

# Perle CS9000

## User Guide

5500049-24

### *Navigating around this manual*



[Fast Contents. See page 9.](#)



[Contents. See page 11.](#)



[Index. See page 271.](#)

Copyright statement

This document must not be reproduced in any way whatsoever, either printed or electronically, without the consent of:

Perle Systems Limited,  
60 Renfrew Drive  
Markham, ON  
L3R 0E1  
Canada

Perle reserves the right to make changes without further notice, to any products to improve reliability, function or design.

Perle CS9000, Specialix, the Specialix logo, JETSTREAM, JETSTREAM4000, JETSTREAM8500 and LANSTREAM2000 are trademarks of Perle Systems Limited.

Microsoft, Windows 95, Windows NT, Windows 2000 and Internet Explorer are trademarks of Microsoft Corporation.

Netscape is a trademark of Netscape Communications Corporation.

Solaris is a registered trademark of Sun Microsystems, Inc. in the USA and other countries.

Perle Systems Limited, Tuesday, November 14, 2006.

**FCC Note** The Perle CS9000 product has been 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 when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this Guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her own expense.

**EN 55022: 1998, Class A, Note**

**WARNING** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.



**Caution:** the Perle CS9000 is approved for commercial use only.



# About this Guide

## Purpose of this manual

This manual tells you how to install, configure and use the Perle CS9000 console server and associated utility software.

## Who this manual is for

This manual is aimed at users who want to communicate directly via the serial port to networked devices (such as routers, servers and so on) in order to perform system administration tasks.

This manual requires a working knowledge of using personal computers and associated operating systems, as well as experience in installing host cards and peripherals.

**NOTE: References of lines and ports are used throughout this manual referring to the serial ports on the Perle CS9000 unless specifically referenceing (i.e TCP and/or UDP ports).**



# Revision history

Date	Part number	Description
March 2001	5500049-10	Initial release of manual.
June 2001	5500049-11	Minor edit to include new colour definitions.
November 2001	5500049-12	Added in 10/100 Base-T functionality and AUI firmware update.
December 2001	5500049-13	Added in SSH support to manual content.
April 2002	5500049-14	Added enhanced security features.
July 2002	5500049-15	Cabling section update.
December 2002	5500049-16	Content update for Local Port Buffering.
March 2003	5500049-17	Content update for Remote Port Buffering feature
March 2003	5500049-18	Content updated for Easy Port Access feature, Line Access Rights, updated SNMP section and updated Authentication
September 2003	5500049-19	Content updated for updated Radius support
December 2003	5500049-20	Content updated for the multi-session feature
January 2004	5500049-21	Content updated for the SNTP, timestamping and daylight saving time features.
January 2004	5500049-22	Content updated for 32 and 48 port version
February 2004	5500059-23	Content updated for CIDR (Supernetting) feature; 48V Dual Power Input
November 2006	5500059-24	Content updated for SNTPD and ICMP service flags.



# Fast Contents

<i>ABOUT THIS GUIDE</i> .....	5
<i>REVISION HISTORY</i> .....	7
<i>FAST CONTENTS</i> .....	9
<i>CONTENTS</i> .....	11
<i>CHAPTER 1 INTRODUCTION</i> .....	21
<i>CHAPTER 2 INSTALLATION</i> .....	31
<i>CHAPTER 3 SYSTEM ADMINISTRATION</i> .....	71
<i>CHAPTER 4 USING CS9000 AS A CONSOLE SERVER</i> .....	113
<i>APPENDIX A CABLING INFORMATION</i> .....	133
<i>APPENDIX B THE CLI COMMANDS</i> .....	151
<i>APPENDIX C SNMP</i> .....	207
<i>APPENDIX D UPGRADING YOUR FIRMWARE</i> .....	213
<i>APPENDIX E SUMMARY OF LINE SERVICE TYPES</i> .....	221
<i>APPENDIX F BOOTP</i> .....	225
<i>APPENDIX G JETSET</i> .....	237
<i>APPENDIX H RADIUS ATTRIBUTES</i> .....	245
<i>APPENDIX I TROUBLESHOOTING</i> .....	257
<i>APPENDIX J CONTACTING PERLE</i> .....	265
<i>INDEX</i> .....	271



# Contents

<i>ABOUT THIS GUIDE</i> .....	5
<i>Purpose of this manual</i> .....	5
<i>Who this manual is for</i> .....	5
<i>REVISION HISTORY</i> .....	7
<i>FAST CONTENTS</i> .....	9
<i>CONTENTS</i> .....	11

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>21</b>
<i>About the Perle CS9000.....</i>	<b>22</b>
<i>Typical applications summary .....</i>	<b>24</b>
<i>Managing the CS9000 Unit .....</i>	24
<i>Managing/Accessing devices attached to the CS9000 .....</i>	24
<i>Network security .....</i>	24
<i>Management and diagnostics .....</i>	25
<b><i>Perle CS9000 front and rear views .....</i></b>	<b>26</b>
<i>CS9000 48V Model.....</i>	27
<i>Electrical Supply Details.....</i>	28
<i>Connecting DC Power Supply(s) to Console Server.....</i>	28
<i>Disconnecting 48V Power Supplies from the Console Server .....</i>	29

<b>CHAPTER 2 INSTALLATION .....</b>	<b>31</b>
<i>General installation procedure.....</i>	<b>32</b>
<i>Rack mounting your Perle CS9000.....</i>	<b>33</b>
<i>Desk mounting your Perle CS9000.....</i>	<b>34</b>
<i>Multiple stacking your Perle CS9000.....</i>	<b>35</b>
<i>LED guide.....</i>	<b>36</b>
<i>Selecting AUI or 10/100 Base T interface.....</i>	<b>38</b>
<i>Setting up an IP address.....</i>	<b>39</b>
<i>Setting up an IP address automatically using DHCP .....</i>	<b>39</b>
<i>Set up procedure.....</i>	<b>39</b>
<i>About DHCP .....</i>	<b>41</b>
<i>Manually setting up an IP address .....</i>	<b>43</b>
<i>Set up procedure.....</i>	<b>44</b>
<i>Server form field descriptions.....</i>	<b>46</b>
<i>Accessing the Perle CS9000 configuration software .....</i>	<b>50</b>
<i>Logging onto your Perle CS9000 .....</i>	<b>50</b>
<i>Setting up your network parameters.....</i>	<b>51</b>
<i>Setting up the host table.....</i>	<b>51</b>
<i>Adding a Host.....</i>	<b>51</b>
<i>Changing a Host .....</i>	<b>52</b>
<i>Deleting a host .....</i>	<b>53</b>
<i>Changing the Admin Password .....</i>	<b>54</b>
<i>RADIUS configuration .....</i>	<b>55</b>
<i>Set up procedure.....</i>	<b>55</b>
<i>RADIUS parameters description.....</i>	<b>57</b>
<i>DNS configuration.....</i>	<b>59</b>
<i>WINS configuration.....</i>	<b>60</b>
<i>Configuring network gateways.....</i>	<b>61</b>
<i>Adding a gateway.....</i>	<b>62</b>
<i>Deleting a Gateway.....</i>	<b>63</b>
<i>Configuring RIP .....</i>	<b>64</b>
<i>Verifying your network installation .....</i>	<b>65</b>
<i>Saving configuration changes.....</i>	<b>66</b>
<i>Saving to non-volatile memory.....</i>	<b>66</b>
<i>Saving to a file .....</i>	<b>66</b>
<i>Setting date and time .....</i>	<b>67</b>
<i>Performing a soft reboot.....</i>	<b>68</b>
<i>Restoring factory default settings .....</i>	<b>69</b>
<i>Resetting to factory defaults using software .....</i>	<b>69</b>

<b>CHAPTER 3 SYSTEM ADMINISTRATION .....</b>	<b>71</b>
<b>Security.....</b>	<b>72</b>
<b>Setting up the line on your Perle CS9000.....</b>	<b>72</b>
<b>Viewing and editing your line settings.....</b>	<b>73</b>
<i>Lines set to reverse Telnet by default.....</i>	<i>73</i>
<b>Lost password.....</b>	<b>74</b>
<b>Configuring a dial in line .....</b>	<b>75</b>
<i>Introduction to SLIP and PPP connections.....</i>	<i>75</i>
<i>Deciding whether to use SLIP or PPP .....</i>	<i>75</i>
<i>Setting up the line .....</i>	<i>76</i>
<i>Configuring SLIP.....</i>	<i>79</i>
<i>Configuring PPP .....</i>	<i>81</i>
<i>PPP configuration procedure .....</i>	<i>81</i>
<i>PPP form field descriptions.....</i>	<i>82</i>
<i>Configuring a modem.....</i>	<i>90</i>
<b>Configuring users.....</b>	<b>91</b>
<i>About user accounts and RADIUS.....</i>	<i>92</i>
<i>Overview .....</i>	<i>92</i>
<i>Example RADIUS user file: telnet service .....</i>	<i>94</i>
<i>Adding a user account .....</i>	<i>95</i>
<i>Configuring a user account.....</i>	<i>96</i>
<i>Configuration procedure.....</i>	<i>96</i>
<i>User form field descriptions.....</i>	<i>97</i>
<i>About user levels .....</i>	<i>103</i>
<i>Line Access Rights.....</i>	<i>103</i>
<i>CLI prompts.....</i>	<i>104</i>
<i>Changing a user's password.....</i>	<i>105</i>
<i>Deleting a user account.....</i>	<i>105</i>
<b>Configuring Break Pass Through.....</b>	<b>106</b>
<b>Setting the CS9000 Time Configuration.....</b>	<b>106</b>
<i>Manually Set the Time.....</i>	<i>106</i>
<i>Time Setup through SNTP .....</i>	<i>107</i>
<i>Setting Time Zones .....</i>	<i>108</i>
<i>Setting Time for Daylight Savings Time.....</i>	<i>109</i>
<b>Resetting the line to default.....</b>	<b>111</b>
<b>Saving your settings.....</b>	<b>112</b>
<i>Saving settings to non-volatile memory.....</i>	<i>112</i>
<i>Saving settings to a file.....</i>	<i>112</i>

<b>CHAPTER 4 USING CS9000 AS A CONSOLE SERVER .....</b>	<b>113</b>
<b>Introduction.....</b>	<b>114</b>
<b>Accessing devices via Telnet from the LAN.....</b>	<b>115</b>
Information required.....	115
Direct Access procedure .....	115
Easy Port Access Procedure.....	116
<b>Accessing devices via SSH.....</b>	<b>117</b>
SSH Setup Procedure.....	117
Information required.....	119
Direct Access procedure .....	119
Easy Port Access procedure .....	120
<b>Accessing devices with Multisession.....</b>	<b>122</b>
<b>Accessing devices via modems using PPP.....</b>	<b>125</b>
<b>Accessing devices via modems using a dumb device.....</b>	<b>126</b>
<b>Accessing Local Port Buffers.....</b>	<b>127</b>
Setup .....	127
Access Port Buffers.....	128
<b>Accessing Remote Port Buffers .....</b>	<b>130</b>
Setup .....	130
<b>APPENDIX A CABLING INFORMATION .....</b>	<b>133</b>
<b>RJ45 RS232 serial ports.....</b>	<b>134</b>
<b>AUI port .....</b>	<b>135</b>
<b>RJ45 10/100BaseT port .....</b>	<b>136</b>
<b>Admin Port.....</b>	<b>137</b>
<b>Third party connection examples.....</b>	<b>138</b>
CS9000 to Sun Microsystem servers.....	139
CS9000 RJ45 to DB9 IBM RS6000 com port .....	139
CS9000 RJ45 to DB25 Sun server .....	139
CS9000 RJ45 to Sun server port DB9.....	139
CS9000 RJ45 to Sun server Netra port RJ45.....	140
CS9000 RJ45 to Perle router DB25 console port .....	141
CS9000 RJ45 to Perle router RJ45 console port.....	141
CS9000 RJ45 to Cisco RJ45 cable with hardware flow control.....	141
CS9000 RJ45 to Nortel switch DB25 cable.....	142
<b>Connecting to PC serial ports .....</b>	<b>143</b>
CS9000 RJ45 to DB9 PC Com port configuration.....	143
CS9000 25-pin Admin port to a PC.....	143

<b>Connecting to Terminals.....</b>	<b>144</b>
CS9000 RJ45 to DB25 terminal with hardware flow control.....	145
CS9000 RJ45 to DB25 terminal using the modem device .....	145
Flow control disabled.....	145
Hardware flow control enabled.....	145
CS9000 to Terminals - slow speed or using software flow control.....	146
CS9000 25-pin Admin port to a terminal .....	147
<b>Connecting to Modems.....</b>	<b>148</b>
CS9000 RJ45 to DB25 modem cable configuration.....	148
CS9000 RJ45 to DB9 modem cable configuration.....	148
<b>Loopback cable on CS9000 RJ45 serial port.....</b>	<b>149</b>
<b>APPENDIX B THE CLI COMMANDS .....</b>	<b>151</b>
<b>CLI commands.....</b>	<b>152</b>
add community.....	152
add DNS.....	152
add gateway.....	153
add host.....	153
add modem.....	154
add radius .....	154
add rip md5.....	155
add trap.....	155
add snmp server.....	155
add user .....	156
add WINS.....	156
admin .....	156
debug .....	156
delete ARP .....	157
delete community .....	157
delete DNS.....	157
delete gateway .....	157
delete host .....	158
delete modem .....	158
delete radius .....	158
delete rip md5.....	159
delete snmp server_1 .....	159
delete trap.....	159
delete user.....	159
delete WINS .....	160

<i>heap</i> .....	160
<i>help</i> .....	160
<i>kill line</i> .....	160
<i>logout</i> .....	161
<i>netload</i> .....	162
<i>netsave</i> .....	163
<i>ping</i> .....	164
<i>reboot</i> .....	165
<i>reset factory</i> .....	165
<i>reset line</i> .....	165
<i>reset user</i> .....	166
<i>restart</i> .....	166
<i>resume</i> .....	166
<i>rlogin</i> .....	167
<i>save</i> .....	167
<i>screen</i> .....	167
<i>set contact</i> .....	168
<i>set date</i> .....	168
<i>set ethernet interface RJ45</i> .....	168
<i>set ethernet interface AUI</i> .....	169
<i>set gateway</i> .....	169
<i>set host</i> .....	169
<i>set line</i> .....	170
<i>set location</i> .....	172
<i>set port_buffering</i> .....	173
<i>set ppp line</i> .....	174
<i>set radius</i> .....	175
<i>set rip</i> .....	175
<i>set server</i> .....	176
<i>set slip line</i> .....	183
<i>set sntp mode</i> .....	183
<i>set summertime mode</i> .....	184
<i>set telnet</i> .....	185
<i>set time</i> .....	186
<i>set timezone offset</i> .....	186
<i>set user</i> .....	187
<i>show ARP</i> .....	189
<i>show date</i> .....	190
<i>show gateways</i> .....	190

<i>show hardware</i> .....	190
<i>show hosts</i> .....	191
<i>show interface</i> .....	191
<i>show line</i> .....	191
<i>show line users</i> .....	193
<i>show modems</i> .....	193
<i>show port_buffering</i> .....	194
<i>show ppp line</i> .....	194
<i>show radius</i> .....	196
<i>show rip</i> .....	196
<i>show rip peers</i> .....	197
<i>show routes</i> .....	197
<i>show server</i> .....	198
<i>show slip line</i> .....	199
<i>show snmp</i> .....	200
<i>show sntp</i> .....	200
<i>show sntp_info</i> .....	201
<i>show summertime</i> .....	202
<i>show telnet</i> .....	202
<i>show time</i> .....	203
<i>show timezone</i> .....	203
<i>show user</i> .....	204
<i>start</i> .....	204
<i>telnet</i> .....	205
<i>version</i> .....	205
<b>APPENDIX C SNMP</b> .....	<b>207</b>
<b>Overview</b> .....	<b>208</b>
<b>Configuring SNMP support</b> .....	<b>209</b>
<b>Network management</b> .....	<b>210</b>
<b>APPENDIX D UPGRADING YOUR FIRMWARE</b> .....	<b>213</b>
<b>Introduction</b> .....	<b>214</b>
<b>Saving your existing Configuration</b> .....	<b>215</b>
<i>Example of saving a configuration file</i> .....	215
<i>Using TFTP from a host</i> .....	215
<i>TFTP configuration</i> .....	216
<i>Writing to FLASH memory</i> .....	217
<b>Using BOOTP from a boothost</b> .....	<b>218</b>

<i>Upgrade using JETset, the web browser interface.....</i>	<i>219</i>
<i>Enabling BOOTP/DHCP after upgrading software.....</i>	<i>219</i>
<i>Disable BOOTP/DHCP.....</i>	<i>219</i>
<b>APPENDIX E SUMMARY OF LINE SERVICE TYPES .....</b>	<b>221</b>
<i>List of line service types.....</i>	<i>222</i>
<b>APPENDIX F BOOTP .....</b>	<b>225</b>
<i>Introduction.....</i>	<i>226</i>
<i>How BOOTP works .....</i>	<i>227</i>
<i>How to setup BOOTP.....</i>	<i>229</i>
<i>The bootptab file entry.....</i>	<i>229</i>
<i>The bootfile .....</i>	<i>231</i>
<i>BOOTP messages output to screen.....</i>	<i>233</i>
<i>Disabling the BOOTP reply.....</i>	<i>233</i>
<i>Booting multiple units.....</i>	<i>234</i>
<i>Multiple BOOTP servers.....</i>	<i>235</i>
<i>Example of BOOTP.....</i>	<i>235</i>
<b>APPENDIX G JETSET .....</b>	<b>237</b>
<i>Introduction to JETset.....</i>	<i>238</i>
<i>Using JETset.....</i>	<i>240</i>
<i>JETset program summary.....</i>	<i>243</i>
<b>APPENDIX H RADIUS ATTRIBUTES .....</b>	<b>245</b>
<i>Access Request Messages .....</i>	<i>246</i>
<i>Access-Accept Message.....</i>	<i>247</i>
<i>Accounting Message .....</i>	<i>249</i>
<i>Perle Specific RADIUS Attributes .....</i>	<i>251</i>

<b>APPENDIX I TROUBLESHOOTING .....</b>	<b>257</b>
<b>Introduction.....</b>	<b>258</b>
<b>General communication matters.....</b>	<b>258</b>
<b>Host problems.....</b>	<b>259</b>
<b>JETset problems.....</b>	<b>260</b>
<b>Login problems .....</b>	<b>261</b>
<b>Problems with terminals .....</b>	<b>262</b>
<b>Emergency recovery.....</b>	<b>263</b>
<b>Problems with framed Routing.....</b>	<b>263</b>
<b>APPENDIX J CONTACTING PERLE .....</b>	<b>265</b>
<b>Making a technical support query .....</b>	<b>266</b>
Who to contact.....	266
Information needed when making a query .....	267
Making a support query via the Perle web page.....	268
<b>Repair procedure .....</b>	<b>269</b>
<b>Perle support centres worldwide.....</b>	<b>270</b>
<b>INDEX.....</b>	<b>271</b>

# Chapter 1 Introduction

*You need to read* You need to read this chapter if you want an overview of the Perle CS9000 product.

*this chapter if you want to...* This chapter provides introductory information about the Perle CS9000, its associated components, software and configuration utilities.

This chapter includes the following sections

- [About the Perle CS9000 on page 22](#)
- [Typical applications summary on page 24](#)
- [Perle CS9000 front and rear views on page 26.](#)

For details of installation procedures, see [Chapter 2 Installation](#).

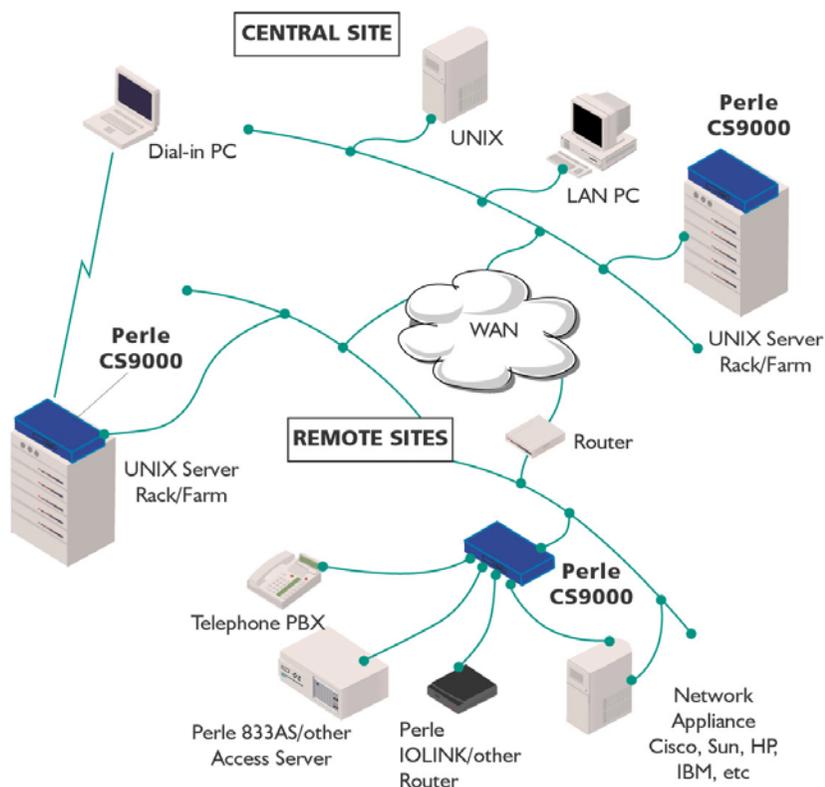
For information about performing system administration tasks with your Perle CS9000, see [Chapter 3 System administration](#).

For information on using your Perle CS9000 as a console server, see [Chapter 4 Using CS9000 as a console server](#).

## About the Perle CS9000

The Perle CS9000 is a console server which allows you to communicate directly via the serial port to networked devices (such as routers, servers and so on) in order to perform system administration tasks.

The Perle CS9000 allows system administrators to diagnose and fix from anywhere on the LAN/WAN or via a modem thus saving on administrator's time and costs to keep system disruption to a minimum.



Typically, you use the Perle CS9000 when a server or network device fails at a remote site or if you want to perform administration tasks from home. Using a Perle CS9000 you can access the unit over the LAN/WAN or via dial-in.

The Perle CS9000 is available in the following variants;

- 9008 with 8 serial ports
- 9016 with 16 serial ports
- 9024 with 24 serial ports
- 9032 with 32 serial ports
- 9048 with 48 serial ports

See also [Typical applications summary on page 24](#) and [Perle CS9000 front and rear views on page 26](#).

# Typical applications summary

## Managing the CS9000 Unit

The Perle CS9000 unit can be managed and configured by administrators through various methods allowing them full configuration capabilities and easy access to management statistics and tools. Administrators can access the CS9000 unit using the following methods

- Direct connection through the administrator port using a Serial Terminal or Terminal Emulation Software
- Connection through the ethernet interface using reverse Telnet (Port 23) or reverse SSH (Port 22).
- Connection through a serial port on the CS9000 configured for CSLogin using a Serial Terminal or Terminal Emulation Software
- Connection through a serial port configured for PPP/SLIP allowing for remote access (Telnet session) through a modem.
- On a 32 and 48 port version of the CS9000, each row must be separately managed. The ports (serial, ethernet and admin) identified in row A are independent of the ports in row B.

## Managing/Accessing devices attached to the CS9000

The Perle CS9000 can be configured to allow users or administrators to view or manage specific devices on the CS9000's serial ports across the Ethernet interface using two different methods.

- Direct Connect - users can directly connect to the devices on the CS9000 serial port by reverse Telnet or reverse SSH using the configured IP Address of the CS9000 and the device's assigned TCP port number.
- Easy Port Access - users can connect to the CS9000 unit using the configured CS9000's IP Address by reverse Telnet (port number 23) or reverse SSH (port number 22) and be provided with a device menu displaying the names of all the devices which that user has access to. This feature eliminates the need for administrators and users to recall the specific port number associated with a certain device on the CS9000. The user can simply connect to a specific device based upon the name of the device and then return to the device menu without disconnecting its initial reverse Telnet or reverse SSH connection.

## Network security

Perle CS9000 provides a comprehensive suite of security features to allow an organization to implement robust security planning to prevent unauthorized access. These include SLIP and PPP Remote User dial-in and support for RADIUS.

For a secure LAN connection, the Perle CS9000 supports SSH version 1 and version 2 protocol. Remote server connections with SSH protocol uses an encrypted data channel with support for password and other authentications.

## Management and diagnostics

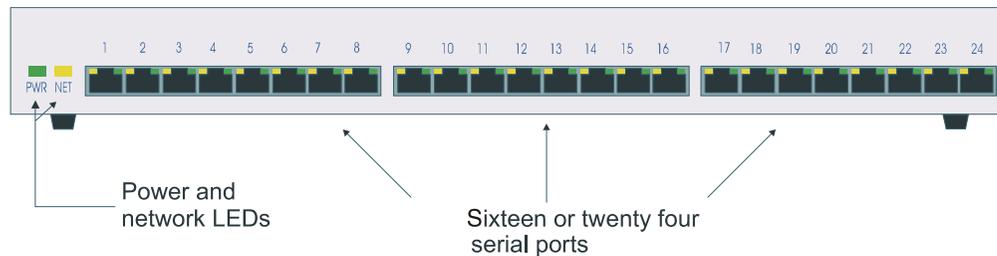
Independent tests have proved that the CS9000 extremely easy to configure and install. A comprehensive array of software tools allows the Perle CS9000 to be configured, managed and upgraded either locally or remotely over the network and even via the Internet.

These tools include JETset, for complete port management from any location via a Web browser, and easy downloads of software upgrades to the unit's flash memory. Command line and menu interfaces are included, as is a separate local management port, plus industry standard control and management facilities - SNMP, BOOTP, DHCP and DNS.

## Perle CS9000 front and rear views

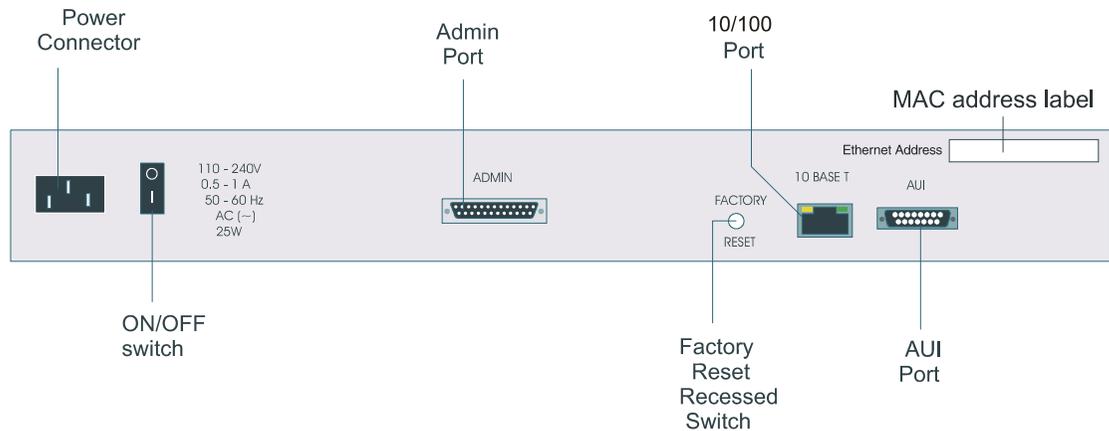
The Perle CS9000 is a network access server with front-mounted RJ45 serial ports. It is designed for use in a rack. The serial ports are RS232. The product has 10/100BaseT network connections and an Administration port for system management. The next picture shows the front view of a 24 port unit.

*Perle CS9000  
front view*



You can mount the Perle CS9000 in a 19 inch rack, on a wall or on a desk.

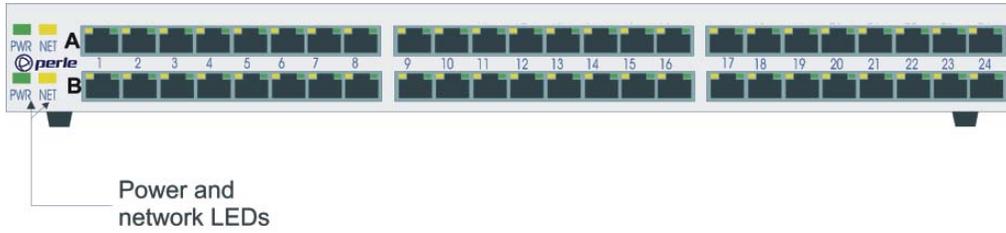
*Perle CS9000  
rear panel*



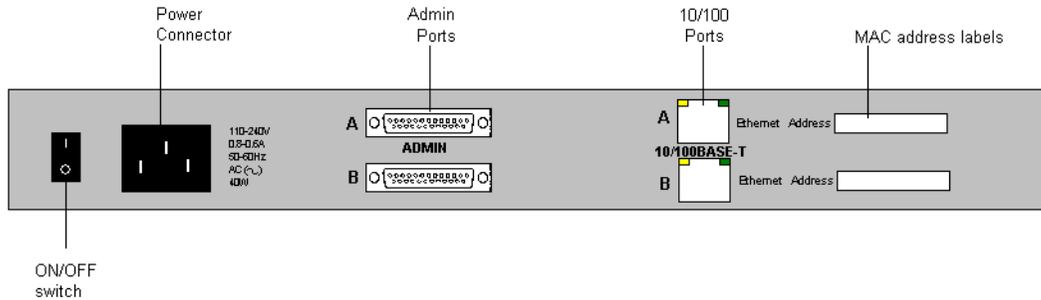
The 32 and 48 port versions of the CS9000 have ports (serial, ethernet and admin) identified as row A which are unique and separate of the ports in row B. Each row must be configured separately and have its own unique configuration.

See the figures below for the front and rear view of a 48 port version

CS9000 48 port  
front view



CS9000 48 port  
rear view

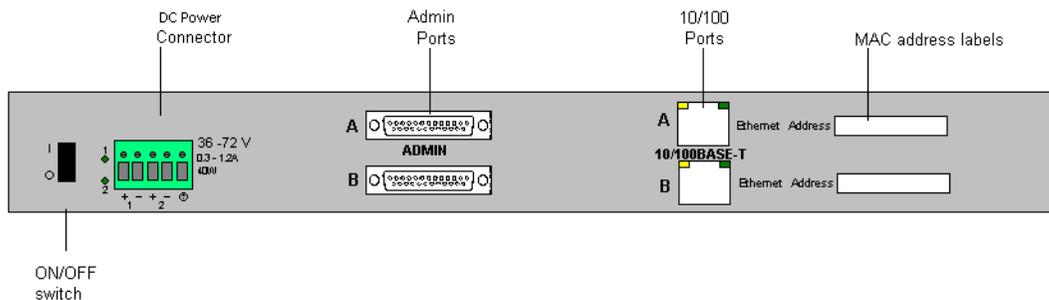


## CS9000 48V Model

The CS9000's unique dual feed DC capability, provides power redundancy. In the event of a DC Power failure or if the voltage level falls below a threshold level, the CS9000 will automatically switch its source of DC power from the primary to secondary DC source increasing its availability to manage mission critical equipment. The CS9000 supports the accepted Telcoms "battery float" range of 36V to 72V DC so that it may fit into the various worldwide DC environments that exist.

