocation 92
 - Settings for LAN-to-LAN users 65, 101
- Modem groups
 - Configuring for Dialout service 73
- Modem groups, pools
 - How to configure 73
- Modem specs
 - Data compression protocols 371
- Modems
 - Configuration
 - add modem_group 192
 - assign interface 201
 - delete modem_group 204
 - enable modem_group 219
 - enable nmc
 - chassis_awareness 219
 - list modem_groups 239
 - list switched interfaces 248
 - set dialout 272
 - Initialization scripts
 - add init_script 187
 - delete init_script 203
 - list init_scripts 232
 - Managing
 - busy_out 201
 - dial 206
 - disable modem_group 211
 - enable ppp offloading 220
 - enable
 - service_loss_busy_out 174, 221
 - enable slip offloading 221
 - hangup interface 223
 - hangup modem_group 223
 - leave 224
 - list chassis 227
 - list connections 227
 - list dialout 228
 - list interfaces 225
 - set modem_group 283
- Multilink PPP 65, 101

Multi-link PPP Interspan Protocol
(MPIP) 113

N

NAC 10
NAC, Definition of 10
NCSI
 Case studies 87
 Configuring NCSIport for 95 80
 How to setup dialout service 82
 Installing NCSI Client software 78
 NCSI dialout case study 87
 Selecting a HiPer ARC port 81
 Specifying a password 81
 Windows options 87
Network Application Cards 10
Network dial-in access 57
 Case Study A 66
 Case Study B 67, 69
 Configuring address pools 59
 Configuring an IP network user 61
 Configuring PPP parameters 63
 IP parameters 58
 Remote addressing options 61
 Remote computer setup 58
 User configuration overview 60
 User types 61
Network dial-out access
 Configuration overview 72
 Configuration steps 73
 NPC installation 78
 Overview 71
Network Interface Cards 10
Network IP address formats 181
Network Management Card 10
Network user 17, 94, 179, 180, 181,
 379
NIC 10
NIC, Definition of 10
NMC 10
Notices
 U.S. compliance 367
NPC 78
 Client installation for Win95 78
 Overview of Windows options 87
 Setting up NCSIport for 95 80
NTP
 set ntp 286
 show ntp settings 340

O

On Demand Routing 94

P

Packet bus commands
 list pbus datagrams 242
Packet bus 12
Packet bus commands
 list pbus sessions 242
 list pbus traps 242
 set pbus trap 287
Packet Filtering 9
 Filter Out All IP Options switch 146
 IP Packet Filtering 9
Password 180, 181
Passwords

add modem_group 192
add user 200
disable authentication local 207
enable authentication local 207, 215
set dial_out user 300
set dialout 272
set modem_group 283
set network user 302
set switched interface 293
set user 303
show authentication counters 311
show authentication settings 310
Ping
 add ping_service_loss_system 174,
 195
 delete ping row 205
 delete ping service_loss_system 205
 disable ping service_loss_system 211
 disable service_loss_busy_out 212
 enable ping service_loss_system 220
 enable service_loss_busy_out 174,
 221
 How to use 172
 list ping 243
 list ping service_loss_systems 242
 ping command 260
 set ping 173, 288
 set ping service_loss_systems 288
 show ping row counters 341
 show ping server counters 342
 show ping server settings 342
 show ping settings 340
 show service_loss_busyout
 settings 351
ping 9
Point-to-Point Tunneling Protocol
(PPTP) 113
Power Supply Unit 10
PPP
 Datalink
 enable datalink ppp 216
 Dial-in
 set modem_group 283
 set switched interface 293
 show ppp settings 345
 list ppp 243
 monitor ppp 253
 PPP offloading
 disable ppp offloading 211
 enable ppp offloading 220
 see ppp ccp_modemtype_accept 288
 set network user ppp 304
 set ppp nbns_primary 288
 set ppp nbns_secondary 288
 set ppp system_dns_usage 288
 show ppp on interface counters 344
 show ppp on interface settings 342
 show ppp settings 345
 WAN
 show ppp settings 345
Protocol 36
Protocols
 layer two tunneling 113
 multi-link PPP interspan 124
 point-to-point tunneling 120
PSU 10