The CS9000 will automatically switch to the alternate DC source and remain on-line providing important access to network equipment.

CS9000 48V DC  
Dual Input Model



## Electrical Supply Details

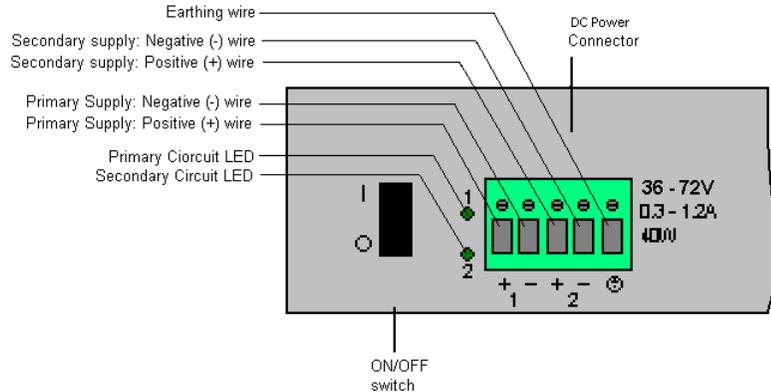
The Console Server is supplied with an integral Terminal Connections block to facilitate connection to a DC source(s). The DC supply(s) should have adequate over-current protection within the closed rack system and comply with local or national standards applicable to the installation territory.

**WARNING:** The equipment must be grounded for safety and to ensure ESD protection for correct operation and protection of the internal circuitry.

## Connecting DC Power Supply(s) to Console Server

For connecting the DC supply(s) to the Console Server should be performed in the following sequence:

1. Switch off the Power Supplies and the Console Server
2. Connect the attached devices to the serial ports
3. Connect the primary and secondary DC input using the following specifications:
  - a) Use wire gauge 20 to 22 AWG
  - b) Strip insulation 7mm from wire ends. (If using stranded wire, twist all strands together to ensure all wire strands are used for the connection.
  - c) Connect supply with reference to the terminal block diagram and electrical specifications:



*Note.* When connecting only a single power supply source ensure the connection is the primary supply and the secondary terminals are left unconnected.

### Primary Supply:

Positive (+) wire to Circuit 1, terminal marked +  
Negative (-) wire to Circuit 1, terminal marked -

### Secondary (back-up) Supply:

Positive (+) wire to Circuit 2, terminal marked +

Negative (-) wire to Circuit 2, terminal marked -

**Note.** *When connecting dual power supply sources, the CS9000 supports a common positive (+) circuit arrangement ONLY.*

#### **Earthing Wire**

Ground wire to terminal marked with circular earthing symbol

#### **Screws**

Tighten terminal connector block screws to 7 lbs-inches torque.

4. Switch on the power supplies.
5. Switch on the Console Server (The power LEDs 1 and 2 will indicate the status of the power source at the respective input. If both the primary and secondary power source are available both LED 1 and LED 2 next to the terminal block will be luminated indicated power detected from each input.)

## **Disconnecting 48V Power Supplies from the Console Server**

To disconnect the power supply(s) from the Console Server, please follow these instructions:

1. Switch off the Console Server
2. Switch off the power source(s).
3. Disconnect all DC power input cables from the Console Server terminal connector block.
4. Remove any attached devices to the serial or ethernet port(s).

Your console server is ready to be moved.



# Chapter 2 Installation

*You need to read this chapter if you want to install the Perle CS9000.*

*this chapter if you want to...* This chapter provides task oriented information about installing the Perle CS9000, its associated components, software and configuration utilities.

This chapter includes the following sections;

- [General installation procedure on page 32](#)
- [Rack mounting your Perle CS9000 on page 33](#)
- [Desk mounting your Perle CS9000 on page 34](#)
- [Multiple stacking your Perle CS9000 on page 35](#)
- [LED guide on page 36](#)
- [Selecting AUI or 10/100 Base T interface on page 38](#)
- [Setting up an IP address on page 39](#)
- [Setting up your network parameters on page 51](#)
- [Saving configuration changes on page 66](#)
- [Setting date and time on page 67](#)
- [Performing a soft reboot on page 68](#)
- [Restoring factory default settings on page 69.](#)

## General installation procedure

The general procedure for installing and setting up your Perle CS9000 is as follows;

1. Install your Perle CS9000 in a rack or on a desktop as required using the procedures described in [Rack mounting your Perle CS9000 on page 33](#) and [Desk mounting your Perle CS9000 on page 34](#).

**Note** *If you are stacking multiple units on a desktop see [Multiple stacking your Perle CS9000 on page 35](#) for the maximum advisable units to stack.*

2. Connect your Perle CS9000 to the network. See [Appendix A Cabling information](#).
3. If required, select the interface type you want. See [Selecting AUI or 10/100 Base T interface on page 38](#).
4. Set up your IP address using the procedures given in [Setting up an IP address on page 39](#).
5. Access the Perle CS9000 configuration software using the procedures given in [on page 46](#)
6. Set up your network parameters using the procedure given in [Setting up your network parameters on page 51](#).

You can now use the unit. For information on using the Perle CS9000 for system administration purposes. See [Chapter 3 System administration](#) for further details.

For information on using your Perle CS9000 as a console server, see [Chapter 4 Using CS9000 as a console server](#).

# Rack mounting your Perle CS9000

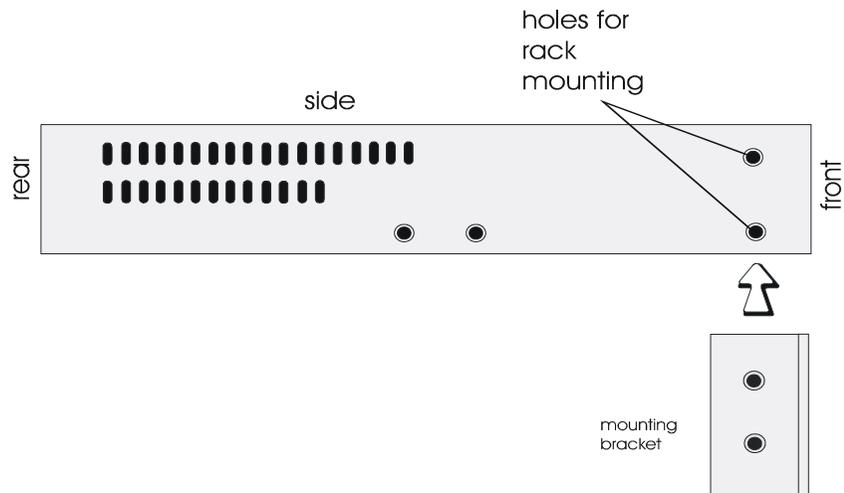
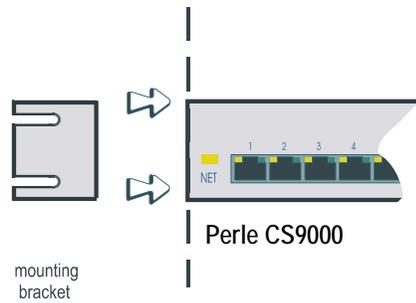
To mount a single Perle CS9000 into a 19 inch rack, use the two mounting brackets and four screws provided with the unit.

**Caution**

*When mounting several Perle CS9000 units in a 19" rack, you must not stack more than 3 units without leaving an air gap between them.*

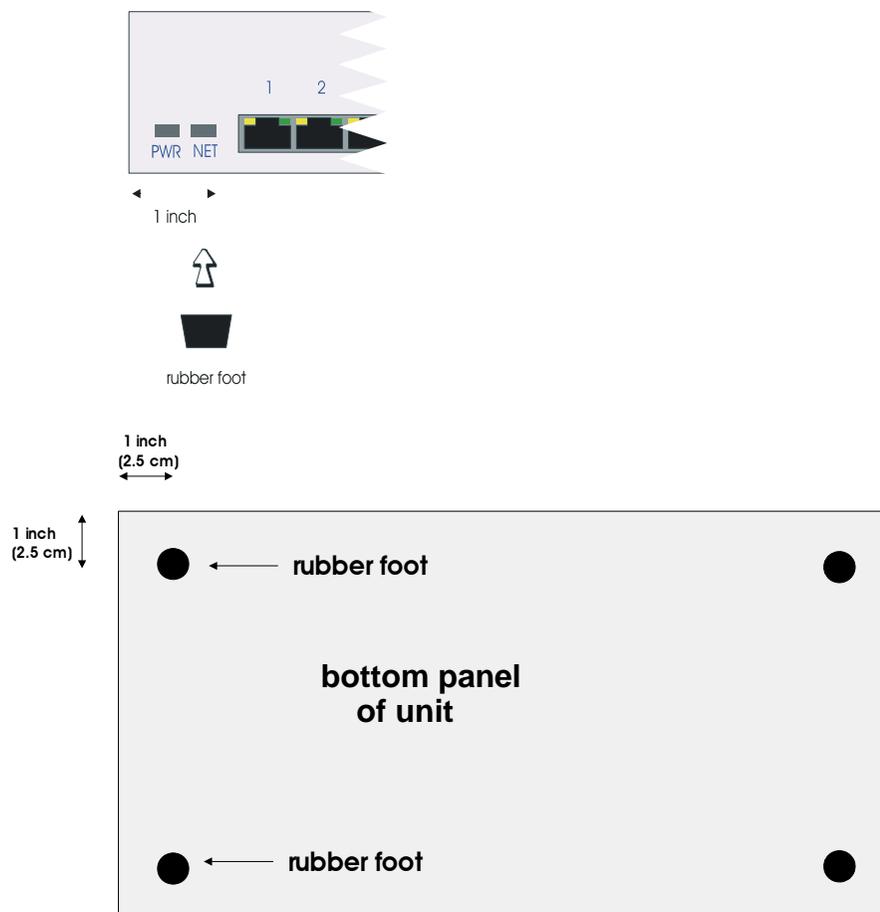
**Caution**

*Observe maximum ambient operating temperatures within a rack; you may have to use forced air cooling.*



## Desk mounting your Perle CS9000

To prepare the Perle CS9000 for use on a desk use the four self-adhesive rubber feet provided with the unit. Stick the four feet to the underside of the unit, one in each corner, approximately one inch from each adjacent edge.



## Multiple stacking your Perle CS9000

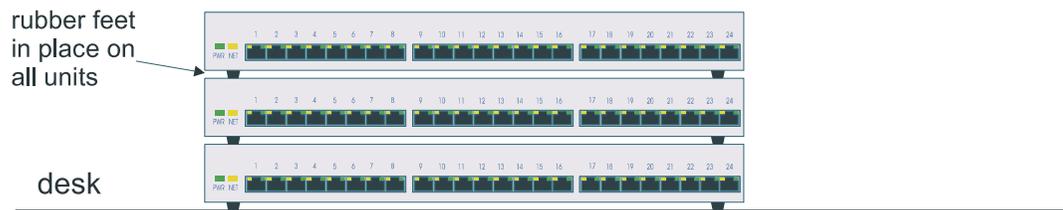
When stacking your unit on a desk we recommend that you stack no more than three units high in a 0 to 40 degrees centigrade environment. This precaution ensures that you keep within the maximum operating temperatures of the units.

---

**Caution**

---

*When desk mounting multiple Perle CS9000 units, make sure you fit the rubber feet to all units before stacking to assist ventilation.*



---

**Caution**

---

*When mounting several Perle CS9000 units in a 19" rack, you must not stack more than 3 units without leaving an air gap between them.*

---

**Caution**

---

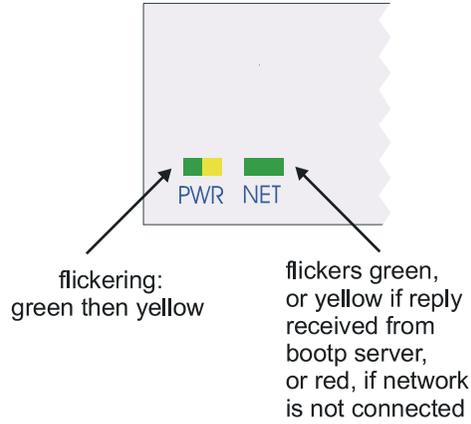
*Observe maximum ambient operating temperatures within a rack; you may have to use forced air cooling.*

# LED guide

During bootup you should see power and network LEDs display the following colours.

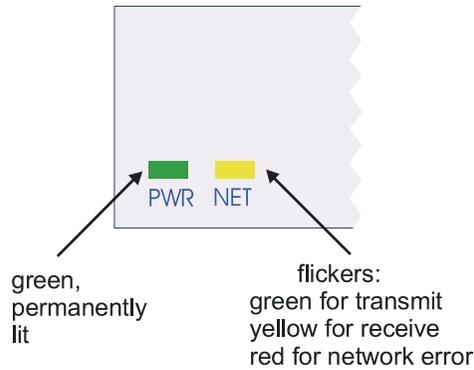
*Power and network LEDs*

Perle CS9000 during bootup

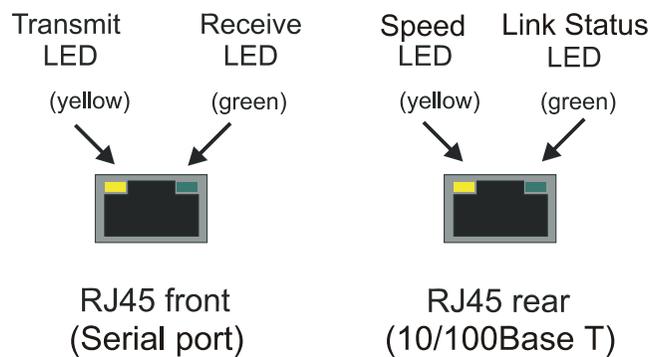


Once power is on and the network is connected, the power and network LEDs will display the following colours:

Perle CS9000  
during normal operations



*RJ45 LEDs* There are bi-colour LEDs on the RJ45 connectors on both the front and rear panels. These LEDs flicker briefly during bootup and then display the following colours,



## Selecting AUI or 10/100 Base T interface

The CS9000 with Blue case, allows you to specify the type of interface you want to use from either AUI or 10/100Base-T (Default setting is 10/100Base-T). To do this proceed as follows;

*Note* To display the currently selected interface type, at the command prompt, type **show hardware** and press the **Enter** key. The resulting display will include the currently selected hardware type. You only need to use these commands on revision 2 Perle CS9000 boards.

1. Login to your unit and display the command prompt.
2. At the command prompt, type one of the commands listed in the next table to select the interface type you want to use.

To set this type of interface	Use this command
10/100Base-T	<code>set ethernet interface RJ45</code>
AUI	<code>set ethernet interface AUI</code>

You can now perform the initial configuration of the unit.

NOTE: There is no AUI feature CS9000 with the black case and defaults automatically to use RJ45 ethernet interface.

# Setting up an IP address

## Setting up an IP address automatically using DHCP

This section includes the following;

- [Set up procedure on page 39](#)
- [About DHCP on page 41](#)

**Note** When configuring a 32 or 48 port version of the CS9000 you must ensure that each row has a unique IP address

### Set up procedure

To set up an IP address automatically using DHCP proceed as follows;

**Note** For details of the BOOTP/DHCP tags (client information items) that are supported by both BOOTP and DHCP see [Appendix F BOOTP](#). In addition on Microsoft Windows NT, DHCP allows for the configuration of WINS server names.

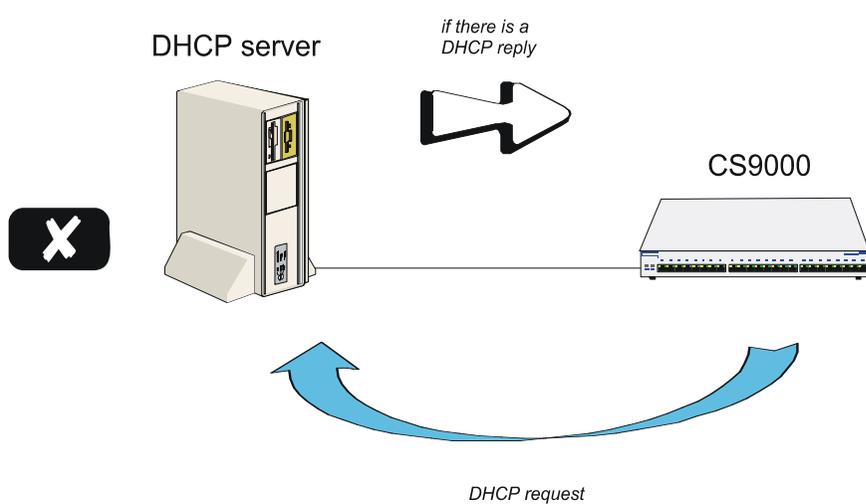
If automatic configuration of Perle CS9000 clients is required, only one service DHCP, BOOTP or RARP should be enabled on your network server.

We strongly recommend that you do not run both the BOOTP and DHCP services on the same network to configure Perle CS9000 clients unless you are very familiar with the potential interactions that may result. For information on BOOTP see [Appendix F BOOTP](#).

1. Set up your DHCP server as required.  
See your system documentation for details of configuring the DHCP service on your server's operating system.

either:  
the DHCP server finds a matching ethernet address and sends a reply to the unit

or:  
the DHCP server does not find a matching ethernet address; it does not reply to the unit



2. Connect your Perle CS9000 to the network and turn on the unit.

The IP address and any other configuration information will now be set up automatically. For more information see [About DHCP on page 41](#).

## About DHCP

You can use DHCP to perform the following actions on a single or multiple Perle CS9000 (the 'unit(s)')s on its/their boot-up:

- auto-configure with minimal information; e.g. only an ip address
- auto-configure with basic setup information (ip address, subnet mask, broadcast address, etc.)
- download a new version of software
- download a full configuration profile (saved from another unit)

DHCP is particularly useful for multiple installations: you can do all the unit's configuration in one DHCP file, rather than configure each unit manually.

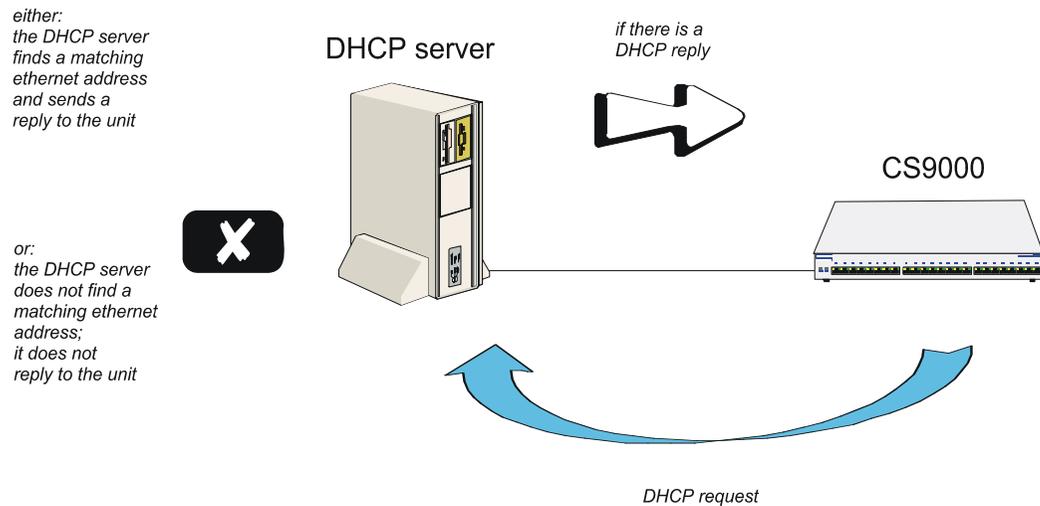
Another advantage of DHCP is that you can connect a unit to the network, turn on its power and let auto-configuration take place. All the configuration is carried out for you during the DHCP process.

The the unit's implementation of DHCP is compatible with RFC 951.

On bootup or power-up, the unit will send a broadcast request to the DHCP server(s) on the network. The request contains the ethernet address of the unit; it asks for network configuration details (internet address, subnet mask, etc.). This process is shown in [DHCP request and response on page 41](#).

You can stop the DHCP server from replying to the unit; see [Appendix F BOOTP](#)

### *DHCP request and response*



The DHCP server checks the ethernet address and looks for a matching address in its DHCP tables:

- if a matching ethernet address is found the DHCP server will reply to the unit; the reply will contain network configuration information. This information is listed in the DHCP tables for that particular unit (identified by its hardware address). The unit then boots using the information sent to it.
- if no matching ethernet address is found the DHCP server does not reply; the unit boots from internal memory.

Refer to [DHCP request and response on page 41](#) for an explanation of the following text:

the DHCP response contains network configuration information; e.g. ip address, subnet mask, broadcast address. It may also contain details of a bootfile (not mandatory)

a bootfile (if you specify one) contains a unit's specific boot information; e.g. authentication method of users, access permission for the GUI. It may also contain details of other files (not mandatory); e.g. software version, language files and a general configuration file

a configuration file (if you specify one) contains general configuration parameters; these parameters will have been created from another unit and saved to a file

in the DHCP response the minimum parameters to specify are **:ht** and **:ha**

there is no minimum number of parameters to specify in the bootfile or configuration file; unspecified parameters will remain unchanged in the unit's memory

After processing the DHCP response the unit will download additional files, as follows:

if a bootfile is specified, the unit will then download that bootfile (using tftp).

if the bootfile specifies other files e.g. a software file, the unit will compare that filename with the filename in its memory; if it has changed the unit will then download that other file using tftp. If the filename has not changed the unit will not download it.

The DHCP protocol provides an industry standard alternative to BOOTP and provides a more sophisticated method of managing IP addresses and configuration parameters. It should be particularly useful when managing the unit from a Windows NT server environment and some versions of UNIX such as UnixWare 7.

DHCP is a superset of the BOOTP configuration service which it completely replaces. DHCP is backward compatible with BOOTP in that the entire suite of BOOTP tags is supported within DHCP. DHCP is now often used in favour of BOOTP as it is supported on a wide range of network operating systems, however to ensure compatibility with existing installations, the Perle CS9000 will continue to fully support BOOTP.

The major differences between BOOTP and DHCP are:

- BOOTP is largely reliant on a network client's low level Ethernet address (MAC address) for client information look-up, DHCP has no such limitation, although it is still possible to associate a specific IP address to a specific MAC address.
- Client information supplied by DHCP is supplied on a lease basis, that is to say that the client negotiates with the server for the lease of an IP address for a specific period of time. This allows for the allocation of a fixed pool of client addresses that are allocated by the DHCP server on a "first come first served" basis.

No additional configuration is required in the unit to enable DHCP, however your network server will need to have its DHCP service configured for Perle CS9000 clients and if boot file download is required, then the TFTP service should be configured and running. DHCP/BOOTP can also be disabled completely by setting the configurable server DHCP parameter to off.

## Manually setting up an IP address

This section includes the following;

- [Set up procedure on page 44](#)
- [Server form field descriptions on page 46.](#)

## Set up procedure

To manually set up an IP address proceed as follows;

1. Set up a terminal or PC running terminal emulation. For examples of connection pinouts see [Appendix A Cabling information](#).

If you connect via the Admin Port you will see a display of diagnostic and bootup messages.

Note that if you cannot emulate VT100, you will have to use the Command Line Interface (cli); (*the cli commands are described in full in [Appendix B The CLI commands](#)*).

2. At the console, with the login prompt displayed, type *admin* and press <return>.
3. At the password prompt, now displayed type *superuser* and press <return>. This is the default admin user password.

The command line prompt will now be displayed:

4. At the command prompt type *screen* and press **Enter** to enter Full Screen mode.

The main menu is now displayed:

```

-----main menu-----
sessions
users
line configuration
server configuration
port buffering configuration
radius configuration
network configuration
time configuration
hardware
command line mode
  
```

5. At the main menu, select **server configuration**. (alternatively, use the cli command `set server`)

The server form will be displayed as shown in the next picture:

```

-----server-----
servername[CS9000 ]
domain name[ ]
internet address[172.16.33.220 ]
subnet mask[255.255.0.0 ]
broadcast address[172.16.255.255 ]
authentication[local ]
ssh protocol[both(ssh-1+ssh-2)]
ssh break string[~break ]
line menu string[~menu ]
session escape string[<026>s ]
reverse session limit[24]
dhcp[off]
gui access[on ]
services[fffe]
break[off]
banner[off]
prompt with name[off]
OEM_mode[ ]
  
```

6. Within the server form, complete the fields by moving between the fields using the arrow keys. Use the <del> key to backspace if necessary.

For a description of the fields in this form see [Server form field descriptions on page 46](#).

Example settings for all the Perle CS9000 configuration fields are shown in the next picture:

```

server
-----
servername[CS9000 ]
domain name[ ]
internet address[172.16.33.220 ]
subnet mask[255.255.0.0 ]
broadcast address[172.16.255.255 ]
authentication[local ]
ssh protocol[both(ssh-1+ssh-2)]
ssh break string[~break ]
line menu string[~menu ]
session escape string[<026>s ]
reverse session limit[24]

dhcp[off]
gui access[on ]
services[fffe]
break[off]
banner[off]
prompt with name[off]
OEM_mode[ ]

```

- When you have completed the form, press <return>.

You will be presented with the following display:

```

server
-----
servername[CS9000 ]
domain name[ ]
internet address[172.16.33.220 ]
subnet mask[255.255.0.0 ]
broadcast add[ ]
authentication[local ]
ssh prot[ ]
ssh break string[~break ]
line menu string[~menu ]
session escape string[<026>s ]
reverse session limit[24]

options
-----
accept and exit form

dhcp[off]
gui access[on ]
services[fffe]
break[off]
banner[off]
prompt with name[off]
OEM_mode[ ]

```

- Accept the form; you will be returned to the Main Menu.

You may want to save your configuration changes permanently; see [Saving configuration changes on page 66](#)

- Reboot the unit. Rebooting will ensure that other network devices can communicate with it.

**Note** *If you set the port to authenticate by RADIUS only, users will not be able to dial in and connect if the network connection is down (no access to RADIUS server).*

**Tip** *If you are not using the RADIUS service, you can leave authentication set to 'both'. You will have entered users in the Perle CS9000's user table. The unit will authenticate users via its own user table and, provided user names and passwords are valid, should not need recourse to a RADIUS host.*

## Server form field descriptions

The server form fields are described in the next table. You can use this information to assist with setting values in [Set up procedure on page 44](#).