Q

Quick Setup
 Beginning 21

R

RADIUS
 Accounting Attributes 476
 Accounting examples 400
 Attributes 471
 Enhanced Packet Formats 461
 UDP Data field 461
 Authentication
 choosing primary server 397
 choosing secondary server 397
 configuring HiPer ARC to use 397
 framed compression 427
 Authentication Attributes 471
 Configuring from the CLI 397
 disable accounting 206
 enable accounting 214
 enable authentication remote 207,
 215
 Enhanced attributes 463
 Enhanced command codes 464
 Enhanced support 461
 HiPer ARC-specific parameters 438
 How to enable/disable
 accounting 400
 Optional parameters 420
 Required parameters 420
 set accounting 264
 set authentication 268
 show accounting counters 308
 show accounting settings 307
 show authentication counters 311
 show authentication settings 310
 User table entries 420
RADIUS authentication
 Authentication
 required parameters 420
RIP 100
 disable ipx rip network 210
 enable ip rip 217
 enable ipx rip network 218
 show ipx RIP settings 332
Rlogin 169
 How to use 170
 Setting for login user 51
 Setting port for login user 50
Run/fail LED 381

S

Scripts
 CLI
 do (run CLI script) 214
 Example 150
 Modem Initialization
 add init_script 187
 delete init_script 203
 list init_scripts 232
Security
 CLI Access
 disable security_option
 remote_user administration 212
 enable security_option remote_user
 administration 221

- Dial-in
 - disable user 213
 - enable authentication local 207, 215
 - enable user 222
 - IP Security 210
 - IP security
 - enable ip security_option
 - drop_all_fragoffset1 217
 - enable ip
 - security_option_disallow_all_header_options 217
 - enable ip
 - security_option_disallow_source_route_options 217
 - enable ip
 - security_option_drop_tcp_fragoff_set1 217
 - Login
 - disable authentication local 207
 - TELNET
 - disable telnet escape 213, 222
 - enable telnet escape 222
 - Serial Modem Ports 12
 - Sessions
 - list sessions 246
 - Set command 17, 36, 179, 180, 181, 182
 - Setting the console baud rate 383
 - Show command 182
 - SLIP commands
 - disable slip offloading 212
 - SNMP
 - add snmp community 195
 - add snmp trap_community 196
 - delete snmp community 205
 - delete snmp trap_community 205
 - disable link_traps interface 210
 - disable security_option snmp_user_access 212
 - disable snmp authentication traps 212
 - enable link_traps interface 219
 - enable security_option snmp_user_access 221
 - enable snmp authentication traps 221
 - list available servers 226
 - list snmp communities 247, 248, 353
 - show snmp counters 352
 - show snmp settings 352
 - Sockets
 - How to configure 75
 - Software configuration
 - Configuring a manage user 35
 - Finding IPX network no. 32
 - IP configuration 30
 - IPX configuration 32
 - Manual setup 28
 - Manually setting LAN interface 29, 35
 - Setting default domain 34
 - Setting default gateway 31
 - Setting DNS server 33
 - Setting IPX parameters 33
 - SNMP parameters 35
 - System parameters 29
 - Software downloads 155
 - Software specifications 371
 - Specifications
 - Environmental specs 368
 - Hardware specs 368
 - Power specs 368
 - Software specs 371
 - System standards & specs 371
 - Spoofing
 - For LAN-to-LAN users 94
 - Stac
 - Setting for compression algorithm 65, 101
 - Standard port number table 143
 - Static routes
 - How to configure 36
 - Subnet Mask Table 379
 - Subnet, mask 379
 - SW-1 and SW-2 383
 - Switched Connections
 - show connection counters 316
 - show connection settings 316
 - Syslog
 - delete syslog 205
 - Event message examples 388
 - How to configure on HiPer ARC 387
 - How to configure on UNIX server 387
 - How to set event log level 388
 - System command
 - copy 201
 - System Commands
 - delete configuration 202
 - delete file 203
 - delete syslog 205
 - do (run a script file) 214
 - help 223
 - history 224
 - kill 224
 - list facilities 230
 - list files 231
 - list processes 244
 - reboot 262
 - rename file 262
 - show configuration 315
 - System commands
 - hide events 223
 - show system settings 354
-
- T**
- T1 Card 12
 - Tables
 - Address Translation Table 47
 - Chassis and Packet Bus Tables 47
 - CLI Port Parameter Table 47
 - Dialout Port Table 46
 - DNS and Associated Tables 46
 - Event Critical Table 46
 - File Table 46
 - Filter Tables 46
 - Forward and IP Routing Table 45
 - Hosts Table 44
 - Initialization Script Configuration Table 45
 - Interface Table 44
 - IP Address Pool Table 45
 - Logging Level Table 45
 - Module Table 45
 - Network Services and Available Servers Tables 46
 - Network Table 45
 - PPP Tables 47
 - Remote Ping and Ping Busy Out Tables 47
 - SNMP Community Table 45
 - SNMP Configuration Tables 45
 - Syslog Table 46
 - TCP Connections Table 46
 - TFTP Access Table 46
 - Traceroute and Traceroute Hop Tables 46
 - UDP Customer Table 46
 - User Manager Active Sessions Table 47
 - User Table 44
 - tap 175, 197
 - TCP
 - Managing
 - add network service 193
 - disable ip security_option_drop_tcp_fragoffset1 210
 - enable ip
 - security_option_drop_tcp_fragoff_set1 217
 - list available servers 226
 - list services 241
 - list tcp connections 249
 - set clearTCP
 - connect_message 270
 - set network user 302
 - set tcp
 - maximum_connections 297
 - show tcp counters 355
 - show tcp settings 355
 - TCP/IP references
 - Douglas Comer 15
 - Network Solutions 15
 - TDM 12
 - TDM bus 12
 - Time Division Multiplexed 12
 - TELNET
 - How to use 170
 - list available servers 226
 - Setting for login user 51
 - Setting port for login user 50
 - Telnet dialout case study 89
 - TELNET commands
 - disable telnet escape 213, 222
 - Telnet socket
 - How to set number 76
 - Terminal emulation
 - Programs for PC, Mac, UNIX 16
 - Settings 16, 49
 - TFTP
 - delete tftp client 206
 - How to use 169
 - list available servers 226
 - Total Control Enterprise Network Hub 10
 - Total Control Manager Software 10
 - Traceroute
 - delete traceroute 206
 - traceroute 9
 - list traceroute 250
 - Troubleshooting
 - Resolving addresses 171
 - Resolving host names 171
 - Using ping 172
 - Using ping to monitor system links 174
 - Using RADIUS to monitor system links 174
 - Viewing facility errors 171
 - Viewing interface status and settings 175