Parameter	Description
<b>servername</b> (also known as hostname or alias)	The familiar name for your Perle CS9000.
<b>Internet Address (IP Address)</b>	The Perle CS9000's unique address in the network.
<b>Broadcast Address</b>	The address used by the Perle CS9000 for sending information to all hosts on your network simultaneously. Once you have entered an IP address and subnet mask, the broadcast address will default to the IP address with the host part(s) set to 255.
<b>Subnet Mask</b>	Allows interconnected local networks to coexist with the same network ID. This hides complicated local environment and routing information from external hosts and gateways. If you want the Perle CS9000 to belong to the same subnet as other hosts, give it the same subnet mask as them. We recommend you set a subnet mask on initial configuration
<b>Domain Name</b>	Unique name which describes your domain - your location in the global network. Like Hostname, it is a symbolic rather than a numerical identifier.
<b>Authentication</b>	You can authenticate all users connecting to the Perle CS9000 in one of four ways:

Parameter	Description
	<p><b>both (local+RADIUS)</b>- (default) The user is authenticated firstly with the CS9000's own local user database. If the username is found in unit but the password is incorrect, an authentication request is sent to the RADIUS host. If the username is not found in the unit, authentication is passed up to the RADIUS host. (The exception is the 'admin' user; if you supply an incorrect password, the unit will not go to the RADIUS host; it will fail the authentication).</p> <p>When the unit uses the RADIUS host, it will try firstly the primary RADIUS host and then - if one is specified - the secondary RADIUS host; (see <a href="#">RADIUS configuration on page 55</a>).</p> <p><b>both (RADIUS+local)</b> - The user is authenticated with the RADIUS host first. If successful the user is authenticated. If the RADIUS host is unattainable or the user is rejected by the RADIUS server , the user is then authenticated using the CS9000 unit's local database.</p> <p><b>local</b> - The user is authenticated with the CS9000's user local database (only)</p> <p><b>RADIUS</b> - The user is authenticated with the RADIUS host's user table (only); does not apply to username 'admin' who is always authenticated locally.</p>
<b>DHCP</b>	<p>You can use the auto configuration method for configuring the CS9000 from a DHCP server. You must turn on this feature by selecting 'on' and disable this feature by selecting 'off'. Default is 'on' or enabled.</p>
<b>SSH protocol</b>	<p>In order to provide a secure connection from the LAN to a device on the CS9000, you must enable the appropriate <b>SSH protocol</b> version. By default, ssh protocol is 'disabled'. To support SSH version 1, select 'ssh-1'. To support SSH version 2 only, select 'ssh-2'. To enable both version of ssh support, select 'both (ssh-1+ssh-2)'. If you are configuring ssh for the first time, you will be prompted to generate the appropriate encryption keys used for negotiating a secure connection. This key generation process could take several minutes. Once generated, the CS9000 will then support the ssh protocol selected.</p>

Parameter	Description
<b>gui access</b>	<p>this parameter controls access to the Perle CS9000's graphical configuration programme JETset.</p> <p>The default is 'off'. When set to 'on' the admin user can access the JETset from a Web browser, using the unit's internet address. Entry to the programme is then controlled by password.</p> <p>If you are not using the JETset to configure the unit, we suggest you set this parameter to 'off'; access will be denied to any person who tries to connect to the unit from their browser.</p> <p>How to access the JETset is described in <a href="#">Appendix G JETset</a>.</p>
services	<p>This command allows the ability to enable/disable specific processes in the CS9000. The services field is a 4 digit hexadecimal number. The number is defined as a bit field, each bit being a different process that is either enabled or disabled. By default, all processes are enabled with the flag set FFFF). This service flag will be saved when configuration is saved to FLASH.</p> <p>See option in <a href="#">set server on page 176</a></p>
ssh break string	<p>The <b>ssh break string</b> can be set up to 8 characters which defines the break string used for inband SSH break signal processing. The default is set to '~break', where ~ is tilde. A break signal is generated on a specific serial port only when the server's break option is enabled and the user currently connected using reverse SSH has typed the break string exactly.</p>
OEM mode	<p>The <b>OEM mode</b> field is a 4 digit hexadecimal number. The number is defined as a bit field, each bit being a different option that is either enabled or disabled</p> <p>See options in <a href="#">set server on page 176</a></p>
break	<p>The <b>break</b> option can be set to either on or off. This option will enable/disable proprietary inband SSH break signal processing as well as the existing Reverse Telnet break signal. The OEM_mode flag 0010 will be set/reset based upon this command. This configuration parameter will be saved when the configuration is saved to FLASH.</p>

Parameter	Description
banner	<p>This parameter concerns the banner information (product name/software version). This banner information is presented to a user with a login prompt. For security reasons you may wish to turn off the display of this information. The choices are ON or OFF. The default is OFF.</p> <p>This parameter does not affect logins using Telnet/Rlogin or the Admin Port; in both these cases the banner information shall always be displayed.</p>
session escape string	<p>The <b>session escape string</b> is a configurable string that allows a user with access to a port to view the multisession screen options allowing the various options while accessing the particular port on the CS9000.</p>
reverse session limit	<p>The <b>reverse session limit</b> defines the number of support simultaneous connections on the CS9000. When decrease the number of supported sessions, the amount of memory allocated for port buffer increases equivalently to all serial ports. The default value for this field is set to the number of ports on the CS9000. The range of value for this field is between 1 and the number of ports.</p>
line menu string	<p>The <b>line menu string</b> field defines the string used to disconnect from the line and return back to the Easy Port Access menu without the disconnecting the initial reverse SSH or reverse Telnet session. The default string is <b>~menu</b>.</p>
prompt with name	<p>The <b>prompt with name</b> option displays the configurable server name instead of default product name and/or version. When enabled the server name will be displayed in the login prompt, CLI prompt, HTML login screens and the heading of the menu screens instead of the default product name CS9000. This option can be set <b>On</b> or <b>Off</b>. The default value is <b>Off</b>.</p>

# Accessing the Perle CS9000 configuration software

## Logging onto your Perle CS9000

1. From your host, telnet to CS9000. For example, telnet 192.65.134.15
2. A login prompt is now displayed.
3. At the console, with the login prompt displayed, type *admin* and press **Enter**. At the password prompt, type *superuser* and press <return>. This is the default admin user password. The command line prompt will be displayed: <product name (abbreviated)> e.g. CS\_9000 or server name if 'prompt with name' is enabled, followed by the hash # sign, indicating that you are now logged in as the system administrator.
4. To enter Full Screen mode (the text-based menus), type *screen* and press **Enter**. The main menu will be displayed:

```
main menu
sessions
users
line configuration
server configuration
radius configuration
network configuration
hardware
command line mode
```

# Setting up your network parameters

## Setting up the host table

The Perle CS9000 needs to know the hostnames and internet addresses of the other hosts in the network (or any hosts anywhere on the Internet) which you want to communicate with on a regular basis. For example, gateways, RADIUS, servers and so on. These hostnames are added to the unit's Host Table. You can add up to twenty hosts. To do this;

1. From the Main menu, select 'Network Configuration'.  
The Network Configuration menu is now displayed.
2. Within the Network Configuration menu, select 'Host Table';  
The Host Table menu will be displayed:

```
|network configuration|
reset
snmp
tft |host table|
hos |add host|
DNS |change host|
WIN |delete host|
gat
security
reboot server
```

You can now add ([Adding a Host on page 51](#)), change ([Changing a Host on page 52](#)) or delete ([Deleting a host on page 53](#)) a host as required.

## Adding a Host

To add a host (cli syntax add host):

1. Within the Host Table menu, select 'Add Host' from the Host Table menu; this option enables you to add the *hostname* of a host to the host table.

You will be asked to enter the hostname:

```
|network configuration|
reset
snmp
tft |host table|
enter host name: |
gat
security
reboot server
```

2. Type in the name of the host (14 characters maximum) and press <return>.

## Changing a Host

This option enables you to add or change a host's internet address:

To change a host (set host, show host):

1. Within the Host Table menu, Select 'Change Host' from the Host Table menu;

```
| network configuration |
| hosts |
hostname internet address
socrates [192.49.144.4 ]
aristotle [0.0.0.1 ]
plato [0.0.0.1 ]
sophocles [0.0.0.1 ]
homer [0.0.0.1 ]
pythagoras [0.0.0.1 ]
```

This form will list all hosts added to the host table. The default internet address is 0.0.0.1.

2. Enter the correct internet address of each host. Use the <del> key to backspace if necessary.

## Deleting a host

This option enables you to delete an entry from the host table. If a host is referenced by a pre-defined session, or is defined as a gateway or name server, you won't be allowed to delete it.

To delete a host (cli command delete host)

1. Within the Host Table menu, When you select 'Delete Host', the host table will be displayed:

```
|network configuration|
reset
snmp |hosts|
tft |socrates|
hos |aristotle|
DNS |plato|
WIN |sophocles|
gat |homer|
secu |pythagoras|
rebo
```

2. Select the host that you want to delete and press <return>.

You will be asked to confirm the deletion:

```
|network configuration|
reset
snmp |hosts|
tft |socrates|
-----
confirm delete host 'sophocles' (y/n)
-----
gat |homer|
secu |pythagoras|
rebo
```

3. Type 'y' to delete the host, 'n' to cancel the command.

## Changing the Admin Password

*cli syntax:*  
*set user*  
*password*

To change the Admin password proceed as follows;

1. Within the Users menu, select 'Set Password'.
2. From the list now displayed, select 'admin' user.

You will be prompted to enter a password. This can be up to sixteen characters. Use the <del> key to backspace if necessary.

3. At the prompt, enter the password and press <return>.

You are now prompted to enter the password a second time to confirm your choice.

4. At the prompt, re-enter the password and press <return>.

The password change will take effect next time you log in.

**Note** *The factory default password is **superuser**.*

## RADIUS configuration

This section includes the following:

- [Set up procedure on page 55](#)
- [RADIUS parameters description on page 57.](#)

### Set up procedure

To configure how the Perle CS9000 interacts with the RADIUS host or hosts:

1. From the Main menu, select '**radius configuration**':

```
main menu
radius configuration
add authentication host
delete authentication host
add accounting host
delete accounting host
change radius settings
command line mode
```

2. Within the radius configuration menu, select from one of add/delete authentication/accounting host. A list of hosts from the unit's host table is now displayed (see [Setting up the host table on page 51](#)):

```
main menu
rad hosts ion
add au socrates ost
delete aristotle n host
add ac plato st
delete sophocles gs
change homer
pythagoras
comm
```

3. Highlight your selection and press <return>. You will be asked to enter a 'secret' (a password):

```
main menu
rad hosts ion
add au socrates ost
secret: *****
change homer gs
pythagoras
comm
```

4. Key a maximum of sixteen alphanumeric characters.  
To change the secret you must delete the host and then add it again; when you add a host you are prompted for a secret. The first host entered becomes the primary authentication/accounting host, the next host entered becomes the secondary host. You can enter a maximum of two hosts in each of the fields.  
You must enter the same secret in the RADIUS host (see your RADIUS documentation); the secret is not transmitted over the network. Note that to set RADIUS authentication on/off, go to back to the Main Menu and select 'server configuration'. See [Setting up an IP address on page 39](#).
5. Select '**change radius settings**', you are presented with the following (shown in the next picture):

```
+radius configuration+
  retry[5 ]
  timeout[3 ]
  accounting[off]
  acct_port[1646 ]
  auth_port[1645 ]
  acct_authenticator[on ]
  session id[5000000 ]
  user level[normal]
```

The RADIUS parameters are described in [RADIUS parameters description on page 57](#).

6. When you have completed the form, press **Enter**. You will be presented with the following display:

```
+radius configuration+
  retry[5 ]
  timeout[3 ]
  +options+
  accept and exit form 46 ]
  45 ]
  acct_authenticator[on ]
  session id[5000000 ]
  user level[normal]
```

7. Accept the form; you will be returned to the menu.

**Tip** You may want to save your configuration changes permanently; see [Saving configuration changes on page 66](#)

## RADIUS parameters description

The RADIUS parameters are as follows:

### retry

(for authentication) the number of times the unit will re-send a request to a RADIUS authentication host, before re-presenting another login to the user.

(for accounting) the number of times the unit will re-send a request to a RADIUS accounting host, before understanding that the accounting request has failed.

The default retry value is 5; the unit will try the primary host up to 5. You can enter values between 0 (don't retry) and 255. If you have different authentication and accounting hosts unit will retry first the authentication host(s) and then the accounting host(s).

**timeout** - the time in seconds between unit sending a request to a RADIUS accounting or authentication host and receiving a reply. If no reply is received before the expiry of the timeout period, the unit will retry the same host up to and including the number of retry attempts specified under 'retry'.

The default timeout period is 3 seconds (you can enter values between 1 and 255).

**accounting** - turns accounting on or off within the unit; the default is off.

RADIUS  
accounting

RADIUS host specified	accounting flag	state of RADIUS host	result
no	off	-	no accounting
yes	on	up	accounting in both Perle CS9000 and RADIUS host
yes	on	down	accounting in Perle CS9000 only

Notes on Table above:

'accounting' within the Perle CS9000 is an increment of the session id (see below).

'accounting' in the RADIUS accounting host means that you should be able to see accounting information by interrogating the host (see your RADIUS documentation).

**acct\_port** - the UDP port number for RADIUS accounting. The default value is 1646 which should match most RADIUS implementations. Change this value if your RADIUS host is using a different UDP port number.

**auth\_port** - the UDP port number for RADIUS authentication. The default value is 1645 which should match most RADIUS implementations. Change this value if your RADIUS host is using a different UDP port number.

**acct\_authenticator** - a flag to instruct the unit to check the authenticator field in the accounting reply transmission from a RADIUS host to the unit. The authenticator field contains the secret, encrypted. The options are 'on' (the unit will check this field) or 'off' (the unit will not check this field); the default is 'on'. Make sure the setting in your RADIUS host is the same as the unit.

**session id** - displays in real-time the hexadecimal value of the current session (incrementing with each session). The current session is the most recent connection into the unit when the line service is set to 'cslogin' (the default line service).

You can reset the session id to zero; enter 0s from your keyboard.

An explanation of the eight digit value displayed in the session id field is as follows:

the first two digits show the number of reboots which have taken place. The maximum number which will be shown is ff (255); on the next reboot, this value will reset itself to 01 (1).

the last six digits show the number of user sessions which have started since the last reboot (on reboot these six digits are reset to zero). The first session will be 000001, the second session will be 000002, etc. The maximum number of sessions is approximately 16 million, i.e. ffffff, at which point the counter would reset itself to all zeros, i.e. 000000.

An example of all eight digits in a session id is:

0a000006

which means there have been 10 reboots (0a) of this unit (since the counter was reset or wrapped around) and 6 (000006) sessions started since that reboot.

Sessions are measured through the RJ45 ports on the front panel; connections through any of the ports on the rear panel are not shown.

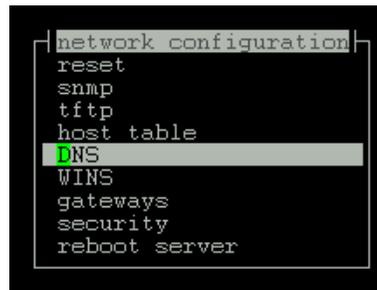
**user level** - displays the default user level for users authenticated by a RADIUS host. If your user is authenticated by RADIUS *and* the RADIUS parameter 'Vendor Specific' is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the user level value configured here (see Appendix xxx) However, the CS9000 RADIUS configuration parameter *user level* allows a default setting for user level for any RADIUS authenticated users that doesn't have the user level specified (see [About user levels on page 103](#)). For all RADIUS authenticated users with a RADIUS user level configured to *menu*, all reverse Telnet and reverse SSH lines will be available to the RADIUS user.

## DNS configuration

You can enter the addresses of two DNS hosts in the Perle CS9000 (the 'unit'); one will be the primary host, the other a secondary host. The DNS hosts do not have to be the same hosts as entered in your unit's host table. On a remote access connection the unit will transmit these addresses to a dial-up Windows NT/95 client. Therefore, your remote user does not have to configure DNS parameters in his/her computer. For more information on DNS see [Appendix D RADIUS & Networking](#).

To configure DNS host proceed as follows;

1. From the Main menu select '**network configuration**':



```
network configuration
reset
snmp
tftp
host table
DNS
WINS
gateways
security
reboot server
```

*Cli syntax:*  
*add DNS*

2. From the network configuration menu, select DNS.

The Add/Delete DNS menu is now displayed.

3. Within the Add/Delete DNS menu select the Add DNS option.

You are now prompted to enter an internet address;

4. Enter this address in dot decimal notation. If you wish, it can be the same address as a machine already entered in the unit's host table.

The first host entered becomes the primary DNS host, the next host entered becomes the secondary host. You can enter a maximum of two DNS hosts.

*delete DNS*

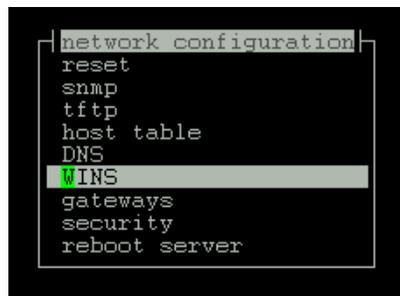
5. If required, change the DNS entry by deleting it, then entering the replacement value.

## WINS configuration

WINS (Windows Internet Name Service) is a database of hostnames and corresponding internet addresses. It is a Microsoft specific name resolution service. The basic function of WINS is the similar to DNS, i.e. it maps computer names to TCP/IP addresses for client computers on a network. For more information on WINS see [Appendix D RADIUS & Networking](#).

You can enter the addresses two WINS hosts in the unit; one will be the primary host, the other a secondary host. On a remote access connection the unit will transmit these addresses to a dial-up Windows NT/95 client. Therefore, your remote user does not have to configure WINS parameters in his/her computer.

1. From the Main menu select '**network configuration**':



```
network configuration
reset
snmp
tftp
host table
DNS
WINS
gateways
security
reboot server
```

*Cli syntax:*  
*add WINS*

2. From the network configuration menu, select WINS.

You are now prompted to enter an internet address;

3. Enter this address in dot decimal notation. If you wish, it can be the same address as a machine already entered in the unit's host table.

The first host entered becomes the primary WINS host, the next host entered becomes the secondary host. You can enter a maximum of two WINS hosts.

*delete WINS*

4. If required, change the WINS entry by deleting it, then entering the replacement value.

## Configuring network gateways

Gateways are hosts that connect Local Area Networks (LANs) together. If you want to access a host which isn't on your local network you will be connected via a gateway. Gateways route data via other gateways until the destination local network is reached. There are three types:

- **Default** - this is a gateway which provides general access beyond your local network.
- **Host** - this a gateway reserved for accessing a specific host external to your local network.
- **Network** - this is a gateway reserved for accessing a specific network external to your local network.

The unit allows you enter a maximum of twenty gateways.

Particularly useful when checking routes to/from gateways is the *show routes* command;

*Active and passive gateways* The unit supports both active and passive gateways. The default is active. Definitions of these types are as follows:

**Active gateway:** a gateway which is temporarily listed in the unit's routing table (while RIP packets are received). If the unit detects that the gateway is no longer operating (no RIP packets received) it will be deleted from the routing table.

**Passive gateway:** a gateway which is permanently listed in the unit's routing table. It is thus always available.

See the following for how to configure gateways:

- [Adding a gateway on page 62](#)
- [Deleting a Gateway on page 63.](#)

## Adding a gateway

To add a gateway proceed as follows:

1. From the Network Configuration menu, select 'Gateway'.
2. From the Gateway menu, select 'Add Gateway'.
3. From the host table now displayed, select a host.  
Note that you can define a host only once as a gateway.  
When you have added a gateway, you must define its type.
4. From the Gateway menu, select 'Change Gateway'.

The Gateways form is now displayed (for example):

```

network configuration
s  reset
u  snmp

gateways
-----
hostname  service  internet address netmask      status
a         [host  ] [172.16.22.2  ] [255.255.255.255] [active ]
timeserv  [host  ] [0.0.0.1     ] [255.255.255.255] [active ]
router312 [default] [             ] [                ] [active ]

h  rip
c  reboot server
  
```

This form lists all gateways defined for your network. In this example, only one has been defined.

5. Complete the Type field; the values are 'host', 'network' or 'default'.  
If you set the field to 'host' or 'network', you must include the internet address of the target host or network. If you change a gateway from 'host' or 'network' to 'default', the internet address will be ignored.
6. Specify the netmask parameter which defines the destination network mask and is only valid for 'network' type gateways. This field is ignored for types 'host' and 'default'. If the netmask parameter is left blank, the netmask will be derived from the the internet address for a 'network' type gateway.
7. Complete the 'Status' field; the values are 'active' or 'passive'.

**Note** *the gateways configured in this table will be ignored if you have used DHCP or BOOTP to download a single passive gateway into the unit; see [Appendix F BOOTP](#).*

## Deleting a Gateway

*delete gateway* If a host on your network is retired from gateway duty, you can use this option to delete it from the list of gateways. Note that the host will NOT be deleted from the host table.

To delete a gateway proceed as follows:

1. From the Network Configuration menu, select 'Gateway'.
2. From the Gateway menu, select 'Delete Gateway' to list your gateways:

```
|network configuration|
reset
snmp
tf      |gateway|
ho      |delete gateway|
DN      |socrates|
WI      |plato|
ga
security
reboot server
```

3. Delete the gateway you require from the list.

## Configuring RIP

The CS9000 which ensures secure administrative access to network console ports, now supports RIP V2 (RFC 2453) with MD5 authentication. Encrypted MD5 Authentication enables secure exchange of routing information on the network, preventing potential hackers from infiltrating precious corporate resource

To configure the CS9000 with specific RIP features see the following commands

1. From the Network Configuration menu, select 'RIP'.
2. From the RIP menu, select 'RIP Settings'.

```

--| network configuration |--
s| reset
  |
  | rip |
  |-----|
  | ethernet mode[send and listen]
  |   send[rip_v2 ]
  |   receive[both ]
  | authentication[md5 ]
  |-----|
h| rip
c| reboot server
  |
  |-----|
  
```

3. Enter the routing parameter on the RIP Settings screen by specifying the **Ethernet mode**, **send** and **receive** parameters and the **authentication** type.
4. Save any changes that you required in the RIP setting screen by hitting **Enter**.
5. If the authentication type has been saved as 'Password' you can specify the RIP password from the RIP menu. Select 'RIP Password' to enter the RIP password used for RIP V2 password authentication.
6. Enter the RIP password and hit **Enter**. Re-enter the RIP password for verification. This RIP password field is only valid for authentication types 'password'.
7. If the authentication type for RIP has been saved as 'MD5', you can configure specific MD5 parameters for authentication from the RIP Menu. Select 'MD5 keys' to display the MD5 Keys menu.

```

--| md5 keys |--
add md5 id
set md5 key
change md5 id
delete md5 id
  
```

8. To add a new MD5 ID, select 'add MD5 id'. You will be prompted for the MD5 ID for a new entry. Enter the name/ID for the new MD5 key and hit **Enter**
9. This will be followed by entering the key associated with the newly created key name/ID. Enter the key and hit **Enter**. Verification of the key is required so re-enter the key and hit **Enter**.
10. To configure the MD5 key parameters, select 'Change MD5 id'.

11. You are then displayed with all MD5 keys, based upon MD5 IDs, and you can configure the start date and time and end date and time. The MD5 keys screens will also display the status of the key associated with the MD5 ID.



id	start	end	key entered
41	[15/10/2003 ] [2:00:00 ]	[15/1/2004 ] [2:10:00 ]	yes
12	[15/1/2004 ] [2:00:00 ]	[15/4/2004 ] [2:10:00 ]	yes
125	[15/4/2004 ] [2:00:00 ]	[15/7/2004 ] [2:10:00 ]	yes
253	[15/7/2004 ] [2:00:00 ]	[15/10/2004 ] [2:10:00 ]	yes

12. After making any necessary configuration changes to the MD5 keys, hit **Enter** and saving the latest configuration changes. NOTE: The MD5 keys will expire based upon the start and end time however they will remain in the MD5 key list and require manual deletion after expiration.

## Verifying your network installation

To check that you have installed the Perle CS9000 (the 'unit') successfully proceed as follows;

1. At the command prompt, try to ping a remote host by typing the following command:

`ping hostname`

Choose a host that you have defined in the host table. If no packet loss is reported, your unit is ready to use. If the command returns an error, refer to the ping cli command. See [Appendix B The CLI commands](#);

# Saving configuration changes

## Saving to non-volatile memory

To save your configuration settings to non volatile memory proceed as follows;

1. After making changes to the configuration exit the text menu screen (form) you are using.  
The 'options' form now appears:



2. Within the options form select 'accept and exit form' to retain your changes in RAM (volatile memory).
3. To save your changes permanently exit the text menu system completely then return to the Main Menu and select 'command line mode';

The exit full screen mode form is now displayed:



4. Within the 'exit full screen mode' form select 'exit and save changes'.  
All the changes made since last entering the menus will be saved to FLASH (permanent, non-volatile) memory.  
You will now be at the command line prompt.
5. To return the menus, at the command prompt, type: screen

## Saving to a file

*cli syntax:* You can also save your configuration information to a file on a host. This can only be done in the cli;  
*netsave* See [Appendix B The CLI commands](#).

## Setting date and time

The Perle CS9000 (the 'unit') has a real-time clock which you can set and view. It is battery-backed and therefore will operate when power is off and over reboots. The clock is year 2000 compliant. Administrators may want to use the advanced time configuration settings specified in [Setting the CS9000 Time Configuration on page 106](#) that allows you to configured the time manually or through an NTP server. Advanced time features like time zone and accomodations for daylight savings time are also described in [Setting the CS9000 Time Configuration on page 106](#).

To set the date and time on your unit proceed as follows;

1. From the Main Menu select `Hardware`.

The hardware form is now displayed. Only the `date` and `time` fields are user editable.

```
hardware
mac address 0080ba0000c2
board id CS4300076R1.6
processor 80386
  warts 2 * Perle ASIC
flash rom 1 x 1MB
  ram 2 x 2MB
battery ram 32kB
serial ports 16

date[23/2/2001 ]
time[14:51:05 ]
```

2. Identify your unit using the hardware information displayed.  
(To view hardware details in command line mode (cli) use the command `show hardware`).
3. Within the 'hardware' form. move the cursor to the start of the field using the 'delete' key; then enter information in the format (for the date):

DD/MM/YYYY e.g. 30/03/2001

and in the format (for the time):

HH:MM:SS e.g. 20:32:00

Note that you do not have to enter the number of seconds.

4. Alternatively, in command line mode (cli) enter the commands 'set date' and 'set time';

To view the date and time select 'hardware' from the Main Menu and check the 'hardware' form; In command line mode, enter the commands `Show date`, `Show time`, or `Show hardware`.

## Performing a soft reboot

To perform a soft re-boot (cli syntax: reboot);

1. From the Network Configuration menu, select 'Reboot'.

You will be asked whether you wish to save your configuration changes to non-volatile memory:

```
|network configuration|
|reset
|snmp
|tftp
|
|save config to flash ROM (y/n)
|
|gateways
|security
|reboot server
```

2. At the prompt, type y and press the Enter key.

The unit will close all connections and then reboot.

# Restoring factory default settings

## Resetting to factory defaults using software

This feature enables you to reset the unit to its default settings. This will clear all configuration data entered by the admin user, and all user accounts, except the default admin user, will be deleted.

To reset to factory default settings from within the software (cli syntax: reset factory):

1. From the Network Configuration menu, select 'Reset'.

You will be asked to confirm the reset:

```
network configuration
reset
snmp
tftp

confirm reboot unit (y/n)

gateways
security
reboot server
```

2. At the prompt, type 'y' to reset the unit, or 'n' to cancel the command.



# Chapter 3 System administration

*You need to read this chapter if you want to do system administration with the Perle CS9000.*

*this chapter if you want to...* This chapter provides task oriented information on system administration with the Perle CS9000.

This chapter includes the following sections;

- [Security on page 72](#)
- [Setting up the line on your Perle CS9000 on page 72](#)
- [Viewing and editing your line settings on page 73](#)
- [Lost password on page 74](#)
- [Configuring a dial in line on page 75](#)
- [Configuring users on page 91](#)
- [Configuring Break Pass Through on page 106](#)
- [Setting the CS9000 Time Configuration on page 106](#)
- [Resetting the line to default on page 111](#)
- [Saving your settings on page 112](#)

## Security

The Perle CS9000 has a number of security features built in that can be enabled or disabled depending on the security level required.

These features include:

- Telnet access - Login and password required.  
See [set line on page 170](#) in [Appendix B The CLI commands](#).
- SSH access - Makes ports only accessible via SSH connections.  
See [Accessing devices via SSH on page 117](#) in [Chapter 4 Using CS9000 as a console server](#).
- Radius authentication - Allows user names and passwords to be authenticated by an external Radius server.  
See [About user accounts and RADIUS on page 92](#) in [Chapter 3 System administration](#).
- Disable Daemons - Allows unused Daemons to be disabled to prevent unauthorised access by hackers.  
See [set server on page 176](#) in [Appendix B The CLI commands](#).
- Trusted host filtering - Prevents the unit from being seen on the network by non-authorized systems  
See [set server on page 176](#) in [Appendix B The CLI commands](#).
- Port idle timers - Each port has configurable idle timers to prevent users leaving a connection open when not being used. By default these are disabled.  
See [set line on page 170](#) in [Appendix B The CLI commands](#).

## Setting up the line on your Perle CS9000

The default use of the Perle CS9000 is as a Console server. Therefore all lines are set with a service of "Reverse Telnet". This allows a user on the LAN to be able to telnet into the ports and access the attached devices.

Each port also requires a TCP port number in order to work. By default, the unit is set to use numbers 10001 to 10024. You can change these to any other port number as long as there is no conflict on the network. Setting the port number to 0 disables access by direct connection to the device on that specific port. This feature allows the administrator of the CS9000 to provide increase security or restriction to devices on the CS9000 by disabling direct connection to devices and only permit access through Easy Port Access menu.

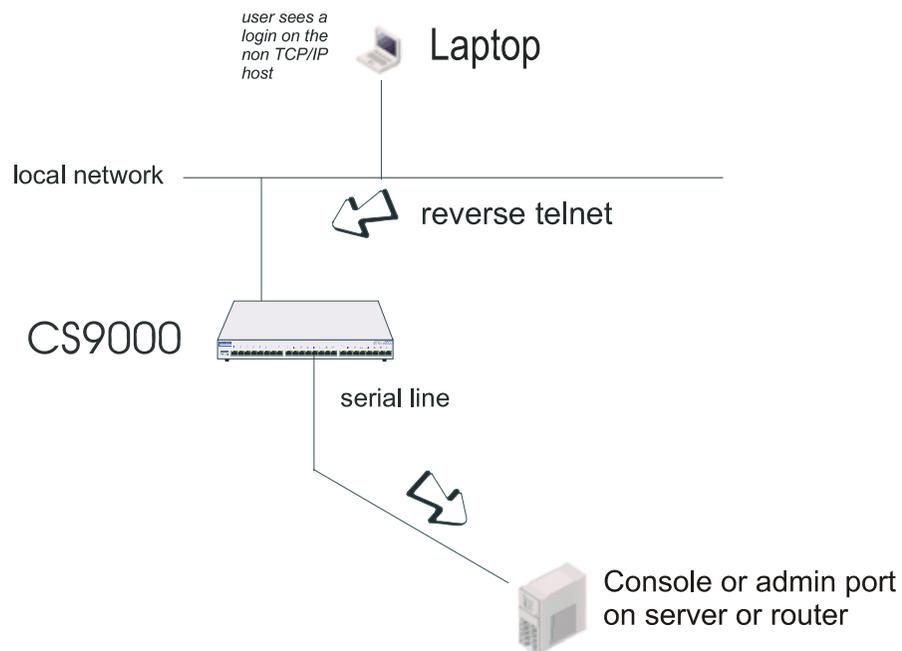
For an explanation of other line services see [Appendix E Summary of Line Service Types](#).

# Viewing and editing your line settings

## Lines set to reverse Telnet by default

*cli syntax:*      A reverse telnet connection enables a TCP/IP host on the local network to establish a login connection via  
*set line*            a Perle CS9000 (the 'unit') port on a non-TCP/IP machine external to the network, such as routers, servers  
and so on.

*A Typical Reverse  
Telnet  
Configuration*



To set up a reverse telnet connection, follow these steps:

1. Select **Line Port Settings** from the Line Configuration menu then select the line that you want to configure.
2. Set 'service' to rev tel (default setting).  
Note when field is highlighted, pressing L will list all available options.
3. Assign a TCP port number to the unit port using the 'CS Port' field. This TCP port number will be used by any host wanting to access the unit port. If you select a TCP port being used by another process, a connection will not be established (By default, lines are set to TCP port 10001 to 10024 for each port. For example, Line 1 10001, Line 16 10016).
4. The 'Hostname' and 'Host Port' fields may contain default or last-used values, but these will be ignored.

- The line should now be configured similar to that shown in the next picture:

```
line 1
service[rev tel] line name[Direct telnet ]
speed[9600 ] terminal[wyse60]
flow[none]
bits[8] user[ ]
parity[none] hostname[sco ]
stop[1] host port[23 ]
security[on ] CS port[10001]
dial[none ] modem name[usr ]
phone number[ ] session timer[ ]
idle timer[ ]
multisessions[100]
```

- Press <return> to exit; if you do not wish to save your changes press the <escape> key.
- If you want to configure all lines with the same parameters, refer to [Resetting the line to default on page 111](#).

## Lost password

If you are an admin user, and you lose your password, there is no way of logging in without it. This restriction is for security reasons. Unless there is another user with admin level privileges (who will have the ability to change your password) you will have to reset the Perle CS9000 (the ‘unit’) to its factory default settings.

*cli syntax:*  
*set user*

If a user forgets his/her password, you can assign a new password; go to the Users Menu and select ‘set password’.

# Configuring a dial in line

## Introduction to SLIP and PPP connections

This section deals with setting up SLIP and PPP connections on a line. There is also a summary of the configurable features of modems.

## Deciding whether to use SLIP or PPP

If you require any of the features listed below, use PPP, otherwise SLIP should be sufficient.