- Viewing memory usage 177
- troubleshooting commands 9
- Tunnel user
 - creating 115
- Tunneling protocols 113
 - layer two tunneling 113
 - multi-link PPP interspan 124
 - point-to-point tunneling 120
 - virtual tunneling 113

U

- UDP
 - list available servers 226
 - list udp listeners 252
 - show accounting counters 308
 - show udp 357
 - traceroute 361
- User Datagram Protocol (UDP) 114
- Users
 - add user 200
 - delete user 206
 - disable user 213
 - list users 252
 - set dial_out user 299
 - set dial_out user site 300
 - set login user 301
 - set network user 302
 - set network user ppp 304
 - set user 303
 - show user settings 358

V

- Van Jacobsen
 - Framed compression 427
- virtual dial-up 113
- Virtual Private Network (VPN) 113
- Virtual Tunneling Protocol (VTP) 113

W

- WAN
 - PPP
 - show ppp on interface counters 344
 - show ppp on interface settings 342
 - show ppp settings 345
- WAN RX LED 382
- WAN TX LED 382
- Windows 95 Dial Up Networking 58, 67, 88

3Com Corporation LIMITED WARRANTY

The duration of the warranty for the HiPer ARC is 2 years.

HARDWARE

3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its authorized reseller:

Network Interface Cards	Lifetime
Other hardware products *unless otherwise specified above	1 year*
Spare parts and spares kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

SOFTWARE

3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation with respect to this express warranty shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product.

YEAR 2000 WARRANTY

In addition to the Hardware Products Warranty and Software Products Warranty identified above, 3Com warrants that all Heritage 3Com products sold or licensed to Customer on and after January 1, 1998 that are date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com products, including hardware, software, and firmware, accurately exchange date data with the 3Com products, with the exception of those products identified at 3Com's Web site, <http://www.3com.com/products/yr2000.html>, as not meeting this standard. A product is considered a "Heritage 3Com product" if it is a member of a product family which was manufactured by 3Com prior to its merger with US Robotics Corporation. This Year 2000 limited warranty does not apply to Heritage US Robotics Corporation products. If it appears that any such product does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days or until April 1, 2000, whichever is later.

OBTAINING WARRANTY SERVICE

Customer must contact 3Com's Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt of the defective product by 3Com.

Dead- or Defective-on-Arrival. In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the defective product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR

PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

3Com Corporation, 5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (408) 764-5000



3Com Corporation
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA
95052-8145

©1999
3Com Corporation
All rights reserved
Printed in the U.S.A.

Part No. 1.024.1905-00