**IP Address Negotiation.** SLIP provides no mechanism for informing the other end of a link of its IP address, whereas PPP will do so.

**Error Checking.** SLIP does not error check whereas PPP does. This is not necessarily a problem in SLIP since most upper layer protocols have their own error checking.

Some systems exchange UDP packets with checksum disabled, which would cause problems should that part of an IP packet get corrupted.

**Authentication.** Once SLIP has started you cannot authenticate the remote device, whereas as PPP provides the option of using security protocols PAP or CHAP. See [Configuring PPP on page 81](#), then sub-section 'Security' for further details.

**Software Flow Control.** You cannot use software flow control on SLIP links since there is no way of escaping control characters from the data stream. PPP has a facility (called ACCM) which allows specific control characters to be escaped from the data stream. See [Configuring PPP on page 81](#) for more details.

For more information on the SLIP and PPP protocols see [Configuring a dial in line on page 75](#).

## Setting up the line

*cli syntax:*  
*set line,*  
*show line*

1. From the Line Configuration menu, select **Line Port Settings**.
2. Within the Line settings menu, select a particular line; e.g. line 3.

The line form will be displayed (default values shown in the next example):

```
line 1
service[rev tel] line name[Direct telnet ]
speed[9600 ] terminal[wyse60]
flow[none]
bits[8] user[ ]
parity[none] hostname[sco ]
stop[1] host port[23 ]
security[on ] CS port[10001]
dial[none ] modem name[usr ]
phone number[ ]
idle timer[ ] session timer[ ]
multisessions[100]
```

3. Within the line form, set the **Service** field using one of the options given in the next table;

Service option	Description
<b>PPP</b>	When you want a remote access service connection using PPP, or when you want to use the unit as a router with PPP. In both cases the user (whether real or dummy) will be authenticated within PPP (provided you use Security - PAP or CHAP).
<b>cslogin</b>	When you want a remote access service connection using SLIP. Do <i>not</i> use the option 'SLIP' because there would be no authentication of the user; (instead, you will set SLIP for a particular user - see <a href="#">Configuring a user account on page 96</a> ). Choosing the 'cslogin' option, the unit will present the login prompt: the user will be required to enter a name and password and hence will be authenticated.
<b>SLIP</b>	When you want to use the unit as a router with SLIP. There will be no authentication of each unit by the other unit.

Option	Description
<b>Line name</b>	Line name can be configured to uniquely identify the line. The Remote Port Logging feature uses this line name instead of the default when creating a file on the remote NFS server.
<b>Speed, Bits, Parity and Stop</b>	Change as necessary from the default line configuration of 9600 baud, 8 data bits, no parity, 1 stop bit.
<b>Flow</b>	Flow Control field to either 'soft' (software) or 'hard' (hardware). For SLIP set to 'hard' only. For PPP set to either 'soft' or 'hard' ('hard' recommended). If you select 'soft' you must set the parameter ACCM when you configure PPP for the line (in <a href="#">Configuring PPP on page 81</a> )
<b>Host port field.</b>	This is the host TCP port number and is set by default to 23. In most cases you can use the default value.
<b>Dial</b>	Set to ' <b>in</b> ' if your user is remote and will be dialling in via modem or ISDN TA; set to ' <b>in</b> ' or ' <b>out</b> ' if using the unit as a router, depending on which end of the link your unit is situated.
<b>Phone Number</b>	When dial is set to 'out' and the line 'service' is set to 'slip' or 'ppp' enter a phone number for the unit to dial (you should only have this combination of settings when you are using two units back-to-back, i.e. as routers.
<b>Idle Timer</b> <i>router use only</i>	Enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of inactivity. When the idle timer expires the unit will end the connection. The default value is 0 seconds so the ports will never timeout. The maximum value is 4294967 seconds (equal to 49 days, approximately). A value of 0 (zero) means the idle timer will not expire, so the connection is open permanently.

---

Service option	Description
<b>Session Timer</b> <i>router use only</i>	Enter a period in seconds for which the session timer will run. Use this timer to forcibly close the session (connection). When the session timer expires the unit will end the connection. The default value is 0 seconds so the ports will never timeout. The maximum value is 4294967 seconds (equal to 49 days, approximately).
<b>Multisessions</b>	Enter the number of supported simultaneous sessions for this line. A value of 0 disables the multisession support on this line.

---

*cli syntax:*  
*add modem*

4. Ignore the other fields in this form. Press **Enter** to exit; if you do not wish to save your changes press the ESC key.
5. Now go to the Line Configuration Menu:
6. Within the Line Configuration Menu, select **Add Modem**.
7. Enter the name of the modem/ISDN TA attached to the unit. You can enter a maximum of twenty names, each with nineteen alphanumeric characters.
8. Within the Line Configuration Menu, select **Change Modem**. Select your modem/ISDN TA name. Enter the initialisation string; see your modem/ISDN TA documentation.
9. Press **Enter** to exit; if you do not wish to save your changes press the ESC key.
10. Go back to the **Line Port Settings** menu. Select your line. When the line parameters form appears go the field **modem name**. Press 'L' (upper or lower case) or the spacebar. Choose the modem name which you entered at Step 5.
11. Press **Enter** to exit; if you do not wish to save your changes press the ESC key.  
You can copy the settings for this line to other lines (an option as you exit this line);  
You can reset this line to default (an option as you exit this form); refer to [Resetting the line to default on page 111](#)
12. You may want to save your configuration permanently; if so, refer to Saving settings to non-volatile memory on page 112.

*set line*

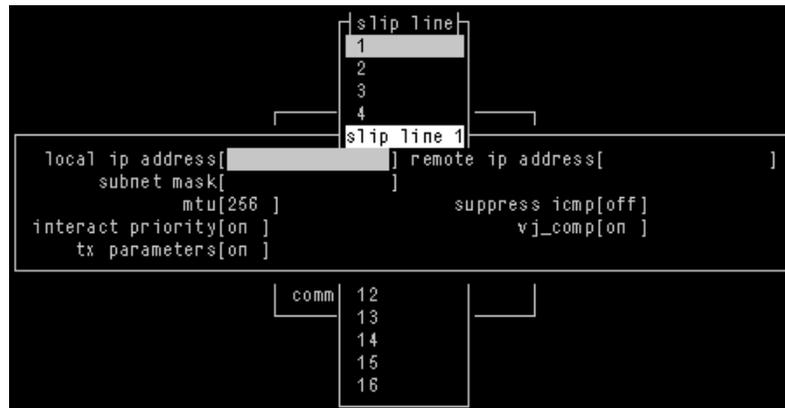
## Configuring SLIP

*cli syntax:* To configure the SLIP parameters proceed as follows;

*set slip line,*  
*show slip line*

1. From the Line Configuration menu, select 'SLIP' and then select a line.

The SLIP form is now displayed (default values shown):



2. Within the SLIP form, set the parameters listed in the next table:

Option	Description
<b>Local ip address</b>	<p>This is the IP address of the unit end of the SLIP link. For routing to work you must enter an IP address in this field. Choose an address which is part of the same network or subnetwork as the remote end; e.g. if the remote end is address 192.101.34.146, your local ip address may be 192.101.34.145; (in the cli, example syntax would be: set slip li 1 lipaddr 192.101.34.145)</p> <p>Do not use the unit's (main) ip address in this field; if you do so, routing will not take place correctly.</p>
<b>Remote ip address</b>	<p>This is the IP address of the remote end of the SLIP link. This must be specified. Choose an address which is part of the same network or subnetwork as the unit (see comment in 'Local ip address' above). Enter the remote ip address in dot notation, e.g.192.101.34.146 (or in the cli, example syntax would be: set slip li 5 ripaddr 192.101.34.146)</p> <p>If your user is authenticated by the unit this remote ip address will be overridden if you have set a 'framed ip' address for the user with values other than 255.255.255.254 or 255.255.255.255; see <a href="#">Configuring a user account on page 96</a>, sub-section 'framed ip'.</p> <p>If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter 'Framed-Address' is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the 'Remote ip address' value configured here.</p>

Option	Description
<b>Subnet Mask</b>	<p>this is the subnet mask of the node on the remote end of the SLIP link. This field is optional. This parameter should be entered in dot notation e.g. 255.255.255.224</p> <p>If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter 'Framed-Netmask' is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the 'Subnet Mask' value configured here.</p>
<b>Maximum transmission unit</b>	<p>The Maximum Transmission Unit (mtu) parameter restricts the size of individual SLIP packets being sent by the unit. Enter a value in bytes between 256 and 1006, e.g. 512 (in the cli, example syntax would be: set slip li 1 mtu 512). The default value is 256. For more information on this parameter see <a href="#">Configuring a user account on page 96</a>, sub-section 'framed mtu'.</p> <p>If your user is authenticated by the unit this mtu value will be overridden when you have set a 'framed mtu' value for the user; see <a href="#">Configuring a user account on page 96</a>, sub-section 'framed mtu'.</p> <p>If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter 'Framed-MTU' is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the 'mtu' value configured here.</p>
<b>Suppress icmp</b>	<p>This option causes ICMP (Internet Control Management Protocol) packets directed to this SLIP link to be discarded. The possible values are 'on' and 'off'; the default is off.</p>
<b>Interactive priority</b>	<p>This determines whether interactive traffic (e.g. telnet sessions) is given priority over batch type traffic (e.g. ftp) thus avoiding the situation where a user has to wait for their character to be echoed while several large ftp packets are transferred. The possible values are 'on' and 'off'; the default is on.</p>
<b>VJ Compression</b>	<p>This determines whether Van Jacobson compression is used on this link; i.e. whether you are using SLIP or C-SLIP (compressed SLIP). The choices are 'on' (C-SLIP) or 'off' (SLIP); the default is 'on'. Select 'on' will turn on VJ compression. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin; see <a href="#">Configuring a dial in line on page 75</a> for more information.</p> <p>In the cli, example syntax would be: set slip li 1 vj on.</p> <p>If your user is authenticated by the unit this VJ compression value will be overridden if you have set a 'framed compression' value for a user; see <a href="#">Configuring a user account on page 96</a>, sub-section 'framed compression'.</p> <p>If your user is authenticated by RADIUS <i>and</i> the RADIUS parameter 'Framed-Compression' is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the 'VJ compression' value configured here.</p>
<b>TX parameters</b>	<p>Meaning Transmit parameters. This will output to the screen of the user all the SLIP parameters configured for that line/port. TX parameters are useful in some applications such as Trumpet Winsock. Options are 'on' or 'off'.</p>

## Configuring PPP

This section describes how to configure a dial in line using PPP and includes the following:

- [PPP configuration procedure on page 81](#)
- [PPP form field descriptions on page 82.](#)

An example of a remote access connection using PPP, including the setup of a remote user is described in [Configuring a dial in line on page 75.](#)

### PPP configuration procedure

*cli syntax:*  
*set PPP line,*  
*show PPP line*

To configure a line using PPP proceed as follows;

1. Within the Line Configuration menu, select 'PPP'.
2. Now select a line.

The PPP form for the selected line is now displayed as shown in the next picture (default values shown in this example):



```

ppp line
1
ppp line 1
local ip address[ ] remote ip address[ ]
  subnet mask[ ] accm[ ]
    mru[1500] security[chap]
      user[ ] password[ ]
        ruser[ ] rpassword[ ]
          address_comp[on ] proto_comp[on ]
            vj_comp[on ] magic_neg[off]
              ipaddr_neg[off]
                conf req. to[3 ] term req. to[3 ]
                  conf req. retries[10 ] term req. retries[2 ]
                    conf nak retries[10 ] auth_tmout[1 ]
                      roaming_callback[off] challenge_interval[ ]
16
  
```

3. Within the PPP form set all the fields to the values you require. See [PPP form field descriptions on page 82](#) for details of how to set each field within the PPP form.

## PPP form field descriptions

This section describes the fields and settings used in the PPP form referred to in [PPP configuration procedure on page 81](#). The following fields are described in this section.

- [Local ip address on page 83](#)
- [Remote ip address on page 83](#)
- [Subnet Mask on page 83](#)
- [ACCM on page 84](#)
- [Max. receive unit on page 84](#)
- [Security on page 84](#)
- [User on page 85](#)
- [Password on page 85](#)
- [Remote User on page 85](#)
- [Remote Password on page 86](#)
- [Address/Control comp on page 86](#)
- [Protocol compression on page 86](#)
- [VJ Comp on page 86](#)
- [Magic No. negotiation on page 87](#)
- [IP address negotiation on page 87](#)
- [Configure req. timeout on page 87](#)
- [Terminate req. timeout on page 87](#)
- [Configure req. retries on page 87](#)
- [Terminate req. retries on page 87](#)
- [Configure NAK retries on page 87](#)
- [Authentication timeout on page 87](#)
- [Roaming callback on page 88](#)
- [Challenge\\_ interval on page 89](#)

*Local ip address* This is the IP address of the unit end of the PPP link. For routing to work you must enter a local IP address. Choose an address which is part of the same network or subnetwork as the remote end; e.g. if the remote end is address 192.101.34.146, your local ip address may be 192.101.34.145; (in the cli, example syntax would be:

```
set ppp li 6 lipaddr 192.101.34.145)
```

To see an example of ip address usage, refer to [‘Setting up an IP address on page 39’](#). Do not use the unit’s (main) ip address in this field; if you do so, routing will not take place correctly.

*Remote ip address*

This is the IP address of the remote end of the PPP link. This must be specified. Choose an address which is part of the same network or subnetwork as the unit (see comment in ‘Local ip address’ above). Enter the remote ip address in dot notation, e.g.192.101.34.146; (or in the cli, example syntax would be: set ppp li 6 ripaddr 192.101.34.146).

If you set the PPP parameter ‘IP address negotiation’ to ‘on’ the unit will ignore the remote ip address value you enter here and will allow the remote end to specify its ip address.

If your user is authenticated by the unit this remote ip address will be overridden if you have set a ‘framed ip’ address for the user other than 255.255.255.254; see [Configuring a user account on page 96](#), sub-section ‘framed ip’.

If your user is authenticated by RADIUS *and* the RADIUS parameter ‘Framed-Address’ is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the ‘Remote ip address’ value configured here. The exception to this rule is a Framed-Address value in the RADIUS file of 255.255.255.254; this value allows the unit to use the remote ip address value configured here.

*Subnet Mask*

This is the subnet mask of the node on the remote end of the PPP link. This field is optional. This parameter should be entered in dot notation e.g. 255.255.255.224 (or in the cli, e.g., set ppp li 9 255.255.255.224).

If your user is authenticated by RADIUS *and* the RADIUS parameter ‘Framed-Netmask’ is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the ‘Subnet Mask’ value configured here.

### ACCM

This allows the specification of an accm (asynchronous control character map) of characters that should be escaped from the data stream. This is entered as a 32 bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped.

The bits are specified most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped i.e. 0x11 (XON). So entering the value 000a0000 (in the cli, e.g.: set ppp li 1 accm 000a0000) will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control.

If you have selected software flow control on the line (see Setting up the line on page 76) you must enter a value of 000a0000 for the ACCM.

The default value is 00000000, which means no characters will be escaped.

### Max. receive unit

The Maximum Receive Unit (mru) parameter specifies the maximum size of PPP packets that the unit's port will accept. Enter a value in bytes between 64 and 1500; e.g. 512 (in the cli, example syntax would be: set ppp li 1 mru 512). The default value is 1500. For more information on this parameter see [Configuring a user account on page 96](#), sub-section 'framed mtu'.

If your user is authenticated by the unit the 'mru' value will be overridden when you have set a 'framed mtu' value for the user; see [Configuring a user account on page 96](#), sub-section 'framed mtu'.

If your user is authenticated by RADIUS *and* the RADIUS parameter 'Framed-MTU' is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the 'mru' value configured here.

### Security

This specifies what type of authentication will be done on the link: none, PAP or CHAP. The default is CHAP.

You can use PAP and/or CHAP to:

- authenticate a port or user on the unit, from a remote location, or
- authenticate a remote client/device, from the unit.

**PAP** is a one time challenge of a client/device requiring that it respond with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully the link will be terminated.

**CHAP** challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the 'secret' (password). A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully the link will be terminated.

With both PAP and CHAP make sure the unit and the remote client/device have the same setting. e.g. if the unit is set to PAP but the remote end is set to CHAP the connection shall be refused.

In the cli, to turn on PAP (for example) the syntax would be:  
set ppp li 7 security pap

If you have selected a line service of 'cslogin', PAP or CHAP will not take place since the user will have already been authenticated. In this case setting security to PAP or CHAP will have no effect.

- User* Complete this field only if you:
- have specified PAP or CHAP (security protocols) in the ‘Security’ field, *and*
  - you wish to dedicate this line to a single remote user, and this user will be authenticated by the unit, *or*
  - you are using the unit as a router (back-to-back with another unit).

‘User’ is the name the remote device will use to authenticate a port on this unit (the opposite of the parameter ‘Remote User’). The remote device will only authenticate your unit’s port when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters, e.g. kevinc8 (or, in the cli, example syntax would be `set ppp li 1 user kevinc8`)

When connecting together two networks, enter a dummy user name; e.g. CS\_HQ.

*Note* *If you want a reasonable level of security the user name and password should not be similar to a user name or password used regularly to login to the unit.*

- Password* Complete this field only if you:
- have specified PAP or CHAP (security protocols) in the ‘Security’ field, *and*
  - you wish to dedicate this line to a single remote user, and this user will be authenticated by the unit, *or*
  - you are using the unit as a router (back-to-back with another unit).

‘Password’ means the following:

in the ‘Security’ field, when you have specified PAP ‘Password’ is the password the remote device will use to authenticate the port on this unit (the opposite of the parameter ‘Remote Password’). The remote device will only authenticate your unit’s port when PAP or CHAP are operating.

in the ‘Security’ field, when you have specified CHAP ‘Password’ is the secret (password) known to both ends of the link upon which responses to challenges shall be based. The remote device will only authenticate your unit’s port when PAP or CHAP are operating.

In both cases, you can enter a maximum of 16 alphanumeric characters; (in the cli, example syntax would be: `set ppp I 7 password *****`)

- Remote User* Complete this field only if you:
- have specified PAP or CHAP (security protocols) in the ‘Security’ field, *and*
  - you wish to dedicate this line to a single remote user, and your user will be authenticated by the unit, *or*
  - you are using the unit as a router (back-to-back with another unit).

‘Remote User’ is the name the unit will use to authenticate the port on the remote device (the opposite of the parameter ‘User’). Your unit will only authenticate the port on the remote device when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters; (in the cli, example syntax would be: `set ppp I 6 ruser kevin`)

When connecting together two networks, enter a dummy user name; e.g. CS\_SALES.

**Note** *If you want a reasonable level of security the user name and password should not be similar to a user name or password used regularly to login to the unit.*

**Remote Password** Complete this field only if you:

- have specified PAP or CHAP (security protocols) in the ‘Security’ field, *and*
- you wish to dedicate this line to a single remote user, and this user will be authenticated by the unit, *or*
- you are using the unit as a router (back-to-back with another unit).

‘Remote password’ means the following:

in the ‘Security’ field when you have specified PAP, ‘Remote Password’ is the password the unit will use to authenticate the remote device.

in the ‘Security’ field when you have specified CHAP, ‘Remote Password’ is the secret (password) known to both ends of the link upon which responses to challenges shall be based.

In summary ‘Remote Password’ is the opposite of the parameter ‘Password’. Your unit will only authenticate the remote device when PAP or CHAP are operating.

In both cases, you can enter a maximum of sixteen alphanumeric characters;  
(or, in the cli, e.g., `set ppp li 1 rpassword *****`)

**Address/Control comp** This determines whether compression of the PPP Address and Control fields shall take place on the link. The choices are ‘on’ or ‘off’; the default is ‘on’. For most applications this should be enabled; i.e. ‘on’. In the cli example syntax would be:  
`set ppp li 1 address_comp on`

**Protocol compression** This determines whether compression of the PPP Protocol field shall take place on this link. The choices are ‘on’ or ‘off’; the default is ‘on’. For most applications this should be enabled; i.e. ‘on’. In the cli example syntax would be:  
`set ppp li 1 proto_comp on.`

**VJ Comp** This determines whether Van Jacobson Compression is used on this link. The choices are ‘on’ or ‘off’; the default is ‘on’. Select ‘on’ will turn on VJ compression. Select ‘on’ will turn on VJ compression. C-SLIP greatly improves the performance of interactive traffic, such as Telnet or Rlogin; see [Configuring a dial in line on page 75](#) for more information. In the cli, example syntax would be: `set ppp li 1 vj on.`

If your user is authenticated by the unit this VJ compression value will be overridden if you have set a ‘framed compression’ value for a user; see [Configuring a user account on page 96](#), sub-section ‘framed compression’.

If your user is authenticated by RADIUS *and* the RADIUS parameter ‘Framed-Compression’ is set in the RADIUS file the unit will use the value in the RADIUS file in preference to the ‘VJ compression’ value configured here.

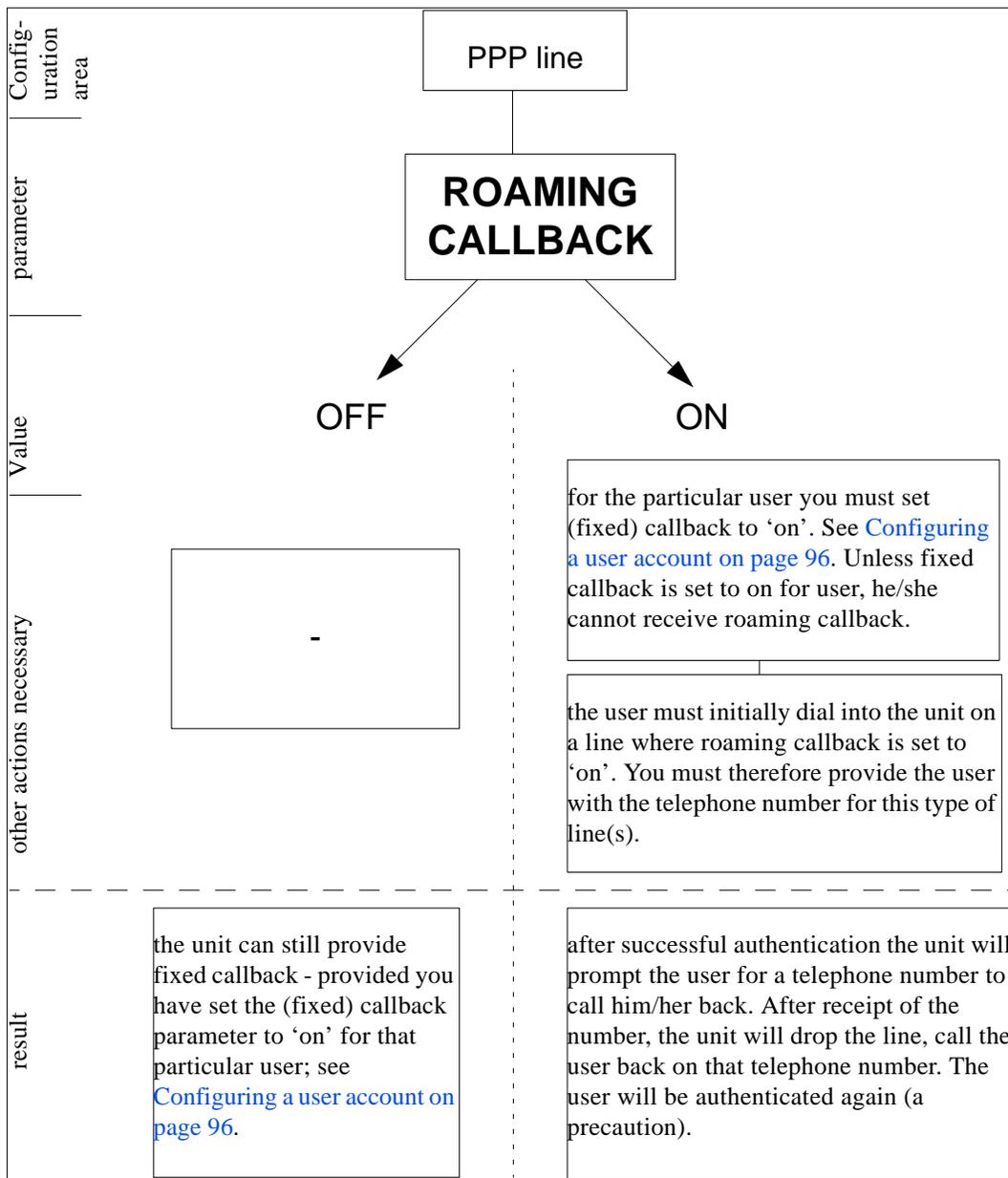
<i>Magic No. negotiation</i>	<p>This is a mechanism whereby a line can determine if it has been looped back. The choices are 'on' or 'off'; the default is 'off'. If enabled (on) this option allows the sending of random numbers on the link. The random numbers should be different, unless the link has been looped back. In the cli, example syntax would be: set ppp li 1 magic_neg off.</p>
<i>IP address negotiation</i>	<p>This parameter specifies whether or not IP address negotiation shall take place. IP address negotiation is where the unit allows the remote end to specify its ip address. The values are 'on' or 'off'. The default value is 'off'.</p> <p>If set to 'on' the unit allows the remote end to specify its ip address; the ip address specified by the remote end will then be used in preference to the Remote ip address set for a line.</p> <p>If set to 'off' the unit will <b>not</b> allow the remote end to specify its ip address. The Remote ip address set for the line will be used.</p> <p>In the cli, example syntax would be: set ppp li 7 ipaddr_neg on.</p> <p>When configuring your user (Configuring a user account on page 96), if you set 'framed ip' address to 255.255.255.255, the unit will override the value for IP address negotiation set here. The result is that the unit will allow the remote end to specify its ip address.</p>
<i>Configure req. timeout</i>	<p>This parameter specifies the maximum time in seconds that LCP (Link Control Protocol) will wait before it considers a 'configure request' packet to have been lost. (in the cli example syntax would be: set ppp li 8 cr_tmout 3).</p>
<i>Terminate req. timeout</i>	<p>This parameter specifies the maximum time in seconds that LCP (Link Control Protocol) will wait before it considers a 'terminate request' packet to have been lost; (in the cli example syntax would be: set ppp li 24 tr_tmout 3).</p>
<i>Configure req. retries</i>	<p>This parameter specifies the maximum number of times a 'configure request' packet will be sent before the link is terminated; (in the cli example syntax would be: set ppp li 23 cr_retry 10)</p>
<i>Terminate req. retries</i>	<p>This parameter specifies the maximum number of times a 'terminate request' packet will be sent before the link is terminated; (in the cli example syntax would be: set ppp li 13 tr_retry 2)</p>
<i>Configure NAK retries</i>	<p>This parameter specifies the maximum number of times a 'configure nak' packet will be sent before the link is terminated; (in the cli example syntax would be: set ppp li 2 nak_retry 10)</p>
<i>Authentication timeout</i>	<p>The timeout in minutes during which successful PAP or CHAP authentication must take place; (you must have PAP or CHAP turned on). If the timer expires before the remote end has been authenticated successfully the link will be terminated. (in the cli example syntax would be: set ppp li 5 auth_tmout 1)</p>

*Roaming callback*

allows the user to specify a telephone number which the unit should use to callback him/her. This feature is particularly useful for a mobile user. The possible values are 'on' and 'off'; the default is 'off'. The operation of roaming callback is shown diagrammatically in Roaming callback on page 88.

Roaming callback can only work with a user whose (fixed) callback parameter is set to 'on'. See [Configuring a user account on page 96](#). Roaming callback therefore overrides (fixed) callback. To use roaming callback, the remote end must be a Microsoft Windows which support Microsoft's Callback Control Protocol (CBCP)

The user is allowed 30 seconds to input a telephone number after which the unit ends the call.



*Challenge\_  
interval*

sets the interval in minutes at which the unit will issue a CHAP re-challenge to the remote end. The default value is 0 (zero) meaning CHAP re-challenge is disabled. During CHAP authentication an initial CHAP challenge takes place, and is unrelated to CHAP re-challenges. The initial challenge takes place even if re-challenges are disabled.

Some PPP client software does *not* work with CHAP re-challenges so you may wish to leave the parameter disabled in the unit.

## Configuring a modem

A summary of the configurable features for modems is listed below.

**Note** *all references to modems apply equally to ISDN Terminal Adaptors*

*cli syntax:*  
*set line*

- you can set the 'dial' parameter to 'in', 'out' or 'none' (default 'none') in the line parameters sub-menu. Setting 'in' or 'out' tells the unit that there is a modem on that line. The unit will communicate with the modem through various RS232 signals. The 'dial' parameter can be set for all line services (e.g. cslogin, silent raw).

*set line*

- when dial is set to 'out' *and* the line service is set to 'slip' or 'ppp' you can enter a 'phone number for the unit to dial (line parameters sub-menu). This combination of circumstances occurs when you have two units connected back-to-back; i.e. they are acting as routers.

*add modem*  
*set modem*

- when the 'dial' parameter to 'in' and the line service is set to 'cs\_login', 'slip' or 'ppp' the unit can initialise a modem. You enter a modem name and initialisation string in the modems sub-menu. The unit will initialise that modem before any new connection is started.

See [add modem on page 154](#) in [Appendix B The CLI commands](#).

## Configuring users

You need to configure user accounts on the Perle CS9000 (the 'unit') for those users who are tasked with administering the attached devices or Remote Access connections. If you are using a RADIUS host you may not need user accounts for those users who are authenticated by the RADIUS host; see [Configuring a dial in line on page 75](#).

When you set up a User account you will see, as an example, the following form in the text menus:

```
-----user johnd-----
  username johnd
  screen switch[1]
  service[csprompt ]
  tcp port[23 ]
  phone number[ ]
  idle timer[ ]
  framed ip[255.255.255.254]
  framed mtu[1500]
  routing[send_and_listen]
  level[normal ]
  ip_host[ ]
  callback[off]
  session timer[ ]
  framed netmask[ ]
  framed compression[on ]
```

More detail on this form is contained in [Configuring a user account on page 96](#).

When telneting or using SSH to connect to a port, the user will need to supply a user name and password.

The **remote access connections** where you will need to configure user accounts are where users:

- are being provided a remote access service, i.e. a SLIP or PPP connection, and they are being authenticated by unit.

As the system administrator you will have your own user account (default name 'admin').

The unit's login accounts are password-protected and assigned a user level; this level restricts the user to certain commands; see [About user levels on page 103](#). A maximum of 32 user accounts can be created.

This section includes the following:

- [About user accounts and RADIUS on page 92](#)
- [Adding a user account on page 95](#)
- [Configuring a user account on page 96](#)

# About user accounts and RADIUS

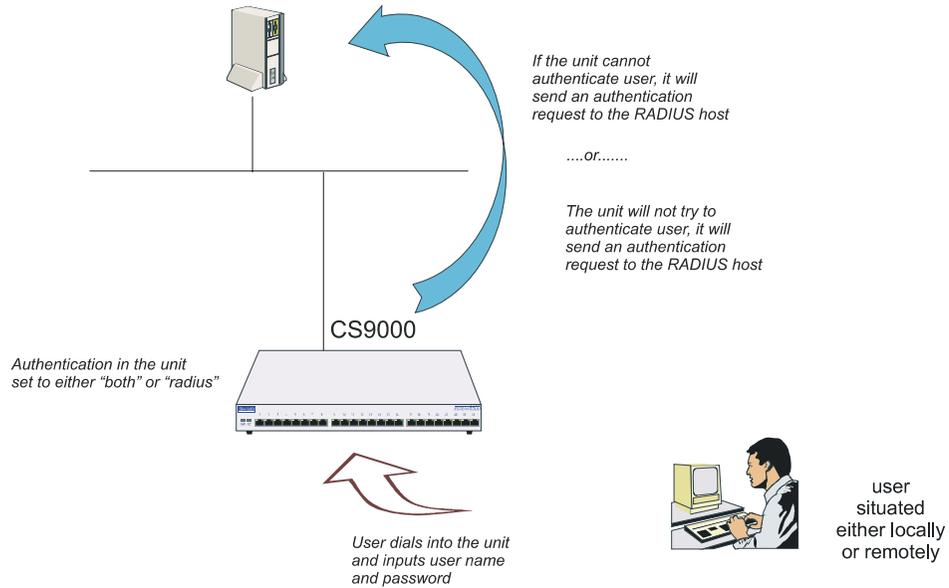
## Overview

You can have a maximum of 32 user accounts on the Perle CS9000. You will also be able to configure user accounts on the RADIUS host. Therefore some users can be authenticated by the unit, other users by RADIUS. You could have other combinations of maintaining user accounts; i.e. duplicated on both the unit and the RADIUS host or, alternatively all user accounts stored on the RADIUS host only.

**Caution**

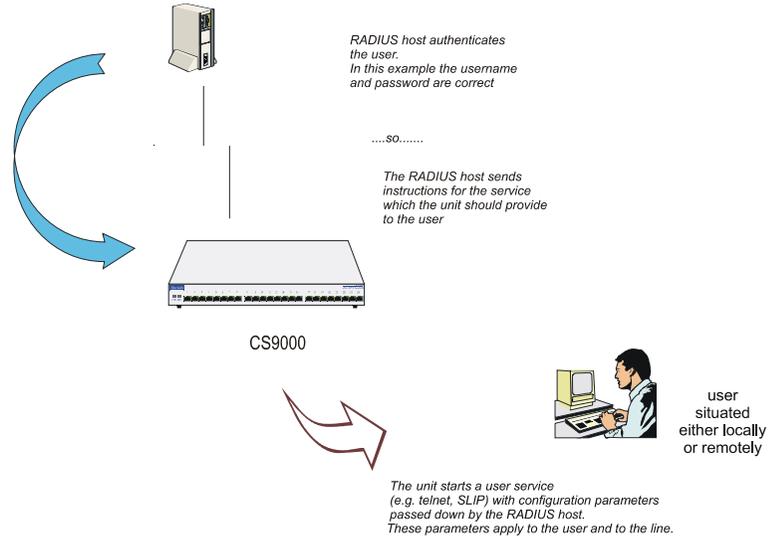
*when a user is authenticated by RADIUS the unit starts a user service - such as telnet or SLIP - based on instructions passed down by the RADIUS host. User parameters - such as 'service' or 'ip\_host' are taken entirely from the RADIUS host. This does NOT apply to reverse SSH or reverse Telnet session types.*

*When RADIUS authenticates users*



**Caution**

*If you set the port to authenticate by RADIUS only, users will not be able to dial in and connect if the network connection is down (no access to RADIUS server).*



## Example RADIUS user file: telnet service

```
davePassword = "garage"
User-Service = Callback-login,
Login-Host = 192.101.34.199,
Login-Service = Telnet,
Login-TCP-Port = 23,
Class = "Indirect Sales Group",
Session-Timeout = 1800,
Idle-Timeout = 600,
CallBack-Number = "3592"
```

An explanation of the file shown in Example RADIUS user file: telnet service on page 94 is as follows:

- the file contains a mixture of user parameters (e.g. callback-number) and line parameters (e.g. login-host).
- this user has been authenticated by RADIUS; therefore, all user parameters are passed down to the unit in this file.
- if you also have user 'dave' listed in the unit's user table (i.e. a duplicate entry - we do not recommend this action) all the user parameters configured in the unit for user 'dave' will be overridden by the parameters in the RADIUS file when authentication method is set to **Both(local + RADIUS)**. For the user to be authenticated by the RADIUS host, where you have a duplicate entry, the password for 'dave' in the unit would have to be different to that entered in the RADIUS user's database *or* authentication in the unit would have to be set to RADIUS (i.e. RADIUS only).
- `Class = "Indirect Sales Group"` is a RADIUS class attribute. The unit can only process a string of maximum 32 characters; therefore limit your string to this size. In this example "Indirect Sales Group" is 20 characters (including spaces).
- line parameters override those configured in the unit; see [Configuring a dial in line on page 75](#) for a more detailed discussion on line parameters.

## Adding a user account

To add a user account, proceed as follows;

1. Within the Users menu, select 'Add User' (cli syntax: add user).
2. Enter a username, maximum sixteen characters (do not use spaces). If your user is equipment allocate an appropriate name, e.g. barcode2.
3. Enter a password, maximum sixteen characters (do not use spaces). Re-enter the password.

Admin users can change user passwords using the 'Set Password' feature described in Changing a user's password on page 105. Normal users can change their own passwords; see [Changing a user's password on page 105](#).

## Configuring a user account

The section includes the following:

- [Configuration procedure on page 96](#)
- [User form field descriptions on page 97.](#)
- [About user levels on page 103](#)
- [Line Access Rights on page 103.](#)

### Configuration procedure

To configure a user account, proceed as follows;

*Tip* Your user configuration will only be used if the user is authenticated by the local user database. If the user is authenticated by RADIUS, the unit will use configuration details for users sent by the RADIUS host; see [Configuring a dial in line on page 75](#) for all line types except reverse SSH and reverse Telnet. Reverse SSH and reverse Telnet sessions refer to the user configuration in the local user database and refer to defaults when authenticated by RADIUS host.

1. Select 'Change User' from the Users menu (cli syntax: set user).
2. Choose your user from the list of names now displayed.

A user form will now be displayed as shown in the next example (uses default values):

```
----- user johnd -----
username johnd
screen switch[1] level[normal ]
service[csprompt ] ip_host[ ]
tcp port[23 ] callback[off]
phone number[ ]
idle timer[ ] session timer[ ]
framed ip[255.255.255.254] framed netmask[ ]
framed mtu[1500] framed compression[on ]
routing[send_and_listen]
```

3. Within the user form, set the fields you require. See [User form field descriptions on page 97](#) for a description of how to set each field in more detail.
4. Press **ENTER** to exit; accept or discard the form as you wish.

*Note* Changes you make in this form, as the system administrator, will only take effect for a user when the user next logs in to the unit.

## User form field descriptions

This section describes the fields within the user form detailed in [Configuration procedure on page 96](#). The following fields are included:

- [Service on page 98](#)
- [TCP Port No on page 99](#)
- [phone number on page 99](#)
- [idle timer on page 99](#)
- [session timer on page 99](#)
- [Level on page 99](#)
- [IP Host on page 99](#)
- [callback on page 100](#)
- [Callback for a user on page 101](#)
- [framed ip on page 102](#)
- [framed netmask on page 102](#)
- [framed mtu on page 102](#)
- [framed compression on page 102.](#)
- [routing on page 102](#)

## Service

Instructs the unit to start a user service by selecting one from the following list (once the user is authenticated successfully):

**csprompt:** a login on the unit (the default setting). This service is for system administrators.

**Telnet:** a Telnet service provided by the unit. Use this service when you/a user is connected directly to a port via a serial line (i.e. not connected into one of the network ports). When the telnet service starts, the user will be authenticated by the host. Now go to the IP Host and TCP Port No fields.

**Rlogin:** an Rlogin service provided by the unit. Use this service when you are is connected directly to a port via a serial line (i.e. not connected into one of the network ports). When the rlogin service starts, the user will be authenticated by the host. Now go to the IP Host field.

**TCP clear:** use for devices which require a login, i.e. authentication. Such devices could be a bar code reader or smart card. 'TCP clear' provides a channel on which 8-bit data is passed, without interpretation, to a host. It has the same meaning as the TCP Clear login service specified in the RADIUS Authentication rfc.

**SLIP:** The SLIP service will be started using the SLIP parameters set for that line; see [Configuring SLIP on page 79](#). There will be no further login prompt (unless callback is operating). The SLIP line settings will be taken from the settings configured for that line.

*Tip* When specifying the 'SLIP' option, we recommend you set the 'line service' on that particular line to 'cslogin'; see [Setting up the line on page 76](#).

**PPP:** The PPP service will be started using the PPP parameters set for that line; see [Configuring PPP on page 81](#). There will be no further login prompt (unless callback is operating). The PPP line settings will be taken from the settings configured for that line.

*Tip* When specifying the 'PPP' option, we recommend you set the 'line service' on that particular port to 'cslogin'; see [Setting up the line on page 76](#).

*Note* Note also that some types of user service have the same name as line service types, e.g. 'user service: SLIP' and 'line service:SLIP'. User 'service' is explained in [Configuring a user account on page 96](#).

- TCP Port No* (ignore this field unless you have selected a user Service of 'telnet')  
(telnet only) enter the TCP/IP port number of the host with which the unit should start the telnet service. The default port is 23; in most cases you should leave the value at default.
- phone number* Enter a telephone number for the unit to call back the user; do not use spaces. You must also have 'callback' set to on. (The number you enter is unrelated to the 'phone\_number' or 'dial' parameters you can set for a line).
- idle timer* (you may wish to change this setting for terminal server connections) enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of user inactivity. When the idle timer expires the unit will end the connection. The default value is 0 seconds so the ports will never timeout. The maximum value is 4294967 seconds (equal to 49 days, approximately). A value of 0 (zero) means the idle timer will not expire so the connection is open permanently.  
  
Note: this idle timer will override the idle timer which you can configure for a line with the exception of reverse Telnet or reverse SSH line configurations.
- session timer* (you may wish to change this setting for terminal server connections) enter a period in seconds for which the session timer will run. Use this timer to forcibly close a user's session (connection). When the session timer expires the unit will end the connection. The default value is 0 seconds so the ports will never timeout. The maximum value is 4294967 seconds (equal to 49 days, approximately).  
  
Note: this session timer will override the session timer which you can configure for a line with the exception of reverse Telnet or reverse SSH line configuration.
- Level* This field cycles through 'admin', 'normal', 'menu' and 'restricted'. These are privilege levels and are described in [Configuring a dial in line on page 75](#). The 'admin' user (i.e. you as system administrator) always has 'admin' level account (maximum privileges).
- IP Host* (ignore this field unless you have selected a user **service** of 'telnet' or 'rlogin' or 'tcp clear').  
  
0.0.0.0 - default. The unit will use the default ip host configured for all users who login to the unit. The default ip host is set in the 'server configuration' menu; see Perle CS9000, (or in the cli see command 'set server'). The IP address entered here does not affect the host table or any line configuration.  
  
255.255.255.255 - specified by user. The unit will prompt the user for an IP address or hostname, when the telnet or rlogin service is started. When the user service is set to Telnet, Rlogin or TCP Clear, the unit will give the user two attempts the enter the required information.  
  
n.n.n.n - (where 'n' is a number) you specify in this field the IP address of a host with which the unit should start the telnet or rlogin service for this user.

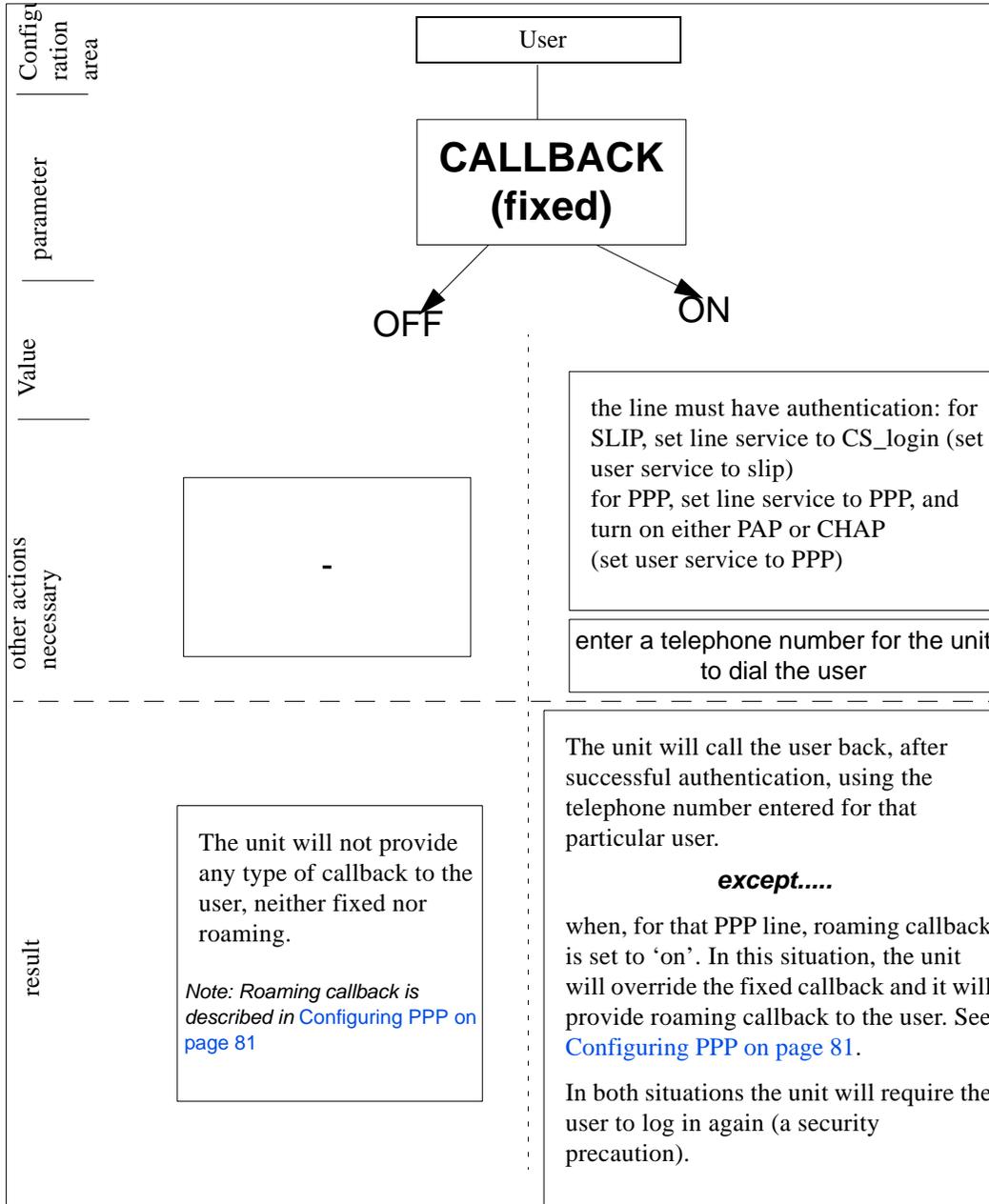
*callback*

(callback for a user is also known as FIXED callback) the values are either 'on' or 'off' (default is off). When 'on' enter a phone number for the unit to call the user back; see the field 'phone number'; (the callback setting is unrelated to the 'dial' parameter you can set for a line).

*Note:* the unit will only allow callback when a user is authenticated. If the protocol over the link does not provide authentication there will be no callback. Hence, when the line service is set to 'PPP' you must use either PAP or CHAP (see Configuring PPP on page 81, sub-section 'Security'), because these protocols provide authentication.

For a diagrammatic view of callback, see Callback for a user on page 101. Note that the unit supports another type of callback - ROAMING callback - which is configurable for a line when you are using the PPP protocol; see Configuring PPP on page 81.

Callback for a user



- framed ip* (use only when the user service field is set to 'slip' or 'ppp') this is the ip address of the remote user. Enter the address in dot decimal notation as follows:
- 255.255.255.254 (default) - if you enter this value, the unit will use the remote ip address set for the line; see [Configuring SLIP on page 79](#) or [Configuring PPP on page 81](#).
- 255.255.255.255 (when user service is set to 'ppp') - if you enter this value the unit will allow the remote machine to specify its ip address; (it therefore overrides the parameter 'ip address negotiation' which you can configure for PPP).
- 255.255.255.255 (when user service is set to 'slip') - if you enter this value the unit will use the remote ip address set for the line (no negotiation).
- n.n.n.n - (where n is a number); enter an ip address of your choice. This ip address will then be used in preference to the remote ip address set for a line.
- framed netmask* (use only when the user service field is set to 'slip' or 'ppp'). If the remote user is on a subnet, enter the subnet mask. This field is for your information only; it is not processed by the software.
- framed mtu* (use only when the user service field is set to 'slip' or 'ppp') This field specifies the maximum size of packets in bytes being transferred across the link. On noisy links it may be preferable to fragment large packets being transferred over the link since there will be quicker recovery from errors. Depending on whether you have selected a user 'service' of SLIP or PPP, details are as follows:
- for PPP, framed mtu will be the maximum size of packets that the unit port will accept. This value is negotiated between the two ends of the link. The default value is 1500 bytes. Enter a value in bytes in the range 64-1500. An example value is 512 bytes; this will restrict the unit to accepting packets no greater than 512 bytes in length.
- for SLIP, framed mtu will be the maximum size of packets being sent by the unit. The unit will send SLIP packets in the range 256-1006 bytes. The default value is 256 bytes. An example setting is 512: this will restrict the unit to sending SLIP packets no greater than 512 bytes in length.
- The framed mtu value will be used in preference to the mtu/mru values set for a line; see [Configuring SLIP on page 79](#) or [Configuring PPP on page 81](#).
- framed compression* (use only when the user service field is set to 'slip' or 'ppp') this parameter determines whether Van Jacobsen Compression is used on the link. Select either 'on' or 'off' (default is 'off'). VJ compression is a means of reducing the standard TCP/IP header from 40 octets to approximately 5 octets. This gives a significant performance improvement particularly when interactive applications are being used. Such an application is typing, where a single character can be passed over the link with a 40 octet header attached. VJ Compression has little effect on other types of link, such as ftp, where the packets are much larger.
- The framed compression value will be used in preference to the VJ compression values set for a line; see [Configuring SLIP on page 79](#) or [Configuring PPP on page 81](#).
- If you set up any restricted users, you must predefine their sessions; they can only open sessions predefined for them by the admin user.
- routing* the routing parameter determine the routing mode used on the PPP and SLIP interfaces that are authenticated by the particular user. Values are **none**, **send**, **listen** and **send\_and\_listen**. It has the same function as the Framed-Routing attribute for RADIUS authenticated users.

## About user levels

There are four user levels which can be used to determine the level of access the user has to Perle CS9000 commands:

- Admin** the system administrator. The admin user has total access to the unit. You can create more than one admin user account but we recommend that you only have one. They can monitor or configure the unit through CLI and screens
- Normal (default)** .the normal user has limited access to the unit. Limited CLI commands are available and no access to screens configurations.
- Restricted** the restricted user can only view or monitor the unit. CLI commands to show information regarding the unit will only be displayed.
- Menu** the menu user will not have any access to CLI commands for the unit. The menu user will only be displayed the Easy Port Access menu that allows a user to view all accessible lines that the user has access rights to. The Easy Port Access allows the user to connect to each accessible line without disconnecting their initial connection to the CS9000 unit.

Note: When a user is authenticated by a Radius host, a user will be entitled to Normal or Menu user level access, based upon the RADIUS **user level** setting.

## Line Access Rights

For administrators of the CS9000, the Line Access Rights feature allows the administrator to permit access to specific devices on the CS9000 based upon user. Each user can be configured to have access rights to specific ports on the CS9000. Whether a user connects directly to the device on the specified line or through the Easy Port Access menu, only devices that a user has rights to will permit a user access.

To configure a user's Line Access Rights

1. Select **line access** from the user menu and press **Enter**.



2. Select the user you wish to modify their line access right and press **Enter**.

- By default all users have access right to all devices on the lines of the CS9000. The **X** indicates the lines that the user has access to and what type of access rights they have with the device (RW - Read/Write, RI - Read Input; RO - Read Output). To set the access right mode to Read Both, enable both the RI (Read Input) and RO (Read Output). By default, all lines are indicated with an **X** for the RW field indicates that the particular user has full access rights to each line. . A blank indicates that the user will be denied access to the specified lines. Specify the lines the user has access right to by setting the appropriate marker **X** and in the type of access mode that they are permitted.

```

line access for test
  RW  RI  RO      RW  RI  RO      RW  RI  RO      RW  RI  RO
1 [X] [ ] [ ]    2 [X] [ ] [ ]    3 [X] [ ] [ ]    4 [X] [ ] [ ]
5 [ ] [X] [ ]    6 [X] [ ] [ ]    7 [X] [ ] [ ]    8 [X] [ ] [ ]
9 [X] [X] [ ]    10 [ ] [ ] [ ]    11 [X] [ ] [ ]    12 [X] [ ] [ ]
13 [X] [ ] [ ]   14 [X] [ ] [ ]    15 [X] [ ] [ ]    16 [X] [ ] [ ]
17 [X] [ ] [ ]   18 [X] [ ] [ ]    19 [X] [ ] [ ]    20 [X] [ ] [ ]
21 [X] [ ] [ ]   22 [X] [ ] [ ]    23 [X] [ ] [ ]    24 [X] [ ] [ ]

```

- Press **ENTER** to exit the line access right screen and accept changes when prompted.

## CLI prompts

For admin users, the cli prompt is followed by a hash sign, for example CS\_9000#. For normal and restricted users the prompt will be followed by a dollar or pound sign, for example CS\_9000\$. The display of a dollar or pound sign will vary according to the characters supported by your terminal.

## Changing a user's password

To change a user's password, proceed as follows;

1. Within the Users menu, select 'Set Password' (cli syntax set user).
2. Select a user from the list displayed.  
You will be prompted to enter a password. This can be up to sixteen characters long (do not use spaces). Use the <del> key to backspace if necessary.
3. Enter the password and press <return>.
4. When prompted, re-enter the password and press <return>.

The password change will take effect next time the user logs in.

## Deleting a user account

To delete a user account, proceed as follows;

**Note** *You will be unable to delete the default admin user, users that are logged in or users dedicated to a specific line.*

1. Within the Users menu, select 'Delete User' (cli syntax delete user).
2. Select the user that you want to delete from the list displayed.  
You will be asked to confirm the deletion;
3. Type 'y' and press <return>.

The user will be deleted.

## Configuring Break Pass Through

The CS9000 will not send break signals on power cycles. It is also configured not to allow break signals to be sent through to attached devices by default. However, some administrators may wish to be able to send the break signal i.e. to take a Sun Solaris system to the Open Boot prompt.

To enable this feature, please use the following CLI command to enable/disable proprietary inband SSH break signal processing as well as existing Reverse Telnet break signal.

```
CS9000# set server break <on/off>
```

```
CS9000# save
```

The OEM mode flag 0x0010 will be set/reset based upon this command.

A break signal is generated on a specific serial port only when the server's break option is enabled and the user has typed the exact break string over a reverse SSH connection.

For SSH, the default break signal is '~break', where ~ is tilde. To change the SSH break signal, use the following command:

```
CS9000# set server ssh_break_string <8-characters>
```

*Note* A terminal client must be used that is capable of sending the break signal

## Setting the CS9000 Time Configuration

The CS9000's internal clock can be configured through all configurators including CLI, menu screens and HTML and can be adjusted through various methods. The internal clock for the CS9000 is displayed for timestamping information for both remote and local port buffering features. The CS9000 time configuration allows the administrator to set the time manually or configured to communicate across the LAN to an NTP or SNTP server to synchronize the CS9000's internal clock. The Simple Network Time Protocol (SNTP) feature on the CS9000 supports the client side of the protocol as described in RFC 2030. The CS9000 will be able to obtain its time from a NTP or SNTP server and then can be synchronized amongst other network devices. Additionally, the CS9000 can also be configured to support various time variations features such as local time zone and adjustments for daylight savings time.

### Manually Set the Time

To configure the CS9000's internal clock manually, proceed as follows:

1. Within the main menu, select **Time Configuration**
2. Within the **Time Configuration** screen, select **set time**
3. The time setting options form is now displayed to set the current date and time:

```
set time
date[31/12/2003]
time[10:30:23] est
```

4. After completing your changes to the time, hit **Enter** and accept change and exit form.

## Time Setup through SNTP

When the CS9000 has SNTP enabled it will periodically send NTP packets to the NTP/SNTP server which will respond with the network time. The CS9000 will synchronize its internal clock with the response from the NTP/SNTP server. The method in which the CS9000 sends or receives the NTP packets from the NTP/SNTP server is configurable in three modes: unicast, multicast and anycast.

In unicast mode, the CS9000 will have to be configured with the IP Address of the NTP server and will periodically send a request packet to the NTP server. The NTP server will then respond directly to this request with the current time. The CS9000 supports a primary and a secondary IP Address for NTP servers.

In multicast mode, the CS9000 does not initiate the request packets but waits to receive the periodic broadcasts from the NTP server with the current time. Once the CS9000 receives an NTP packet from the server, it will then synchronize its internal clock with the current time.

In anycast mode, the CS9000 will send out a request packet as a broadcast on the LAN to get a response from any NTP server. When the first response is received from an NTP server, the internal clock of the CS9000 is synchronized. The CS9000 will learn the IP Address of the NTP server that responded and then operate in unicast mode.

To configure the CS9000's internal clock to be synchronize to an SNTP or NTP server on the LAN, proceed as follows:

1. Within the main menu, select **Time Configuration**
2. Within the **Time Configuration** screen, select **SNTP settings**
3. The SNTP setting options form is now displayed to configure the NTP primary and secondary servers in which the CS9000 will communicate with.

```
sntp settings
add server 1
delete server 1
add server 2
delete server 2
sntp settings
```

4. To configure the primary SNTP server, select **add server 1**
5. The list of host available will be displayed and can be selected or designated as the SNTP primary server in which the CS9000 will obtain its time information. See [Setting up the host table on page 51](#) for changing the hosts or host details.
6. To configure the secondary SNTP server, select **add server 2**. Again a list of available host will be displayed and can be selected as the designated SNTP secondary server.

7. To configure the method in which the CS9000 communicated with the primary and secondary STNP servers, select **sntp settings**
8. The SNTP settings forms is now displayed.

```
sntp settings
mode[unicast]
version[4]
server 1[linux]
server 2[pc]
```

9. To change the communication method with the SNTP server select **mode** and chose one of three modes **unicast**, **multicast**, or **anycast**
10. To change the SNTP version, select **version** and choose the appropriate version which is compatible with the SNTP server the CS9000 will be communicating with.
11. The **server 1** and **server 2** options displayed indicate the current primary and secondary SNTP servers, respectively. If you wish to change the designated host to communicate SNTP, select **server 1** or **server 2** and hit **1** to display all available hosts.
12. After completing your changes to the SNTP setting, hit **Enter** and accept change and exit form.

## Setting Time Zones

The CS9000 supports time variation feature of local time zones and daylight savings time regardless if the internal clock is synchronized with an NTP server. The local time zone feature allows the CS9000 to offset the internal clock by a configurable time from the UTC time. The configurable time zone off set can be specified in hours (0 to 23) and minutes (0 to 59) and can also be specified by a specific name up to 4 characters.

To configure the CS9000's internal clock adjust to a configurable time zone, proceed as follows:

1. Within the main menu, select **Time Configuration**
2. Within the **Time Configuration** screen, select **time zone settings**
3. The time zone settings form is now displayed to configure the specific name of the time zone and time adjustments

```
time zone settings
name[est]
offset[-5:00]
```

4. To configure the name of the time zone, select **name** and enter the id name for the time zone (up to 4 characters)
5. To configure the deviation from the UTC, select the **offset** option and enter hours (-12 to +14 ) and minutes (0 to 59) with a direction indicator (+) adjust forward or (-) adjust backward.

6. After completing your changes to the time zone settings, hit **Enter** and accept change and exit form.

## Setting Time for Daylight Savings Time

Adjustments to the internal clock for daylight saving time (Summer-time) can be enabled and specified for one time within the year or recurring year after year. Configuration parameters allow the CS9000 to enable Summer-time each year by specifying the month, week, day and hour for the begin and end Summer-time

To configure Summer-time for the CS9000, proceed as follows:

1. Within the main menu, select **Time Configuration**
2. Within the **Time Configuration** screen, select **summer time mode**.
3. The summer time mode form is displayed and selecting the option **mode** allows you to configure the summer-time to take effect at a specified time for that year (**fixed**) or recurring year after year with the option of **recurring**. The option **none** disabled the summer time feature on the CS9000

```
summer time mode
mode[recurring]
```

4. After completing your changes to the summer mode settings, hit **Enter** and accept change and exit form.
5. Within the **Time Configuration** screen, select **summer time settings**
6. The summer time setting form is now displayed and indicated on the top of the form is the selected summer mode (recurring or fixed). NOTE: Summer time setting form is displayed different based upon the type of summer mode.

```
summer time settings
mode recurring
name[edt]
offset[60]
start month[april ]
start week[1 ]
start day[sunday ]
start time[2:00:00 ]
end month[october ]
end week[last]
end day[sunday ]
end time[2:00:00 ]
```

```
summer time settings
mode fixed
name[edt ]
offset[60]
start date[4/4/2004 ]
start time[2:00:00 ]
end date[31/10/2004]
end time[2:00:00 ]
```

7. Select the **name** option to configure the name of the timezone.
8. Select the **offset** option to specify the number of minutes to adjust the internal clock by when summertime begins and re-adjusts when summertime ends.
9. The options for the summer time settings are configurable to the summertime **start** and **end** times specified in **month, week, day, time** for recurring mode and **start** and **end date** and **time** for fixed mode. Each **start** and **end** option can be configured as follows:

**month:** month option specifies the month of the year in which daylight savings time will start/end. This mode is available for recurring mode only.

**week:** week option specifies the week of the month in which daylight savings time will start/end. This is available in recurring mode only.

**day:** day option specifies the day of the week in which daylight savings time will start/end. This is available in recurring mode only.

**time:** time option specifies the time of day in which daylight savings time will start/end. This is configurable in both recurring and fixed mode.

**date:** the day, month and year in which daylight savings time will start/end. The date format is dd/mm/yyyy, where dd is the day, mm is the month and yyyy is the year. This is only available in fixed mode.

10. After completing your changes to the summer mode settings, hit **Enter** and accept change and exit form.

## Resetting the line to default

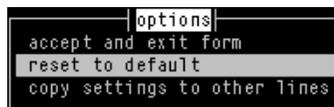
This feature enables you to reset the serial line which you are configuring to the default settings. It is available in the Line Settings form (under the Line Configuration Menu).

To reset the line to the default settings proceed as follows;

1. Within the Line Configuration Menu, select **Line Port Settings** (cli syntax reset line).

The **Line Port Settings** form is now displayed

2. Within the **Line Port Settings** form, with the cursor at any position inside the form, press <return>.
3. The Options form is now displayed:



4. Within the Options form, select **reset to default**.

The line will be reset to 9600 baud, 8 data bits, 1 stop bit, no parity and software flow control; the line type will become 'rev tel', the TCP Port '23', the Idle Timer '0' seconds (so the ports will never timeout) and the hostname the first host entered in the host table. security to 'on' enabled and the CS port to 100xx.

# Saving your settings

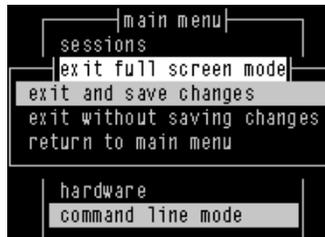
## Saving settings to non-volatile memory

1. After making changes to the configuration, exit the text menu screen (form) you are using.  
The 'options' form now appears:



2. Within the options form select 'accept and exit form' to retain your changes in RAM (volatile memory).
3. To save your changes permanently exit the text menu system completely then return to the Main Menu and select 'command line mode';

The exit full screen mode form is now displayed:



4. Within the 'exit full screen mode' form select 'exit and save changes'.  
All the changes made since last entering the menus will be saved to FLASH (permanent, non-volatile) memory.  
You will now be at the command line prompt.
5. To return the menus, at the command prompt, type: screen

## Saving settings to a file

*netsave*

**You can also save your configuration information to a file on a host. This can only be done in the cli; see [Appendix B The CLI commands](#)**

# Chapter 4 Using CS9000 as a console server

*You need to read* You need to read this chapter if you want information on how to use the Perle CS9000 as a console *this chapter if you* server.

*want to...*

This chapter provides task orientated information on using the Perle CS9000 as a console server.

This chapter includes the following sections

- [Introduction on page 114](#)
- [Accessing devices via Telnet from the LAN on page 115](#)
- [Accessing devices via SSH on page 117](#)
- [Accessing devices with Multisession on page 122](#)
- [Accessing devices via modems using PPP on page 125](#)
- [Accessing devices via modems using a dumb device on page 126.](#)
- [Accessing Local Port Buffers on page 127](#)
- [Accessing Remote Port Buffers on page 130](#)

For details of installation procedures, see [Chapter 2 Installation](#).

For information about performing system administration tasks with your Perle CS9000, see [Chapter 3 System administration](#).

# Introduction

Once the unit has been configured and users added using the procedures given in [Chapter 2 Installation](#) and [Chapter 3 System administration](#), you can begin to use it as a console server.

There are three methods of accessing the devices attached to the serial ports:

- Accessing devices via telnet from the LAN. See [page 115](#)
- Accessing devices via SSH from the LAN. See [page 117](#)
- Accessing devices via modems on a dial in link using PPP. See [page 125](#)
- Accessing devices via modems on a dial in link with no network. See [page 126](#)

## Accessing devices via Telnet from the LAN

### Terminal emulators

In order to perform this function you must have a system capable of running a telnet session. Microsoft Windows does have an implementation of telnet but it is limited. You may wish to use a terminal emulator package such as:

- Term - Century Software - [www.censoft.com](http://www.censoft.com) (eval available)
- NetTerm - shareware
- PuTTY - freeware

## Information required

For a user with **normal** or **admin** access rights, accessing a device on the CS9000 requires a direct access connection (see [Direct Access procedure on page 115](#)). A user with **menu** access rights can choose to connect to a device by direct access or through Easy Port Access.

To connect to a specific device using a direct access connection, you must know the following information:

- IPAddress of CS9000 unit
- Port on CS9000 the device is connected to
- TCP port number of CS900 port (by default port 1 will be 10001, port 2 10002 etc.)

For a user with **menu** access rights and choosing to connect to a device through Easy Port Access, only requires a connection to the CS9000 unit on well known Telnet port 23. The user will then be presented with Easy Port Access menu to connect to any device on the CS9000 (see [Easy Port Access Procedure on page 116](#)). In order to view the Easy Port Access menu you must know the following:

- IP Address of the CS9000
- Well known Telnet port number 23

## Direct Access procedure

To access a device using Telnet proceed as follows;

1. Set your terminal emulator to connect to the ip address of the CS9000 and set port number for correct port.
2. If running from Windows command line, run following command:  
telnet 'ipaddress' 'port num'  
Example - telnet 192.65.121.4 10004

A CS9000 login prompt will then be displayed.

**Note: To disable this feature use the cli command, *set line security <on/off>***

3. At this prompt, enter your user name for the CS9000 and press **Enter**.
4. At the password prompt, enter your password for the CS9000 and press **Enter**.

You will now be connected to the port and thus the connected device. At any time, you may bring up the Easy Port Access menu to connect to a different line or log out.

## Easy Port Access Procedure

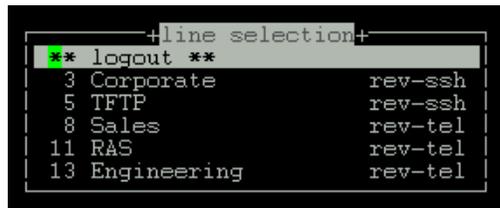
To access a device using Telnet proceed as follows;

1. Set your terminal emulator to connect to the ip address of the CS9000 and set port number for 23 (usually the default).
2. If running from Windows command line, run following command:  
telnet 'ipaddress'  
Example - telnet 192.65.121.4

A CS9000 login prompt will then be displayed.

3. At this prompt, enter your user name for the CS9000 and press **Enter**.
4. At the password prompt, enter your password for the CS9000 and press **Enter**.

You will now be presented with a Easy Port Access menu, displaying all available ports that the user has access rights to.



```
+line selection+
** logout **
 3 Corporate      rev-ssh
 5 TFTP           rev-ssh
 8 Sales          rev-tel
11 RAS            rev-tel
13 Engineering    rev-tel
```

5. Select the port of the device you will to connect to and press **Enter**.

You will now be connect to the device selected. At any time that you wish to return to the Easy Port Access menu, type the configurable line menu string (see [Server form field descriptions on page 46](#)) and the Easy Port Access menu will be displayed. The connection to the device will be dropped allowing for you to select the next device you wish to manage.

**Note** *You must choose a port that matches the connection type that you established with the CS9000. For example, you will be able to view all port that you have acces to but can only connect to the port configured for reverse Telnet. The CS9000 does not permit access to reverse SSH configured ports unless the initial connection to the CS9000 is established using SSH protocol.*

## Accessing devices via SSH

In order to perform this function you must have a system capable of running an SSH session. The Perle CS9000 supports both SSH version 1 and SSH version 2. You may wish to use a SSH client software such as :

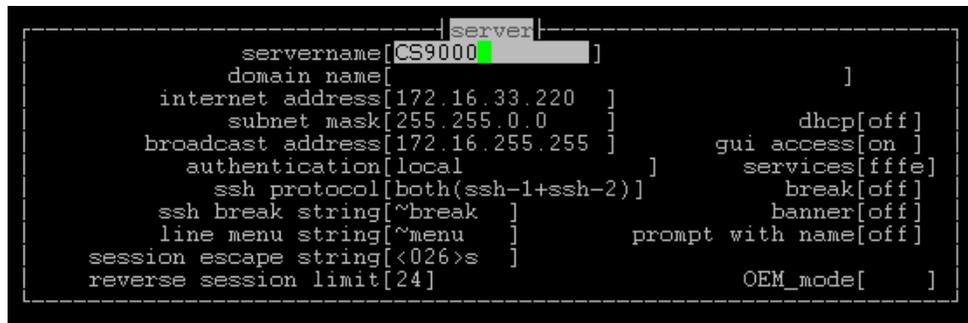
PuTTY - PuTTY is a free implementation of Telnet and SSH for Win32 platforms available from the web.

## SSH Setup Procedure

To connect to a specific device using SSH you must configure the CS9000 to support the SSH protocol. By default, the SSH protocol is disabled.

To configure the CS9000 for SSH perform the following steps:

1. Through console/admin port or by telnet access across the LAN, access the server configuration through CLI commands or through the menu configuration screens.



```
server
-----
servername[CS9000 ]
domain name[ ]
internet address[172.16.33.220 ]
subnet mask[255.255.0.0 ]
broadcast address[172.16.255.255 ]
authentication[local ]
ssh protocol[both(ssh-1+ssh-2)]
ssh break string[~break ]
line menu string[~menu ]
session escape string[<026>s ]
reverse session limit[24]
dhcp[off]
gui access[on ]
services[ffff]
break[off]
banner[off]
prompt with name[off]
OEM_mode[ ]
```

2. Select the appropriate SSH protocol setting.

SSH1 – SSH version 1 only

SSH2 – SSH version 2 only

Both – Both SSH version 1 and SSH version 2 supported

Disabled – SSH protocol is disabled.

```

server
-----
servername[CS9000 ]
domain name[ ]
internet address[172.16.33.220 ]
subnet mask[255.255.0.0 ]
broadcast address[172.16.255.255 ]
authentication[local ]
ssh protocol[both(ssh-1+ssh-2)]
ssh break string[~break ]
line menu string[~menu ]
session escape string[<026>s ]
reverse session limit[24 ]
dhcp[off]
gui access[on ]
services[fffe]
break[off]
banner[off]
prompt with name[off]
OEM_mode[ ]

```

3. You will be prompted to generate the SSH keys associated with the version of SSH selected. This initial generation of key takes a few minutes and you will be asked to confirm if you want to proceed with the key generation. The SSH key generation is only performed once unless the CS9000 is reset back to factory default.

```

+server+
servername[ ]
internet address[172.16.1.30 ]
broadcast address[172.16.255.255 ]
About to generate SSH-1 keys.
This will take 5 to 10 minutes - proceed? y/n
gui access[off]
banner[off]
OEM_mode[ ]

```

4. During key generation, an indicator at the bottom of the screen shows the keys being generated. During the key generation process, any users connected to the box may experience performance delays due to the intense CPU time to generate secure keys for the SSH protocol support.

```

+server+
servername[ ]
internet address[172.16.1.30 ]
broadcast address[172.16.255.255 ]
About to generate SSH-1 keys.
This will take 5 to 10 minutes - proceed? y/n
. . . + + + + + .
gui access[off]
banner[off]
OEM_mode[ ]

```

5. Once the keys have been generated, you will be prompted to save your settings.
6. Each line which you require secure access to will have to be configured for reverse ssh. Go to the appropriate line configuration setting to set the line service to **rev ssh**  
**NOTE:** the line will only support the SSH protocol which was selected in the server configuration.

```
service[lev ssh] line name[Corporate ]
speed[9600 ] terminal[dumb ]
flow[none]
bits[8] user[ ]
parity[none] hostname[sa_test ]
stop[1] host port[23 ]
security[on ] CS port[10003]
dial[none ] modem name none
phone number[ ]
idle timer[ ] session timer[ ]
```

7. Save your line configuration settings and SSH protocol is now supported.

## Information required

For a user with **normal** or **admin** access rights, accessing a device on the CS9000 requires a direct access connection (see [Direct Access procedure on page 119](#)). A user with **menu** access rights can choose to connect to a device by direct access or through Easy Port Access.

To connect to a specific device using a direct access connection, you must know the following information:

- IP Address of CS9000 unit
- Port on CS9000 the device is connected to
- TCP port number of CS9000 port (by default port 1 will be 10001, port 2 10002 etc.)
- SSH protocol enabled and associated key generated on the CS9000
- Disable decompression on SSH client software – feature is not supported on CS9000

For a user with **menu** access rights and choosing to connect to a device through Easy Port Access, only requires a connection to the CS9000 unit on well known SSH port 22. The user will then be presented with Easy Port Access menu to connect to any device on the CS9000 (see [Easy Port Access procedure on page 120](#)). In order to view the Easy Port Access menu you must know the following:

- IP Address of the CS9000
- Well known SSH port number 22
- SSH protocol enabled and associated key generated on the CS9000
- Disable decompression on SSH client software – feature is not supported on CS9000

## Direct Access procedure

To access a device over a secure SSH session, proceed as follows:

1. Set up your SSH client software to connect to the IP Address of the CS9000 and set port number for the correct port.
2. Setup your SSH client software to match the SSH protocol version that is configured on the CS9000 unit.
3. Connect to the CS9000 using the above parameters.
4. A login prompt will appear and you can enter your user name.  
**NOTE:** In order to provide a secure SSH connection across the LAN the login prompt can be delayed by a few seconds as the secure line is being negotiated.
5. At the password prompt, enter your password for the CS9000 and press **Enter**.

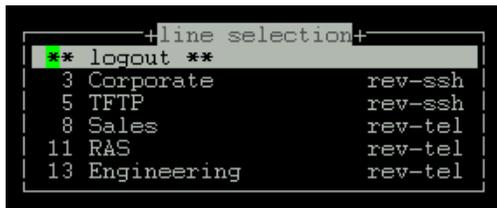
You will now be connected to the port over a secure SSH LAN connection. At any time, you may bring up the Easy Port Access menu to connect to a different line or log out.

## Easy Port Access procedure

To access a device using SSH proceed as follows;

1. Set up your SSH client software to connect to the IP Address of the CS9000 and set socket number for the well know SSH port 22 (usually the default).
2. Setup your SSH client software to match the SSH protocol version that is configured on the CS9000 unit.
3. Connect to the CS9000 using the above parameters.
4. A login prompt will appear and you can enter your user name.  
**NOTE:** In order to provide a secure SSH connection across the LAN the login prompt can be delayed by a few seconds as the secure line is being negotiated.
5. At the password prompt, enter your password for the CS9000 and press **Enter**.

You will now be connected to the CS9000 over a secure SSH LAN connection and be presented with an Easy Port Access menu, displaying all available ports that the user has access rights to.



```
+line selection+
** logout **
 3 Corporate      rev-ssh
 5 TFTP           rev-ssh
 8 Sales          rev-tel
11 RAS            rev-tel
13 Engineering    rev-tel
```

6. Select the port of the device you will to connect to and press **Enter**.

You will now be connect to the device selected. At any time that you wish to return to the Easy Port Access menu, type the configurable line menu string (see [Server form field descriptions on page 46](#)) and the Easy Port Access menu will be displayed. The connection to the device will be dropped allowing for you to select the next device you wish to manage.

**Note** *You must choose a port that matches the connection type that you established with the CS9000. For example, you will be able to view all port that you have acces to but can only connect to the port configured for reverse SSH. The CS9000 does not permit access to reverse Telnet configured ports unless the initial connection to the CS9000 is established using Telnet.*

## Accessing devices with Multisession

Devices attached to the CS9000 can be accessed by more than one user with the multisession feature on the CS9000 enabled. The multisession feature permits multiple users to connect to the same device on the line of the CS9000 and perform tasks based upon their line access rights and access modes that they have been configured for. Users can be configured to have access to specific ports and access modes for these ports such as Read/Write (RW), Read Input (RI), Read Output( RO) and Read Both (RI & RO). See [Line Access Rights on page 103](#) for more detailed information of configuring users.

To setup your CS9000 lines for support of multisessions, you must initially setup at least one of the lines to be enabled with the number of multisessions supported for that particular line (non-zero). Enabling multisession feature is not dynamic and does require a reboot in order for the configuration and feature to take effect

1. Through console/admin port or by telnet access across the LAN, access the line configuration through CLI commands or through the menu configuration screens.
2. Select the line you wish to configure.
3. In the line configuration screen, the **multisession** field can be configured up to 124 sessions per unit. These 124 sessions per unit can be distributed on multiple line setup configurations or designated to one particular line or device. (NOTE: on the blue CS9000 the maximum number of multisession is

```

service[New tel] line name[Direct telnet ]
speed[9600 ] terminal[wyse60]
flow[none]
bits[8] user[ ]
parity[none] hostname[sco ]
stop[1] host port[23 ]
security[on ] CS port[10001]
dial[none ] modem name[usr ]
phone number[ ]
idle timer[ ] session timer[ ]
multisessions[100]
  
```

24). Multisession is considered enabled on the CS9000 if at least one port has multisessions configured (non-zero). To disable multisession support on the particular line, configure the multisession field to 0.

In addition to configuring the multisessions, the **security** field must be enabled for multisession functionality to be enabled.

4. Each user by default will be enabled to have full access rights (RW) to all lines present on the CS9000 unit. Changes to the user's access rights and access modes can be configured in the Line Access Rights screen.
5. Select the User Configuration and then the Line Access option.
6. Select the user in which you want to configure for and the **Line Access** screen will be displayed for that particular user. When a user connects to a line, the initial mode is determined by their line access rights with the following priority. RW (Read/Write) is the highest priority, followed by both RI (Read Input) and RO (Read Output) enabled, then RI or RO individually

```

-----|line access for test|-----
  RW  RI  RO      RW  RI  RO      RW  RI  RO      RW  RI  RO
1  [X] [ ] [ ]    2  [X] [ ] [ ]    3  [X] [ ] [ ]    4  [X] [ ] [ ]
5  [ ] [X] [ ]    6  [X] [ ] [ ]    7  [X] [ ] [ ]    8  [X] [ ] [ ]
9  [X] [X] [ ]   10  [ ] [ ] [ ]   11  [X] [ ] [ ]   12  [X] [ ] [ ]
13 [X] [ ] [ ]   14  [X] [ ] [ ]   15  [X] [ ] [ ]   16  [X] [ ] [ ]
17 [X] [ ] [ ]   18  [X] [ ] [ ]   19  [X] [ ] [ ]   20  [X] [ ] [ ]
21 [X] [ ] [ ]   22  [X] [ ] [ ]   23  [X] [ ] [ ]   24  [X] [ ] [ ]
-----|-----

```

- While in session, multisession users can enter an escape sequence which allows them to send messages to other users connected to the same line, kill other session connected to the same line and switch modes (RW, RI, RO, RB) depending upon their line access rights. The escape sequence is configurable and can be set in the server configuration screen. The default is <CTRL-Z> S.

```

-----|server|-----
servername[CS9000 ]
domain name[ ]
internet address[172.16.33.220 ]
subnet mask[255.255.0.0 ]
broadcast address[172.16.255.255 ]
authentication[local ]
ssh protocol[both(ssh-1+ssh-2)]
ssh break string[~break ]
line menu string[~menu ]
session escape string[<026>s ]
reverse session limit[24]
dhcp[off]
gui access[on ]
services[iffe]
break[off]
banner[off]
prompt with name[off]
OEM_mode[ ]
-----|-----

```

- While in session, the user can at any time enter the session escape sequence to view the multisession menu which presents the user the options of sending messages, kill session or switch modes. The kill session option will only be made available to users configured for RW access mode.

```

reverse session menu
change mode
send message
kill session
-----|-----

```

9. If you want to switch access modes during the session, depending upon the users configuration for access modes, the access mode options will be displayed and take effect immediately.

```
┌ session mode ─┐
│ readwrite     │
│ readin       │
│ readout      │
│ readboth     │
└────────────────┘
```

10. If you want to send messages to the other user connected to the same line, select **Send message** from the multisession menu and then you will be prompted for the text of the message you wish to send

```
┌ reverse session menu ─┐
└────────────────────────┘
message: █
```

The other users connected to the port will be display the text of the message. For example

```
[Message from admin]: 'testing this' █
```

11. If you want to kill another session or user that is connected to the same serial port, select the **Kill Session** option. **NOTE: Only users with RW access mode are permitted to kill another session.** A list of the present users connected to that serial port will be displayed and you are able to select the user to terminate their connection. The option of **all** is available to terminate all other sessions or users. Once selected, the session is immediately terminated.

```
┌ reverse session menu ─┐
└────────────────────────┘
┌ kill session ─┐
│ ** all **     │
│ test          │ [pid 024]
└────────────────┘
```

## Accessing devices via modems using PPP

For this method you will need to setup one of the serial ports for PPP (see [Configuring a dial in line on page 75](#) in [Chapter 3 System administration](#)).

With a line configured for PPP you will be able to dial in for a PC using Microsoft's dial up networking.

A remote user will dial up by using dial up networking and once authenticated by the CS9000 will be connected to the network. At this point a telnet session can be initiated as in the [Accessing devices via Telnet from the LAN on page 115](#).

**Note** *Even in the event of a main network failure a user will still be able to connect to the CS9000 and access a port.*

## Accessing devices via modems using a dumb device

For this method you will be using either a PC with a terminal emulator or a dumb terminal.

To setup a serial port for this method proceed as follows:

1. Login in to CS9000 as admin.
2. At CS9000 prompt type **screen** and press **Enter**.  
The Main menu now appears.
3. From the Main menu, select Line Configuration - **Line Port Settings**.
4. Select the line number you wish to configure.

```
line 1
service[rev tel]      line name[Direct telnet ]
speed[9600 ]          terminal[wyse60]
flow[none]
bits[8]               user[ ]
parity[none]          hostname[sco ]
stop[1]              host port[23 ]
security[on ]        CS port[10001]
dial[none ]          modem name[usr ]
phone number[        session timer[ ]
idle timer[ ]
multisessions[100]
```

5. Set the service to **cslogin**.
6. Check speed, flow, bits, parity and stop are the same as your modem settings.
7. Press **Enter** and select **Save settings**.
8. Exit menus and save settings to flash memory.
9. Connect modem to the serial port on your CS9000.
10. Dial into your Perle CS9000 unit via modems.  
You are now presented with a login prompt
11. At the login prompt enter your CS9000 user name and press enter,  
A password prompt is now displayed
12. At the prompt enter the password and press enter.  
A CS9000 prompt is now displayed.
13. At this prompt telnet to the appropriate port  
For example Telnet 'ipaddress' 'port #'

## Accessing Local Port Buffers

Port Buffers are available on the entire Perle CS9000 range of Console Servers. The Port Buffering feature allows data activity on the CS9000 serial ports to be held in memory for viewing at a later stage without affecting the normal operation of the serial ports.

Port Buffering is required by system administrators to capture important information from devices attached to the CS9000 Console Server. If a device (such as a Router) has a problem and sends a warning message out of its console port while no one is connected, the warning can be lost. With Port Buffers enabled on the CS9000 the messages will be captured in memory and can be viewed later to aid administrators in diagnosing and fixing problems.

There are two versions of the CS9000 hardware available with different sizes of port buffers:

CS9000 with Blue case- Available as a software upgrade. This will allow customers with this variant of the CS9000 to gain from the benefits of port buffers. The buffer sizes are:

CS9016 – 58k per port up to 114k per port

CS9024 – 19k per port up to 76k per port

The default buffer sizes can be increased by trading off against the number of simultaneous connections needed. For instance, a 24 port unit can have 24 simultaneous users connected as a default, however, this can be reduced to 1, 2, 3 or more up to 23 simultaneous users. For every simultaneous user removed, extra memory is released for the port buffers and is spilt evenly across all ports.

CS9000 with Dark Grey case – This variant of the 8, 16 and 24 port CS9000's have increased memory that allow much bigger port buffers to be configured. Again, reducing the number of simultaneous connections allowed will increase the default buffer sizes. For every simultaneous user removed extra memory is released for the port buffers and is spilt evenly across all ports.

CS9008 – 1.051Mb per port up to 1.103Mb per port

CS9016 – 495k per port up to 552k per port

CS9024 – 310k per port up to 368k per port

Port buffer information for each serial port can be viewed after successful connection to a device on a serial port. The user can toggle between communicating to the device on the serial port and viewing the port buffer data for that device by entering a configurable string (default `~view`).

## Setup

To enable port buffers on the CS9000, proceed as follows:

1. Login in to CS9000 as admin.
2. At CS9000 prompt type **screen** and press **enter**.  
The Main menu now appears.
3. From the Main menu, select **Port Buffering Configuration**.
4. Select the Port Buffering option and select **Local**.

```
port buffering configuration
mode local ]
view port buffer string [~view ]
time stamp on ]
nfs host linux ]
nfs directory [/cs9000/portlogs ]
nfs encryption off ]
```

To view the local port buffer for a particular serial port, you must connect to the device on that serial port by reverse Telnet or reverse SSH. Once you have established a connection to a device, at any time you can enter the **View Port Buffer String** which will switch the display to view the content of the port buffer for that particular serial port. To return to communicating to the device, hit the **ESC** key and the communication session will continue from where you left off.

By default the View Port Buffer String is set to **~view**. To configure and customize the View Port Buffer String, proceed as follows

5. Select View Port Buffer String from the **Port Buffering Configuration** menu
6. Define your Port Buffer String (up to 8 characters). You can specify control (unprintable) codes, specify the decimal value enclosed in < > (e.g. to specify escape b, <027>b )

The port buffer data can be timestamped and displayed with the date and time of data being received on the port. To enable this feature, proceed as follows:

7. Select time stamp from the **Port Buffering Configuration** menu
8. To enable the timestamping feature, select **on**. To disable the timestamping feature select **off**.

To decrease the number of simultaneous users that is supported on the CS9000 and provide more port buffer memory to each serial port, you can configure the Reverse Session Limit within the Server Configuration.

9. Select the Reverse Session Limit field from the **Server Configuration** menu
10. Select the number of support sessions (between 1 and the # of CS9000 ports).
11. Press **Enter** and select **Save settings**.
12. Exit menus and save settings to flash memory.
13. Reboot the CS9000.

## Access Port Buffers

To access and view the port buffers for the serial ports on the CS9000, proceed as follows

1. Connect to the device on the serial port through reverse Telnet (See “Accessing devices via Telnet from the LAN” on page 115.) or reverse SSH (See “Accessing devices via SSH” on page 117.).

2. Once successfully connected to the device at any time enter the **View Port Buffer String** and the display will show the last entries in the port buffer.

To navigate through the port buffer data the following chart illustrates the keyboard keys or “hot keys” that can be used to view the port buffer data. To return to the connection to the device at any time hit the ESC key and you can continue to communicate with the device on that particular serial port.

**Table 1: Port Buffer Viewing**

<b>Keyboard Buttons</b>	<b>Hot Keys</b>	<b>Direction</b>
Page Up	<CTRL>B	Up
Page Down	<CTRL>F	Down
Home	<CTRL>T	Top of the buffer data (oldest data)
End	<CTRL>E	Bottom of the buffer (latest data)
ESC		Exit viewing port buffer data.

# Accessing Remote Port Buffers

The CS9000 has the ability to support Remote Port Buffering . The Remote Port Buffering feature allows data received from the serial lines on the CS9000 to be sent to a remote server, supporting NFS (Network File System), for logging purposes. The data that is transmitted to the remote NFS server can be raw data or encrypted for security reasons. This feature only logs data from serial lines configured for reverse SSH or reverse Telnet. The Remote Port Buffering feature works alongside with the Local Port Buffer feature, described in [Accessing Local Port Buffers on page 127](#), giving administrators the capability to analyse data and messages from the servers connected to the CS9000.

With the Remote Port Buffering feature, the data received from the servers on the serial lines configured for reverse SSH or reverse Telnet will be encrypted (configurable option) and transmitted to an NFS server (configured within the CS9000) on the LAN interface. The console server will create unique remote files on the NFS host using the console server's configured line names for each line. If the line names are left at a default setting, the console server will create unique files using the console server's Ethernet MAC address and line number. It is recommended that a unique NFS directory and line names be configured if multiple console servers use the same NFS host for Remote Port Buffering. The filenames will always be created on the NFS host with a .ENC extension to indicate data encrypted files and .DAT for unencrypted files. If the data is encrypted across the LAN, the Decoder utility application, available on Windows (DOS/9x/NT/ME/2000/XP), SUN Solaris x86, SUN Solaris SPARC 64 and 32, Linux x86, can be run on the NFS server to convert the encrypted data to a readable file for the administrators to analyze. NOTE: The Windows/DOS platform restricts the converted readable file to an 8.3 filename limitation.

## Setup

To enable the CS9000 for Remote Port Buffering, proceed as follows:

1. Login to the CS9000 as admin
2. At CS9000 prompt type **screen** and press **enter**. The Main menu appears
3. From the Main menu, select **Port Buffering Configuration**
4. Select the Port Buffering option and select **Remote**. NOTE: Port Buffering option set to Both will enable both Local and Remote Port Buffering features.

```
-----|port buffering configuration|-----
      mode[remote]
view port buffer string[~view  ]
      time stamp[on ]
      nfs host[linux      ]
      nfs directory[/cs9000/portlogs ]
      nfs encryption[on ]
```

To configure the specific NFS server information in which all data is transmitted to across the LAN, the following configuration options must be set:

5. Select the **NFS Host** field and select the host name specified to your NFS server. NOTE: the NFS server can be configured through the [Setting up the host table on page 51](#)
6. Select the **NFS Directory** field and specify the directory on the NFS host that will be used to house the remote port log files.
7. Optionally, you can configure the transmitted data to be encrypted or raw data (default) by enabling the **NFS Encryption** option to **ON**. NOTE: if the NFS encryption option is enabled, installation of the corresponding Decoder utility on the NFS server is required to decrypt the files created on the NFS server by the CS9000.



# Appendix A Cabling information

*You need to read this appendix if you want cabling information for the Perle CS9000.*

*this appendix if you want to...* This appendix provides connector pinout and cabling information for the Perle CS9000 console server.

This appendix includes the following sections;

- [RJ45 RS232 serial ports on page 134](#)
- [AUI port on page 135](#)
- [RJ45 10/100BaseT port on page 136](#)
- [Admin Port on page 137](#)
- [Third party connection examples on page 138](#)
- [Connecting to PC serial ports on page 143](#)
- [Connecting to Terminals on page 144](#)
- [Connecting to Modems on page 148](#)
- [Loopback cable on CS9000 RJ45 serial port on page 149](#)

# RJ45 RS232 serial ports

The RS232 RJ45 serial ports are 8-pin shielded and surge-suppressed to 15KV. Note that DCD is an input.

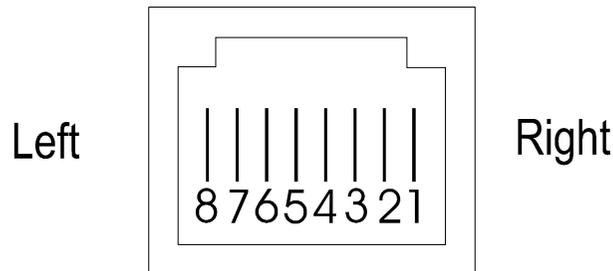
*shielded RJ45  
pinouts RJ45  
pinouts  
(serial ports)*

Pin	Circuit	Direction	Function
1	DCD	Input	Data Carrier Detect
2	DSR	Output	Data Set Ready
3	DTR	Input	Data Terminal Ready
4	S/GND	—	Signal Ground
5	TXD	Output	Transmit Data
6	RXD	Input	Receive Data
7	CTS	Output	Clear To Send
8	RTS	Input	Request To Send
Shield	P/GND	—	Protective (Chassis) Ground

Notes:

1. P/GND means Protective (Chassis) Ground
2. S/GND means Signal Ground

*Pin locations RJ45 connectors* The pins in all the RJ45 connectors (front and rear panels) are located at the bottom, with pin 1 on the right;



## AUI port

The port labelled AUI, on the rear panel on CS9000 with blue case, is a 15-way female D-type. Pinouts are:

*Note* To use the AUI port on Perle CS9000 units equipped with Revision 2 boards you need to select the AUI interface during initial configuration using CLI commands. See [Selecting AUI or 10/100 Base T interface on page 38](#).

Pin	Signal	Pin	Signal
1	Ground/chassis link	9	Collision-
2	Collision+	10	Data Out-
3	Data Out+	11	Ground
4	Ground	12	Data In-
5	Data In+	13	+12 volt
6	Ground	14	Ground
7	not used	15	not used
8	Ground		

## RJ45 10/100BaseT port

The RJ45 port on the *rear* panel, labelled '10/100BaseT' is 8-pin shielded RJ45. It is wired as shown in on page 136 the next table. The positions of the pins inside the connector are shown in *The pins in all the RJ45 connectors (front and rear panels) are located at the bottom, with pin 1 on the right; on page 134*. The pinouts are shown below .

Pin	Signal	Function
1	TXD+	Transmit Data+
2	TXD-	Transmit Data-
3	RXD+	Receive Data+
4	-	not used
5	-	not used
6	RXD-	Receive Data-
7	-	not usedt
8	-	not used

## Admin Port

The port labelled 'Admin' is on the rear of the unit. When fitted with a 25-pin female D-type connector the wiring is as follows:

Pin	Signal	Function
2	RXD	Receive
3	TXD	Transmit
7	S/GND	Signal Ground
all others	-	(do not connect)

If you wish to connect a terminal into the Admin Port, see the connection example in [Connecting to Terminals on page 144](#).

## Third party connection examples

This section provides examples of direct (1:1) connections. Defined as when a single length of cable joins the Perle device and your equipment, so there is *no* structured cabling system or any other connection in-between.

The following are included:

- [CS9000 to Sun Microsystem servers on page 139](#)
- [CS9000 RJ45 to Perle router DB25 console port on page 141](#)
- [CS9000 RJ45 to Perle router RJ45 console port on page 141](#)
- [CS9000 RJ45 to Cisco RJ45 cable with hardware flow control on page 141](#)
- [CS9000 RJ45 to Nortel switch DB25 cable on page 142](#)

### Notes:

1. Some user equipment need additional signals on the connector. These may not be supported by the Perle device or your cable. The normal way to overcome this is to loopback - on your equipment - one of the output lines to the required input. Refer to the documentation supplied with your equipment, or the supplier of the equipment, for information on which loop-backs, if any, are required.
2. Other than a specific requirement at your equipment (as in note 1), do not connect unused pins on either connector.
3. Protective Ground (P/GND) terminates on the connector and so does not have a pin number.

In this section we show example connections between Perle ports and the following devices:

## CS9000 to Sun Microsystem servers

### CS9000 RJ45 to DB9 IBM RS6000 com port

Perle CS9000			IBM RS6000 Com port	
RJ45			DB9	
2	DSR	-----	1	DCD
6	RXD	-----	3	TXD
5	TXD	-----	2	RXD
4	S/GND	-----	5	S/GND
8	RTS	-----	7	RTS
7	CTS	-----	8	CTS

### CS9000 RJ45 to DB25 Sun server

Here are the 2 main cable pinouts required to connect to Sun servers and work stations.

Perle CS9000			Sun server	
RJ45			DB25	
2	DSR	-----	6	DSR
3	DTR	-----	20	DTR
4	GND	-----	7	GND
5	TXD	-----	3	RXD
6	RXD	-----	2	TXD
7	CTS	-----	5&8	CTS ( 5 ) , DCD ( 8 )
8	RTS	-----	4	RTS

### CS9000 RJ45 to Sun server port DB9

Perle CS9000			Sun Server Port	
RJ45			DB9	
1	DCD	-----	4	DTR
3	DTR	-----	4	DTR
2	DSR	-----	1&6	DCD ( 1 ) , DSR ( 6 )
4	GND	-----	5	GND
5	TXD	-----	2	RXD
6	RXD	-----	3	TXD
7	CTS	-----	8	CTS
8	RTS	-----	7	RTS

## CS9000 RJ45 to Sun server Netra port RJ45

Perle CS9000 RJ45			Sun Server Netra T1 RJ45	
2	DSR	-----	7	DSR
3	DTR	-----	2	DTR
4	GND	-----	4	GND
5	TXD	-----	6	RXD
6	RXD	-----	3	TXD
7	CTS	-----	8	CTS
8	RTS	-----	1	RTS

## CS9000 RJ45 to Perle router DB25 console port

Perle CS9000 RJ45				Perle router DB25			
DSR	2	----->	20	DTR			
TX	5	----->	2	RX			
RX	6	<-----	3	TX			
GND	4	-----	7	GND			

## CS9000 RJ45 to Perle router RJ45 console port

Perle CS9000 RJ45				Perle router RJ45			
DSR	2	----->	3	DTR			
TXD	5	----->	5	RXD			
RXD	6	<-----	6	TXD			
GND	4	-----	4	GND			

## CS9000 RJ45 to Cisco RJ45 cable with hardware flow control

This example supports both DTR/DSR and RTS/CTS signalling for both routers and switches.

Perle CS9000 RJ45				Cisco Console port RJ45			
2	DSR	-----	7	DSR			
3	DTR	-----	2	DTR			
4	S / GND	-----	4	GND			
5	TXD	-----	6	RXD			
6	RXD	-----	3	TXD			
7	CTS	-----	8	CTS			
8	RTS	-----	1	RTS			

## CS9000 RJ45 to Nortel switch DB25 cable

Perle CS9000			Nortel switch	
RJ45			DB25	
1	DCD	-----	4	RTS
4	S/GND	-----	7	S/GND
5	TXD	-----	3	RXD
6	RXD	-----	2	TXD
8	RTS	-----	20	DTR

# Connecting to PC serial ports

PC, example connections, with a Perle RS232 RJ45 connector and a direct (1:1) connection to the PC (connection not through a structured cabling system), and using hardware flow control:

This section includes the following:

- [CS9000 RJ45 to DB9 PC Com port configuration on page 143](#)
- [CS9000 25-pin Admin port to a PC on page 143](#)

## CS9000 RJ45 to DB9 PC Com port configuration

Perle CS9000 RJ45			PC Com Port DB9		
1	DCD	-----	1	DCD	
2	DSR	-----	6	DSR	
3	DTR	-----	4	DTR	
4	S / GND	-----	5	S / GND	
5	TXD	-----	2	RXD	
6	RXD	-----	3	TXD	
7	CTS	-----	8	CTS	
8	RTS	-----	7	RTS	

1. If your PC is fitted with a DB25 connector, use the same DB25 pinouts as for modems, shown in [Connecting to Modems on page 148](#).
2. We assume you are connecting your PC directly to the Perle device (no structured cabling system).
3. In addition to the signals shown in the examples above, you may connect Protective Ground (P/GND) if you have shielded twisted-pair (STP) cable. Connect P/GND at *either* your equipment *or* the Perle device (but not both). P/GND will reduce interference in noisy environments.
4. The application of the connection example is a PC running terminal emulation software set to 'hardware flow control'.

## CS9000 25-pin Admin port to a PC

Perle 25-pin Admin Port DB25			PC DB9		
	TXD	3	----->	2	RXD
	RXD	2	<-----	3	TXD
	GND	7	-----	5	GND

## Connecting to Terminals

This section details the cabling used for connecting to terminals and includes the following;

- [CS9000 RJ45 to DB25 terminal with hardware flow control on page 145](#)
- [CS9000 RJ45 to DB25 terminal using the modem device on page 145](#)
- [CS9000 25-pin Admin port to a terminal on page 147.](#)

## CS9000 RJ45 to DB25 terminal with hardware flow control

For terminals operating at speeds high than 9600 baud or for terminals which do not support software flow control. Terminal supports DTR flow control.

Perle CS9000			Terminal	
RJ45			DB25	
4	S / GND	-----	7	S / GND
5	TXD	-----	3	RXD
6	RXD	-----	2	TXD
7	CTS	-----	5	CTS
8	RTS	-----	20	DTR

## CS9000 RJ45 to DB25 terminal using the modem device

### Flow control disabled

Using the modem device on a local connection ensures that the login process is killed when the terminal is switched off. This is achieved by wiring the terminals RTS or DTR to the RJ45 DCD.

Perle CS9000			Terminal	
RJ45			DB25	
1	DCD	-----	20 or 4	DTR ( 20 ) or RTS ( 4 )
4	S / GND	-----	7	S / GND
5	TXD	-----	3	RXD
6	RXD	-----	2	TXD
		-----		

### Hardware flow control enabled

Using the modem device on a local connection ensures that the login process is killed when the terminal is switched off. This is achieved by wiring the terminals RTS to the RJ45 DCD

Perle CS9000			Terminal	
RJ45			DB25	
1	DCD	-----	20 or 4	DTR ( 20 ) or RTS ( 4 )
4	S / GND	-----	7	S / GND
5	TXD	-----	3	RXD
6	RXD	-----	2	TXD
8	RTS	-----	20	DTR

This example assumes that DTR on the terminal is being used for hardware flow control. If RTS is used for hardware flow control connect DTR on the terminal to DCD on the RJ45 and RTS on the terminal to RTS on the RJ45.

## CS9000 to Terminals - slow speed or using software flow control

For a standard terminal operating at slow speeds, or using software flow control, a simple 3-pin connection can be used:

CS9000 RS232				Terminal	
RJ45				DB25	
RXD	6	<-----	2	TXD	
TXD	5	----->	3	RXD	
S / GND	4	-----	7	S / GND	

Notes:

1. In addition to the signals shown in the examples above, you may connect Protective Ground (P/GND) if you have shielded twisted-pair (STP) cable. Connect P/GND at *either* your equipment *or* the Perle device (but not both). P/GND will reduce interference in noisy environments.

## CS9000 25-pin Admin port to a terminal

Perle CS9000 Admin Port				Terminal	
DB25				DB25	
TXD	3	----->	3	RXD	
RXD	2	<-----	2	TXD	
GND	7	-----	7	GND	

For a terminal operating at speeds faster than 9600 baud, or for a terminal which cannot use xon/xoff flow control, the following connections are required:

Perle device				Terminal	
RS232 RJ45				DB25	
RXD	6	<-----	2	TXD	
TXD	5	----->	3	RXD	
RTS	8	<-----	4 or 20	RTS or DTR	
*CTS	7	----->	5	*CTS	
S/GND	4	-----	7	S/GND	

### Notes:

1. In addition to the signals shown in the examples above, you may connect Protective Ground (P/GND) if you have shielded twisted-pair (STP) cable. Connect P/GND at *either* your equipment *or* the Perle device (but not both). P/GND will reduce interference in noisy environments.
2. \* asterisk denotes that you connect CTS to CTS only if input flow control (from the Terminal to the Perle device) is required.

# Connecting to Modems

This section details the cabling used to connect to modems and includes the following;

- [CS9000 RJ45 to DB25 modem cable configuration on page 148](#)
- [CS9000 RJ45 to DB9 modem cable configuration on page 148](#)

## CS9000 RJ45 to DB25 modem cable configuration

Perle CS9000			Modem	
RJ45			DB25	
1	DCD	-----	8	DCD
2	DSR	-----	20	DTR
3	DTR	-----	6	DSR
4	S / GND	-----	7	S / GND
5	TXD	-----	2	TXD
6	RXD	-----	3	RXD
7	CTS	-----	4	RTS
8	RTS	-----	5	CTS

## CS9000 RJ45 to DB9 modem cable configuration

Perle CS9000			Modem	
RJ45			DB9	
1	DCD	-----	1	DCD
2	DSR	-----	4	DTR
3	DTR	-----	6	DSR
4	S / GND	-----	5	S / GND
5	TXD	-----	3	TXD
6	RXD	-----	2	RXD
7	CTS	-----	7	RTS
8	RTS	-----	8	CTS

## Loopback cable on CS9000 RJ45 serial port

This section details the loopback cable used for testing a CS9000 RJ45 serial port.

DCD	1	---
DSR	2	---
DTR	3	---
TXD	5	---
RXD	6	---
CTS	7	---
RTS	8	---



# Appendix B The CLI commands

*You need to read this appendix if you want information on the Perle CS9000 Command Line Interface (CLI).*

*you want to...* This appendix provides descriptions of each Command Line Interface (CLI) command.

This appendix includes the following sections;

- [CLI commands on page 152.](#)



## add gateway

*user level:* This command enables you to define the gateways in your network. You can add up to twenty gateways and these must be hosts that you have defined in the host table.

*admin*

*Syntax*            `add gateway hostname type [inetaddress][netmask]`

Where:

<i>hostname</i>	is the name of the host that you want to define as a gateway
<i>type</i>	is the gateway type: default, host or network. The types are: <ul style="list-style-type: none"><li>• <b>Default</b> - this is a gateway which provides general access beyond your local network.</li><li>• <b>Host</b> - this a gateway reserved for accessing a specific host external to your local network.</li><li>• <b>Network</b> - this is a gateway reserved for accessing a specific network external to your local network.</li></ul>
<i>inetaddress</i>	if you define the type as host or network, you must define the internet address of the target host or network.
<i>netmask</i>	dotted decimal value which specifies the destination network mask. If not defined, the mask will be derived from the class of <i>[inetaddress]</i> . Only valid for network type gateways.

Your gateway by default is 'active'; you can change it to 'passive'; see the command `set gateway`.

*Menu equivalent* Network Configuration - Gateway - Add Gateway

*See also*            [delete gateway](#), [set gateway](#)

## add host

*user level:* This command enables you to add the details of the other hosts in your network. These will be added to the host table. You can also add hosts accessed frequently not in your LAN.

*admin*

*Syntax*            `add host hostname inetaddress`

Where:

<i>hostname</i>	is the name of the host (14 characters maximum).
<i>inetaddress</i>	is the internet address of the machine.

*Menu equivalent* Network Configuration - Host Table - Add Host

*See also*            [delete host](#), [set host](#)

## add modem

*user level:* Use this command to add modem details to the unit. You will want to add modems which you want the unit to control.

*admin*

*Syntax*                    add modem *name*        *init\_string*

Where:

<i>name</i>	is the name of your modem, e.g. usrobotics28.8, or a name you wish to use, e.g. modem4. Do not enter spaces in the name; use the underscore _ character; e.g. us_robotics_28.8
<i>init_string</i>	is the initialisation string of the modem; see your modem's documentation.

*Menu equivalent* Line Configuration - Modems - Add Modem or Change Modem

*See also:*            [delete modem](#), [show port\\_buffering](#)

**Note**            *To change modem details in the cli you must 'delete' the modem, then 'add' it again, with the changed details.*

## add radius

*user level:* Use this command to add RADIUS authentication and accounting hosts to the unit.

*admin*

*Syntax*                    add radius *host type*    *host name* *secret*

Where:

<i>host type</i>	is either <code>authentication_host</code> or <code>accounting_host</code>
<i>hostname</i>	is the name of the RADIUS host
<i>secret</i>	is the secret (password) shared between the unit and the RADIUS host.

**Note**            *You must have the host already entered in the unit's host table; see [add host on page 153](#). If not you will see a message saying that no host is configured.*

*Menu equivalent* radius configuration - add authentication host

radius configuration - add accounting host

*See also:*            [delete radius](#), [set radius](#), [set server](#), [show radius](#)

## add rip md5

*user level:* Use this command to add RIP MD5 key entry.

*admin*

*Syntax*                    `add rip md5 [id] [start_date] [start_time] [end_date] [end_time]`

Where:

<i>id</i>	ID for the MD5 key
<i>start_date</i>	Start date for the MD5 key to be in effect. Format is <i>dd/mm/yyyy</i> .
<i>start_time</i>	Start time for the MD5 key to be in effect. Format is <i>hh:mm:[ss]</i>
<i>end_date</i>	End date for the MD5 key. Format is <i>dd/mm/yyyy</i> .
<i>end_time</i>	End time for the MD5 key. Format is <i>hh:mm:[ss]</i>

**Note**     *To add a MD5 key entry all parameters must be entered. After ENTER is pressed, the user will be prompted for the key string and then prompted again for the key string for verification.*

*Menu equivalent* Network configuration- RIP - MD5

*See also:*         [delete rip md5](#)

## add trap

*user level:* Use this command to define communities which will receive trap messages generated by the unit. Note that the unit does not generate any enterprise-specific traps. Up to four trap communities may be defined.

*admin*

*Syntax*                    `add trap trap_name inetaddress`

Where:

<i>trap_name</i>	is an arbitrary name assigned to the community.
<i>inetaddress</i>	is the internet address that identifies the host(s) in the community.

## add sntp server

*user level:* Use this command to define SNTPserver which will communicate to the CS9000 to synchronize its internal clock. Both a primary and secondary server can be defined.

*admin*

*Syntax*                    `add sntp server_1 server1 server_2 server2`

Where:

<i>server1</i>	is the name of the primary SNTP server from the host table
<i>server2</i>	is the name of the secondary SNTP server from the host table.

## add user

*user level:* This command enables you to add a new user to the system. You will be prompted to enter a password (maximum sixteen characters). You must also set the user's level using the `set user` command.

*admin*  
*Syntax*            `add user username`

Where *username* is the required login name (maximum sixteen characters).

*Menu equivalent* Users - Add User

*See also*            [delete user](#), [set user](#), [show timezone](#)

## add WINS

*user level:* This command enables you to define the WINS (Windows Internet Naming Service) host or hosts in your network. You can define a maximum of two hosts. If you wish, it/they can be the same address(es) as a machine(s) already entered in the unit host table.

*Syntax*            `add WINS internet_address`

Note 'WINS' must be entered in upper case. Also:

*internet address* is the internet address of your machine providing the WINS; enter the address in dot decimal notation.

*Menu equivalent* Network Configuration - WINS - Add WINS

*See also*            [delete WINS](#), [add DNS](#), [show server](#)

## admin

*user level:* If you are a normal user, this command enables you to enter Admin mode. But only if you know the admin password. This will give you full access to the unit's commands. The unit's prompt will change to a hash or pound sign (JS\_8500# or JS\_8500£) to indicate that you are in admin mode. You must log out and back in again to revert to your original mode.

*normal*  
*Syntax*            `admin`

## debug

*level of user:* This command will send debug information to the screen. You can be connected to either the Admin port or a front-mounted port. Use this command only when instructed by your Technical Support.

*admin*  
*Syntax*            `debug`

*Menu equivalent* (none available)

## delete ARP

This command enables you to delete the ARP table. This is useful for diagnostic and debugging purposes.

This command is only available from the CLI.

*Syntax*            `delete arp`

*See also*          [show ARP](#)

## delete community

*user level:*        This command enables you to delete SNMP communities defined using the `add community` command.

*admin*  
*Syntax*            `delete community 1 | 2 | 3 | 4`

Communities are numbered according to the order they are created in. You can list them using the `show snmp` command.

*See also*          [add community](#), [delete snmp server\\_1](#), [show snmp](#)

## delete DNS

*user level:*        This command enables you to delete the DNS (Domain Name Service) host or hosts in your network.

*admin*  
*Syntax*            `delete DNS internet_address`

Note 'DNS' must be entered in upper case. Also:

*internet address* is the internet address in dot decimal notation. If you cannot remember the address type a space and then a question mark after DNS; e.g. `del DNS ?`  
The unit will list the ip addresses of DNS machines entered in its DNS table. Type the ip address.

*Menu equivalent* Network Configuration - DNS - delete DNS

*See also*          [add DNS](#), [delete WINS](#), [show server](#)

## delete gateway

*user level:*        This command enables you to delete a gateway. The host will not be deleted from the host table.

*admin*  
*Syntax*            `delete gateway hostname`

*Menu equivalent* Network Configuration - Gateways

*See also*          [add gateway](#), [set gateway](#), [show gateways](#)



## delete rip md5

*user level:* Use this command to remove RIP MD5 key entry.

*admin*

*Syntax*                    `delete rip md5 [id]`

Where:

*id*                                    ID for the MD5 key

*Menu equivalent* Network configuration- RIP - MD5

*See also:*            [add rip md5](#)

## delete sntp server\_1

*user level:* Use this command to remove an SNTP server which that communicates to the CS9000 to synchronize its internal clock. Both a primary and secondary server can be removed.

*admin*

*Syntax*                    `delete sntp server_1 server_2`

## delete trap

*user level:* This command enables you to delete SNMP trap communities defined using the `add trap` command.

*admin*

*Syntax*                    `delete trap 1 | 2 | 3 | 4`

Communities are numbered according to the order they are created in. You can list them using the `show snmp` command.

*See also*            [add trap](#), [delete community](#), [show snmp](#).

## delete user

*user level:* This command enables you to delete a user. You cannot delete the following: the default admin user, users that are logged in or users whose line is dedicated to them.

*admin*

*Syntax*                    `delete user username`

*Menu equivalent* Users - [delete user](#)

*See also*            [add user](#), [set user](#), [show timezone](#)

## delete WINS

*user level:* This command enables you to delete the WINS (Windows Internet Naming Service) host or hosts in your network.

*admin*  
*Syntax*            `delete WINS internet_address`

Note 'WINS' must be entered in upper case. Also:

*internet address* is the internet address in dot decimal notation. If you cannot remember the address type a space and then a question mark after WINS; e.g. del WINS ?  
The unit will list the ip addresses of WINS machines entered in its WINS table. Type the ip address.

*Menu equivalent* Network Configuration - WINS - delete WINS

*See also*            [add WINS](#), [delete DNS](#), [show server](#)

## heap

*user level:* This command tells you how much free memory currently exists and the largest available fragment.

*admin*  
*Syntax*            `heap`

## help

*all users*            The *help* command displays a brief description of how to use the Command Line:

```
Type ? at any time to list possible options
(e.g. set user?)
```

*Syntax*            `help`

## kill line

*user level:* This command can be used to kill the processes on a *serial* line.

*admin*  
*Syntax*            `kill line n`

Where *n* is the line that you want to kill.

*Menu equivalent* Line Configuration - Kill Line

*See also*            [reset line](#), [restart](#)

## logout

*user levels:*        This command logs you off the unit. You won't be allowed to log out if you still have sessions running.

*all users*

*Syntax*                `logout`

*Menu equivalent*    Sessions - Logout

*See also*             [kill line](#)

## netload

*user level:*

*admin*

*Syntax*

This command allows you to download a file over a network from a host using TFTP. The file can be one of several types; e.g. a configuration file of another unit. The list of file types is shown below.

```
netload [nowrite] filetype hostname filename
```

where you replace the word 'filetype' with one of the following words:

configuration	a configuration file of a unit
term1	the first of your extra terminal definition files
term2	the second of your extra terminal definition files
term3	the third of your extra terminal definition files
software	a new version of a unit's software

*and where:*

hostname	is one from the list of hosts defined in the unit's host table. Type ? to show the host table entries. Select a host by typing its name, e.g. aristotle.
filename	must include the path to the file e.g. /etc/xxxx/config/... The path/filename must start with the 'forward slash' / character; do <i>not</i> specify a drive letter.  For terminal definition files, the unit will refer to your filename (after downloading) as either 'term1' 'term2' or 'term3'.
nowrite	is an optional parameter which allows you to put the downloaded file into RAM without a write to FLASH memory. You must type the word 'nowrite' immediately after 'netload' (separated by a space). Subsequently you can save the file to FLASH by re-using the netload command <i>without</i> the 'nowrite' option.

During and/or after download you will see status messages at the command line, e.g.

```
TFTP: transfer succeeded
```

**Note** *you can configure TFTP in the unit; see the command `set server`.*

The downloaded files will take effect as follows:

configuration	immediately after successful download. When you continue to use the cli or menus, you will be using the new configuration
term1, term2 and term3	
software	when you reboot the unit. See <a href="#">reboot on page 165</a>

If you have used the 'nowrite' option and you now wish to discard this file in RAM and revert to the original file in FLASH, you must reboot the unit. Use the cli command `reboot`.

*Menu equivalent* (none available)

*See also* [netsave](#), [reboot](#), [set server](#)

## netsave

*user level:*  
*admin*

This command enables you to save two types of information to a file on a remote host: the configuration of your unit and crash details.

Configuration information

The following information will be saved:

User Profiles, including passwords

Port Configuration

Host Table

Gateways

RADIUS details

Modems

SNMP

Information unique to this unit (name, IP Address, Subnet mask) will not be saved. Make sure you have write permission to the file. You can use this configuration file to configure other units. The configuration can subsequently be reloaded using the `netload` command.

Crash information

When the unit has rebooted after a crash you can save crash information to a file on a remote host. This information will be diagnostic data for use by Technical Support personnel.

*Syntax:*

```
netsave type hostname filename
```

where you replace the word 'type' with one of the following words:

configuration	the configuration of your unit
crash	information associated with the last crash of the unit

and where

hostname	is one from the list of hosts defined in the unit host table. Type ? to show the host table entries. Select a host by typing its name, e.g. aristotle.
filename	must include the path to the file e.g. /etc/xxxx/config/...

*Menu Equivalent:*(not available)

*See Also:* [netload](#), [save](#)

## ping

*all users*

If you are having trouble accessing a host, try the *ping* command. This tries to elicit a response from the specified host. If successful, a report similar to the following will be generated:

```
# ping socrates

PING socrates (192.101.34.1): 100 data bytes
108 bytes from 192.101.34.1: icmp.seq=0. time=15. ms
108 bytes from 192.101.34.1: icmp.seq=1. time=12. ms

- - - socrates PING statistics - - -
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms) min/avg/max = 12/12/15
```

You can interrupt the process by pressing any key.

If the hostname cannot be resolved, the following message will be displayed:

```
Ping: hostname: Host not found
```

If the host has been resolved, but the network it is on is unreachable, the following output will be generated:

```
ping hostname/inetaddress 100 data bytes

ping: t_rcvudata: ENETUNREACH - Network is
unreachable
```

If the host has been resolved, but it isn't answering, the following will be displayed:

```
ping hostname/inetaddress 100 data bytes

10 packets transmitted, 0 packets received,
100% packet loss.
```

*Syntax*

```
ping hostname/inetaddress [packet_size] [packets_sent]
```

Where:

<i>hostname/</i> <i>inetaddress</i>	is the hostname or internet address of the machine that you want to ping.
<i>packet_size</i>	is the size of packet sent (default = 100 bytes).
<i>packets_sent</i>	is the number of packets sent (default = 10).

## reboot

*user level:* This command will reboot the unit. You will be asked to confirm the reboot with the following prompt:  
*admin*

```
save config to flash ROM y/n
```

If you press 'y' the unit will save your configuration, close all connections and then reboot. If you press 'n' the unit will prompt you:

```
confirm reboot unit y/n
```

Press 'y' to reboot, 'n' to cancel.

For more information on how the unit reboots, see BOOTP, [Appendix F BOOTP](#).

Rebooting does not reset the unit to factory default settings.

*Syntax*            reboot

*Menu equivalent* Network Configuration - Reboot Server

*See also*           [show server](#)

## reset factory

*user level:* This command will reset the unit to its default values. The unit will save the factory default settings to FLASH memory; this saving will take a few seconds. After this period you will be logged out and presented with a new login prompt.

*Syntax*            reset factory

*Menu equivalent* Network Configuration - Reset

*See also*           [reboot](#)

## reset line

*user level:* This command will reset the specified serial line(s) to the default line configuration.

*admin*

*Syntax*            reset line ./n/\*

Where:

.	specifies the current line.
<i>n</i>	is a specific serial line number.
*	specifies all serial lines.

*Menu equivalent* Line Configuration - Line Port Settings - Quit form

*See also*           [kill line](#), [restart](#), [show line](#), [set line](#)

## reset user

*user level:* This command will reset the specified user(s) to the default user settings. This sets the user level to 'normal' and the screen switch character to '1'. Any predefined sessions are switched off. The default admin user will not be reset.

*Syntax*            `reset user ./*/username`

Where:

.	specifies the current user.
<i>username</i>	is the name of a specific user.
*	specifies all users.

*See also*        [reboot](#)

## restart

*user level:* When there is insufficient free memory to start a login or virtual circuit on a line, that line will appear dead and you will be unable to restart it. You must wait until sufficient memory is available and then restart all such lines using this command. You can enter the command on any active serial line. The execution of the command will affect halted processes on all lines, both serial and parallel.

*Syntax*            `restart`

*Menu equivalent* (none available)

*See also*        [heap](#), [kill line](#)

## resume

*user level:* The resume command enables you to resume any session that you have left running. You will be returned to your last position in a session.

*all users*

*Syntax*            `resume n`

Where *n* is the session you want to resume.

*Menu equivalent* Sessions - Resume Session

*See also*        [start](#)

## rlogin

*user level:* *admin, normal* This command will establish a connection with a host using the rlogin protocol. Rlogin passes your login name to the host, so you are prompted for your password only. If your unit's login name exists in the 'rhost' file of the target login directory, you won't be prompted for a password. You will be logged straight in.

*Syntax* `rlogin hostname/inetaddress [termttype termttype] [user username]`

Where:

<i>hostname/ inetaddress</i>	is the hostname or internet address of the machine you want to log into.
<i>termttype</i>	is your terminal type. By default a dumb terminal type is passed to the host. When connecting to a UNIX host, you must define the termttype in accordance with its UNIX TERM variable.
<i>username</i>	is your login name on the target host if different to your unit's login. You can also use this argument to log in as someone else.

*Menu equivalent* Sessions - Start telnet/rlogin

*See also* [resume](#), [show line](#), [start](#), [telnet](#)

## save

*user level:* *admin* This command enables you to save the configuration information of your unit to FLASH (permanent, non-volatile) memory. Note that the save command does not apply to language files or any other files downloaded into RAM using the netload command. The writing to FLASH will take a few seconds and during this time the unit will not respond to user input.

---

### WARNING

do not turn the power on/off while the unit is writing to FLASH memory.

*Syntax:*

`save`  
*See also* [netload](#), [netsave](#)

## screen

*user level:* *admin* This command will change you from Command Line mode to Full Screen mode (on supported terminal types only).

*Syntax* `screen`

## set contact

*user level:* This command enables you to configure the SNMP sysContact object.

*admin*

*Syntax*            `set contact contact_name`

Where *contact\_name* is a string representing your contact name; it cannot contain spaces (e.g. john.smith, john\_smith or johnsmith)

*See also*            [set location](#), [show snmp](#)

## set date

*user level:* This command enables you to set the date in the unit. The date is used by the real-time clock. For more information on the real-time clock see Perle CS9000, [Setting date and time on page 67](#).

*admin*

*Syntax*            `set date dd/mm/yyyy`

for example; set date 05/12/2000

*Menu equivalent* Main Menu - hardware

*See also*            [set time](#)

## set ethernet interface RJ45

*user level:* This command enables you to select the RJ45 10/100Base-T interface on the CS9000 with blue case.

*admin*

### Syntax

```
set ethernet interface RJ45
```

### See also

[set ethernet interface AUI](#), [show hardware](#)

## set ethernet interface AUI

**user level:** This command enables you to select the AUI interface on CS9000 with blue case.  
**admin**

### Syntax

```
set ethernet interface AUI
```

### See also

[set ethernet interface RJ45](#), [show hardware](#)

## set gateway

**user level:** This command enables you to redefine a gateway.  
**admin**

**Syntax** `set gateway hostname status type [inetaddress][netmask]`

Where:

<i>hostname</i>	is the name of the gateway.
<i>type</i>	is one of 'default', 'host' or 'network'.
<i>inetaddress</i>	is the internet address of the target host or network.
<i>netmask</i>	dotted decimal value which specifies the destination network mask. If not defined, the mask will be derived from the class of <i>[inetaddress]</i> . Only valid for network type gateways.
<i>status</i>	is one of: 'active' or 'passive'.

**Menu equivalent** Network Configuration - Gateway - Change Gateway

**See also** [add gateway](#), [delete gateway](#), [show gateways](#)

## set host

**user level:** Use this command if you need to change the internet address of one of the hosts in your host table.  
**admin**

**Syntax** `set host hostname inetaddress`

**Menu equivalent** Network Configuration - Host Table - Change Host

**See also** [add host](#), [delete host](#), [show hosts](#)

## set line

*user levels:*  
*admin, normal*

Use this command to configure lines on the front-mounted RJ45 ports only. The command cannot set: the Admin Port line configuration; this is fixed.

An admin user can change the setup of any line; a normal user can change their own line only. On login connections, changes to the terminal type or number of video pages will take effect immediately. Other changes will take effect when a user next logs in on the line.

*Syntax*

```
set line line_number
[speed speed]
[parity parity]
[stop stop-bits]
[data data-bits]
[flow flow-control]
[pages pages]
[termttype term-type]
[dial dial-status]
[user user-name]
[nouser]
[service line_service]...followed by (optionally)
[raw/telnet/ssh][raw/telnet] [hostname][cs_port][host_port]
[phone_number phone-number]
[modem_name modem-name]
[idle_timer i-timer value]
[session_timer s-timer value]
[security security]
[line_name line-name]

[multisessions number]
```

Where:

*line\_number* may also be specified as '\*' for all lines or '.' for the line currently being used.

*speed, parity, stop-bits, data-bits, flow control* are standard line settings

*pages* (for 'cslogin' line service) is the number of video pages the terminal supports.

*term-type* is the type of terminal attached to this line; e.g. ansi. Note this value will be ignored if you have set a termttype value using the command `telnet`.

*dial-status* use when a modem is attached to a port; set to 'in' or 'out' (default none). Note that 'dial-status' is unrelated to the User 'callback' parameter.

*user-name* (for `cslogin` line service) can be used to dedicate the line to a specific user. Only this user will be able to log in on this line and they won't need to enter their login name - just their password.

*nouser* (for `cslogin` line service) nullifies the user argument; it enables any user to log in on this line.

- line-service* select from one of: cslogin, direct, silent, reverse, bidir, slip or ppp.  
for remote access connections, see [Setting up the line on your Perle CS9000 on page 72](#),  
when you select ‘direct’, ‘silent’ or ‘reverse’, you must specify whether the line service is ‘raw’, ‘telnet’ or ‘ssh’; e.g. silent telnet.  
when you select ‘direct’, ‘silent’ or ‘bidir’, you must enter the target host name; e.g. sophocles.  
when you select ‘direct raw’, ‘silent raw’ or ‘bidir’, you must specify the TCP port assigned on the target host to listen for the incoming connection.  
when you select ‘reverse raw’, ‘reverse ssh’, ‘reverse telnet’ or ‘bidir’, you must specify the TCP port assigned to the unit’s port (that is the Perle CS9000 TCP port number). TCP/IP hosts will use this TCP port to establish a connection with the unit. Setting the port to 0 will disable direct connect access to the device on that port. Easy Port Access menu is still available.
- phone-number* a number which the unit will dial on that line, when ‘dial’ is set to ‘out’. Enter the number without spaces. To change the phone number overwrite the previous entry.
- modem-name* is the name of the attached modem; e.g. usrobotics28.8, or a name you wish to use, e.g. modem 1. Do not enter spaces in the name; use the underscore \_ character; e.g. us\_robotics\_28.8. You can enter a total of nineteen alphanumeric characters (including spaces).
- i-timer value* enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of inactivity. When the idle timer expires, if there has been no exchange of data, the unit will end the connection. The default value is 0 (zero), meaning that the idle timer will not expire (the connection is open permanently).  
This idle timer will be overridden by the idle timer which you can configure for a user; i.e. the user idle timer takes precedence, with the exception of reverse telnet or reverse SSH sessions.
- s-timer value* enter a period in seconds for which the session timer will run. Use this timer to forcibly close the session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until you kill the line or you/the user log(s) out).  
This session timer will be overridden by the session timer which you can configure for a user; i.e. the user session timer takes precedence, with the exception of reverse SSH or reverse Telnet sessions.
- security* This may be set to on or off to enable login/password authentication on reverse telnet and other reverse type connections. The unit’s stored user database is always used for this authentication. The default setting is **off**.

<i>line-name</i>	Name to help identify the line. Do not enter spaces. The Remote Port Buffering feature uses this line name instead of the default when creating a file on the remote NFS server. Easy Port Access menu also uses the line name to unique identify the line on the connection menu.
<i>multisession</i>	To enable the multisession functionality on the unit specific the number of multisession permitted on the particular line. The number of multisessions permitted is 0 (disabled) to 124 (maximum number of session per unit).

Any number or combination of the arguments can be used.

Examples:

```
set line 6 service silent telnet plato
set line 3 service reverse raw 1000
set line 9 speed 38400 modem in service bidir
homer 1000 900
```

You can set all lines to the same parameters by using the \* asterisk character, e.g.

```
set line * speed 38400 dial in
```

will set all lines to this speed and dial values.

*Menu equivalent* Line Configuration - Line Settings

*See also* [show line](#), [add modem](#),

## set location

*user level:* This command enables you to configure the SNMP sysLocation object.

*admin*

*Syntax* `set location location`

*See also* [set contact](#), [show snmp](#)

## set port\_buffering

*user level:* This command enables you to setup and define the port buffering configuration.

*admin*

*Syntax*

```
set port_buffering
[mode mode]
[view_port_buffer_string string]
[nfs_host hostname]
[nfs_dir directory]
[nfs_encryption state]
[time_stamp time_stamp_mode]
```

Where:

<i>mode</i>	The <b>mode</b> field can enable/disable Local or Remote Port Buffering feature or both. This field is disabled by default
<i>string</i>	The <b>view port buffering</b> string is a configurable string that allows a session connected to a serial port to display or view the port buffer for that particular serial port. The default string is <b>~view</b> .
<i>hostname</i>	The <b>nfs host</b> hostname field specifies the hostname that the console server will use as a remote NFS host for its Remote Port Buffering feature. The console server will open a file on the NFS host for each reverse SSH or reverse Telnet line, and send any port data to be written to those files. The default will be the first host defined in the host table. To setup host see <a href="#">Setting up the host table on page 51</a> . This field will only be used when port buffering is set to Remote or Both indicating that the Remote Port Buffering feature is enabled.
<i>directory</i>	The <b>nfs directory</b> field defines the directory and/or subdirectories in which the Remote Port Buffering files will be created. This field will only be used when port buffering is set to Remote or Both indicating that the Remote Port Buffering feature is enabled. For multiple console servers using the same NFS host, it is recommended that each console server has its own unique directory to house the remote port log files. The default is /cs9000/portlogs.
<i>state</i>	The <b>nfs encryption</b> state option determines if the data sent to the NFS host will be sent encrypted or in the clear across the LAN. To encrypt the data, this option needs to be enabled or set to <b>On</b> . The default is set of <b>Off</b> .  <b>NOTE:</b> When the nfs encryption is enabled the Decoder utility software is required to be installed on the NFS host for decrypting the data to a readable format.
<i>time_stamp_mode</i>	Enable ( <b>on</b> ) or disable ( <b>off</b> ) time stamping of port buffered data. Default is off.

*Menu equivalent* Network Configuration - Port Buffering Configuration

## set ppp line

*user level:* Use this command to configure PPP on a line.

*admin*

*syntax*

```
set ppp line line_number parameter
```

where: line\_number may also be specified as \* for all lines, or . for the current in-use line.

parameters are any from the list below:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
accm	asynchronous character control map
mru	maximum receive unit
security	security
user	user
password	password
ruser	remote user
rpassword	remote password
ac_comp	address/control compression
proto_comp	protocol compression
vj_comp	VJ compression
magic_neg	magic number negotiation
ipaddr_neg	ip address negotiation
cr_tmout	'configure request' timeout
tr_tmout	'terminate request' timeout
cr_retry	'configure request' retries
tr_retry	'terminate request' retries
nak_retry	'configure nak' retries
auth_tmout	authentication timeout

The meanings and values of these parameters are explained in [Introduction to SLIP and PPP connections on page 75](#).

You can include multiple parameters in one line of syntax.

*Menu equivalent* Line Configuration - PPP

*See also* [show port\\_buffering](#)

## set radius

*user level:* Use this command to set RADIUS settings of the unit:

*admin*

*Syntax*                    `set radius <parameter>`

Type a question mark ? at the command line prompt to see a list of the parameters. You can enter multiple parameters on one line.

*Menu equivalent* radius configuration- radius settings

*See also*                [add radius](#), [show radius](#), [set server](#)

## set rip

*user level:* This command enables you to setup and define the rip networking parameters.

*admin*

*Syntax*

```
set rip
[ethernet_mode mode]
[send send_mode]
[receive receive_mode]
[authentication type]
[password]
[md5<id> start <start_date><start_time>
end<end_date><end_time> key]
```

Where:

<i>mode</i>	The <b>mode</b> field can enable/disable the RIP mode for the ethernet interface. Valid modes include: <b>none</b> , <b>send</b> , <b>listen</b> and <b>send_and_listen</b>
<i>send_mode</i>	The <b>send</b> mode is the send RIP protocol for all interfaces. Valid modes include: <b>rip_v1</b> , <b>v1_compatible</b> or <b>rip_v2</b> .
<i>receive mode</i>	The <b>receive</b> mode is the receive RIP protocol for all interfaces. Valid modes include: <b>rip_v1</b> , <b>rip_v2</b> or <b>both</b> .
<i>type</i>	The <b>authentication</b> mode for the ethernet interface (PPP and SLIP interfaces are always no authentication). Valid authentication types include:  <b>none:</b> no authentication  <b>password:</b> password authentication.  <b>md5:</b> md5 authentication using configurable MD5 keys (see add rip).
<i>id</i>	Identification id for the MD5 key entry
<i>start_date</i>	Start date for the MD5 key to be in effect. Format is <i>dd/mm/yyyy</i> .
<i>start_time</i>	Start time for the MD5 key to be in effect. Format is <i>hh:mm:[ss]</i>

*end\_date* End date for the MD5 key. Format is *dd/mm/yyyy*.  
*end\_time* End time for the MD5 key. Format is *hh:mm:[ss]*

**Note** If *set rip password* is entered the user is prompted for the password and re prompted for password verification.

**Note** If the key parameter is entered with the MD5 and ENTER is pressed, the user will be prompted for the key string and then prompted again for the key string for verification.

Menu equivalent Network Configuration - RIP - RIP Settings

See also [add rip md5](#), [delete rip md5](#)

## set server

*user level:* Use this command to configure the home setup of the unit.

*admin*

*Syntax*

```
set server
```

```
[name server-name]
[internet inet-address]
[subnet subnet]
[broadcast broadcast]
[domain domain]
[ip_host user-iphost]
[authentication auth-method]
[tftp retry retry-value]
[tftp timeout timeout-value]
[security security-status]
[dhcp dhcp-status]
[ssh-protocol ssh-protocol-status]
[gui_access gui-status]
[banner banner-status]
[OEM-mode mode-flags]
[services XXXX]
[break break-status]
[ssh_break_string ssh-string]
[session_escape_string escape-string]
[reverse_session_limit rev-session-value]
[line_menu_string line-menu-string]
[prompt_with_name prompt-status]
```

Where:

*server-name* The **name** string *server-name* configures the name of the unit. The name can be a maximum of 14 characters. After this action, you must reboot the unit; use the command `reboot`.

*inet-address* The **internet** field configures the internet address of the unit. After this action, you must reboot the unit afterwards; use the command `'reboot'`.

<i>subnet</i>	The <b>subnet</b> field configures the subnet mask of your network. For information on the subnet mask parameter, see <a href="#">General installation procedure on page 32</a> .
<i>broadcast</i>	The <b>broadcast</b> field configures the broadcast address. Once you have entered an IP address and subnet mask, the broadcast address will default to the IP address with the host part(s) set to 255. After this action, you must reboot the unit; use the command <code>reboot</code> .
<i>domain</i>	The <b>domain</b> field configures your domain name. After this action, you must reboot the unit; use the command <code>reboot</code> .
<i>user-iphost</i>	The <b>ip host</b> is the default ip host for all users who login to the unit. Enter an internet address in dot decimal notation; e.g. 192.101.34.202. The IP address entered here does not affect any line configuration.
<i>auth-method</i>	The <b>authentication</b> sets the authentication method for users, when they login to the unit; the method is <ul style="list-style-type: none"><li>• local - CS9000's local user database only</li><li>• both (local + RADIUS) - authenticated by local user database then RADIUS if required</li><li>• both (RADIUS + local) -authenticated by RADIUS host then the local user database if required.</li><li>• RADIUS - authenticated by the RADIUS host only.</li></ul>
<i>retry-value</i>	The <b>tftp retry</b> is the number of times the unit will attempt to transfer (using tftp) a file to/from a host. Enter a value between 0 and 255. The default value is 5. A value of 0 means that the unit will not attempt a retry should tftp fail.
<i>timeout-value</i>	The <b>tftp value</b> is the time in seconds the unit will wait for successful transmit or receipt of tftp packets before retrying a tftp transfer. Enter a value between 1 and 255. The default value is 3.
<i>security-status</i>	By enabling <b>security</b> , the CS9000 will restrict incoming connections to the source IP addresses that are configured host table. Regardless of the type of access (SNMP, reverse telnet, SSH, etc), all frames from any IP host NOT configured in the host table will be filtered/dropped if security is enabled. By not responding to unauthorised IP hosts (even pings), it prevents common IP/port mapping utilities from discovering the server's IP address and listening port information
<i>dhcp-status</i>	By enabling <b>dhcp</b> , the CS9000 allows a dhcp server to provide the configuration for the CS9000. The values are 'on' or 'off'; the default is 'off' (dhcp disabled).

*ssh-protocol-status* By enabling the **ssh protocol**, you allow secure ssh connections to be established across the LAN to a port device. The values that ssh-protocol-status can be set to are "disabled", "ssh-1", "ssh-2" and "both (ssh-1+ssh-2)".

By default, the ssh protocol is set to "disabled". By setting the ssh protocol to "ssh-1", ssh client connecting using SSH version 1 protocol will be allowed access. Encryption keys will only be generated for SSH version 1 which you will be prompted to generate. Similarly, encryption keys will only be generated for SSH version 2, when set to "ssh-2" and only ssh clients that connect using SSH version 2 protocol will be allowed access. Both sets of keys will be generated when setting ssh-protocol-status to "both (ssh-1+ssh-2)" and will support both SSH version 1 and 2 protocols.

NOTE: generation of keys can take several minutes depending upon the SSH version chosen. Key generation is only required once unless the CS9000 is reset back to a factory default state.

*gui-status* Use this parameter to control access to the unit's graphical configuration programme, JETset .

The default is 'off'. When set to 'on' the user with username 'admin' can access the JETset program from a Web browser, using the unit's internet address. Entry to the programme is controlled by password.

If you are not using JETset to configure the unit, we suggest you set this parameter to 'off'; access will be denied any person trying to connect to the unit.

*banner-status* This parameter concerns the banner information (product name/software version). This banner information is presented to a user with a login prompt. For security reasons you may wish to turn off the display of this information. The choices are ON or OFF. The default is OFF.

This parameter does not affect logins using Telnet/Rlogin or the Admin Port; in both these cases the banner information shall always be displayed.

### *OEM-mode*

The **OEM mode** field is a 4 digit hexadecimal number. The number is defined as a bit field, each bit being a different option that is either enabled or disabled.

The following options are currently used :-

Bit	Value	Option
-----	-------	--------

0	1	<b>Login prompt uses OEM1 string</b>
---	---	--------------------------------------

When set, and a custom language file is in use, the login prompt will use the string defined in the language file as the login prompt instead of the 'login: ' default prompt.

Note that this option applies to earlier versions of the software only.

1	2	<b>Bypass Password</b>
---	---	------------------------

When set, authorised users who do not have a password set, with the exception of the admin account, WILL NOT be prompted for a password at login.

2	4	<b>Disable Routed</b>
---	---	-----------------------

When set, the routed process will not be started at boot time. Instead, a static route will be created using the first entry found in the gateways table that is set to type default.

This is a read-only parameter for OEM\_mode. To enable/disable, use the *services* parameter.

3	8	<b>Telnetp Single Connection</b>
---	---	----------------------------------

Sets all reverse connections ( raw and telnet ) to a one connection at a time mode. Server side applications will get a (socket) connection refused until :

- All data from previous connections on that serial port have drained;
- There are no other connections;
- A (upto) 1 second interconnection poll timer has expired.

OEMmode 8 also enables a per-connection keepalive TCP keepalive feature - after approx 3 minutes of network connection idle time, the connection will send a gratuitous ACK to the network peer – thus either ensuring the connection stays active OR causing a dropped connection condition to be recognised by the reverse raw service.

Without OEM mode 8 set the software continues to work as before.

Applications using OEM mode 8 need to be aware that there may be some considerable delay between a network disconnection and the port being available for the next connection attempt - this is to allow any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature.

**Bit Value Option**

**4 10 Send Break Option**

When set a port will allow the sending of a break signal through to attached device. This can be used in the Sun Server environment when the administrator needs to take the Sun Server to the OBP mode (Open Boot Prompt)

This is a read-only parameter in OEM\_mode. To enable/disable this feature, use the 'set server break <status>' command.

*services*

This command allows the ability to enable/disable specific processes in the CS9000. The **services** field is a 4 digit hexadecimal number. The number is defined as a bit field, each bit being a different process that is either enabled or disabled. By default, all processes are enabled with the flag set FFFF). This service flag will be saved when configuration is saved to FLASH.

The following options can be used:

**Bit Value Option**

**0 0001 DHCP Process**

The DHCP process will be enabled when the service flag is displaying 0001. This is a read-only parameter . The DHCP is controlled by the command 'set server DHCP <status>', this flag will be updated accordingly.

**1 0002 ROUTE Process**

The ROUTE process will be enabled on well-know port 520 when the service flag is set to 0002. ROUTE process can also be viewed by OEM\_mode bit however it is a read-only parameter in OEM\_mode

**2 0004 Telnet Process**

The Telnet process will be enabled on well-known port 23 when the services flag is set to 0004.

**3 0008 SSH Process**

The SSH process will be enabled on well-known port 22 when the services flag is set to 0008.

**4 0010 HTTP Process**

The HTTP process will be enabled on well-known port 80 when the services flag is set to 0010. Note that disabling the server's services flag for HTTP process is different than GUI\_ACCESS configuration in such that there will be no response from the server when the HTTP process is disabled.

**5 0020 SNMP Process**

The SNMP process will be enabled on well-known port 161 when the services flag is set to 0020.

**6 0040 SPCD Process**

The proprietary SPCD (Trueport) process will be enabled on port 668 when the services flag is set to 0040.

**7 0080 SNTPD Process**

The SNTPD process will be enabled on UDP port 123 when the services flag is set to 0080.

**8 0100 ICMP Process**

ICMP will be enabled when the services flag is set to 0100.

*break-status*

The **break** option can be set to either on or off. This option will enable/disable proprietary inband SSH break signal processing as well as the existing Reverse Telnet break signal. The OEM\_mode flag 0010 will be set/reset based upon this command. This configuration parameter will be saved when the configuration is saved to FLASH.

*ssh\_break\_string*

The **ssh break string** can be set up to 8 characters which defines the break string used for inband SSH break signal processing. The default is set to '~break', where ~ is tilde.

A break signal is generated on a specific serial port only when the server's break option is enabled and the user currently connected using reverse SSH has typed the break string exactly.

*session\_escape\_string*

The **session escape** string is a configurable string that allows a user session to toggle to and from the multi-session menu screen to the session connection. The default string is <CTRL>**zs**

*rev-session-value*

The **reverse session limit** defines the number of support simultaneous connections on the CS9000. When you decrease the number of supported sessions, the amount of memory allocated for port buffer increases equivalently to all serial ports. The default value for this field is set to the number of ports on the CS9000. The range of value for this field is between 1 and the number of ports.

*line\_menu\_string*

The **line menu string** field defines the string used to disconnect from the line and return back to the Easy Port Access menu without the disconnecting the initial reverse SSH or reverse Telnet session. The default string is **~menu**.

*prompt\_status*

The **prompt with name** option displays the configurable server name instead of default product name and/or version. When the prompt status is enabled the server name will be displayed in login prompts, CLI prompts, HTML login screens and the heading of the menu screens instead of the default product name CS9000. This option can be set **On** or **Off**. The default value is **Off**.

Any combination of the arguments can be used. Examples:

```
set server name stimp  
set server name stimp tftp retry 2  
set server internet 192.101.34.202 broadcast 255.255.255.254 ip_host  
72.96.0.2
```

*Menu equivalents* server configuration

network configuration

*See also* [show server](#), [set date](#), [set time](#), [show hardware](#), [reset factory](#)

## set slip line

*user level:* Use this command to configure SLIP on a line.

*admin*

*syntax*                    `set slip line line_number parameter`

where:

line\_number may also be specified as \* for all lines, or . for the current in-use line.

parameters are any from the list below:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
mtu	maximum transmission unit
priority	interactive priority
transmit_parameters	transmit parameters
icmp_suppress	suppress icmp
vj_comp	VJ compression

The meanings and values of these parameters are explained in [Introduction to SLIP and PPP connections on page 75](#).

You can include multiple parameters in one line of syntax (up to a maximum of 100 characters).

*Menu equivalent* Line Configuration - SLIP

*See also* [show slip line](#)

## set sntp mode

*user level:* Use this command to configure SNTP parameters.

*admin*

*syntax*                    `set sntp mode mode server_1 server1 server_2 server2 version  
version_number`

where:

<i>mode</i>	The mode of the SNTP. Valid values are none, unicast, multicast and anycast. Default is none.
<i>server1</i>	The name of the primary NTP server from the host table. Valid with unicast or multicast mode
<i>server2</i>	The name of the secondary NTP server from the host table. Valid with unicast and multicast modes.
<i>version</i>	Version of NTP. Valid values are 1 to 4. Default value is 3.

*Menu equivalent* Time Configuration - SNTP Settings

*See also* [show sntp](#)

## set summertime mode

*user level:* Use this command to configure SNTP parameters.

*admin*

*syntax*                    `set summertime mode mode`

where:

*mode* is set for recurring or fixed. Depending upon which mode is entered the **set summertime mode** command has additional specific parameters associated with the *mode*.

```
set summertime mode fixed start_date dd/mm/yyyy start_time hh:mm
end_date dd/mm/yyyy end_time hh:mm offset mm name name
```

OR

```
set summertime mode recurring start_month mon start_week week
start_day day start_time hh:mm end_month mon end_week week end_day
day end_time hh:mm offset mm name name
```

where:

*start\_date* The date to change to summer time. Valid *dd* values from 1 to 31. Valid *mm* values from 1 to 12. Valid *yyyy* is 1970 to 2036.

*start\_time* The time to change to summertime. Valid *hh* values is 0 to 23. Valid *mm* values from 0 to 59.

*end\_date* The date to change to standard time. Valid *dd* values from 1 to 31. Valid *mm* values from 1 to 12. Valid *yyyy* is 1970 to 2036.

*end\_time* The time to change to standard time. Valid *hh* values is 0 to 23. Valid *mm* values from 0 to 59.

*start\_month* The month to change to summer time. Valid *mon* values are January to December.

*start\_week* The week of the month to change to summer time. Valid *week* values are 1 to 5 or last.

*start\_day* The day of the week to change to summer time. Valid *day* values are Sunday to Saturday.

*start\_time* The time of day to change to summer time. Valid *hh* values is 0 to 23. Valid *mm* values from 0 to 59

*end\_month* The month to change back to standard time. Valid *mon* values are January to December.

*end\_week* The week of the month to change back to standard time. Valid *week* values are 1 to 5 or last.

*end\_day* The day of the week to change back to standard time. Valid *day* values are Sunday to Saturday

*end\_time* The time of the day to change back to standard time. Valid *mm* values from 0 to 59

*offset*      The offset from standard time in minutes. Valid *mm* values are 0 to 180.

*name*        The name of the time zone to be displayed in during summer time. Maximum 4 characters.

*Menu equivalent* Time Configuration - Summer Time settings

*See also*        [show summertime](#)

## set telnet

*user levels:*    Use this command to set telnet parameters on a line. It is available for line service types of:

*admin*

[Direct telnet](#)

[Silent Telnet](#)

This command also sets default telnet values when you telnet to a host using the cli command `telnet`.

*Syntax*

```
set telnet
```

```
[line line_number]  
[termtyp terminal-type]  
[echo value]  
[mapnl value]  
[mode value]  
[intr value]  
[quit value]  
[eof value]  
[erase value]  
[break value]
```

Where:

<i>line_number</i>	is the serial line number connected; for example 3
<i>terminal type</i>	is your terminal type; for example wyse60. Note this value will be ignored if you have set a <code>termtyp</code> value using the command <code>telnet</code> .
<i>echo</i>	on or off
<i>mapnl</i>	on or off
<i>mode</i>	on or off
<i>intr</i>	<hexadecimal>
<i>quit</i>	<hexadecimal>
<i>eof</i>	<hexadecimal>
<i>erase</i>	<hexadecimal>
<i>break</i>	<hexadecimal>

Note:

echo, mapnl, mode, intr, quit, eof, erase and break are telnet options.

*Menu equivalent* not available in the text menus

*See also* [show telnet](#), [telnet](#)

## set time

*user level:* This command enables you to set the time in the unit. The time is used by the real-time clock. For more information on the real-time clock see Perle CS9000, [Setting date and time on page 67](#).

*admin*

*Syntax* `set time hh:mm [:ss]`

for example; set time 11:23

Optionally you can specify the number of seconds; e.g. set time 11:23.30

*Menu equivalent* Main Menu - hardware

*See also* [set date](#), [show time](#)

## set timezone offset

*user level:* This command enables you to specify the offset from UTC for your local time zone.

*admin*

*Syntax* `set timezone offset hh:mm name name`

for example; set timezone offset -5:00 name EST.

Where

*hh:mm* The hours *hh* (valid -12 to +14 ) and minutes *mm* (valid 0 to 59 minutes) for the offset from UTC

*name* The name of the time zone to be displayed during standard time. Maximum 4 characters.

*Menu equivalent* Main Menu - Time Configuration - Time Zone Setting

*See also* [show timezone](#)

## set user

*user levels:* *admin, normal* This command enables you to modify a user's setup, including predefined sessions. An admin user can change any user's setup. A normal user can only change certain elements of their own setup, e.g. password and language.

*Syntax*            `set user username / .`

```

[password]
[level user-level]
[switch switch_character]
[service user-service]
[ip-host iphost-address]
[tcp_port t-port number]
[callback callback-flag]
[phone_number phone-number]
[idle_timer i-timer value]
[sess_timer s-timer value]
[framed_ip f-ip address]
[framed_netmask f-netmask]
[framed_mtu f-mtu value]
[framed_compression f-compression value]

[routing routing_value]
[line_access access-value line-numbers-and-ranges]
```

### Where:

- password*            if you include this argument you will prompted to enter a new password.
- user-level*            is 'admin', 'normal', 'restricted' or 'menu'.
- user-service*        select one of: csprompt, telnet, rlogin, tcp\_clear, slip or ppp. For more information on these user services see [Appendix E Summary of Line Service Types](#).
- iphost-address*      (use only when you have selected a service of 'telnet' or 'rlogin'); select:
- 0.0.0.0 for the unit to select the default host set for all users; see [set server on page 176](#).
- 255.255.255.255 for the unit to prompt the user for the ip address or name of the host to which he/she wishes to connect
- n.n.n.n (where n is a number) for any other ip address of your choosing (as system administrator); e.g 192.65.144.6
- t-port number*        (use only when you have selected a user-service of 'telnet') enter the TCP port number of the host with which the unit should start the service. The default port is 23; in most cases you can use the default value.

<i>callback-flag</i>	whether the unit calls the user back when he/she connects to the unit (a security feature). Set either 'on' or 'off' (default is 'off'). When 'on', enter a phone number (see below).
<i>phone-number</i>	a number which the unit will dial to callback the user (you must have set 'callback' to 'on'). Enter the number without spaces. To change the phone number, overwrite the previous entry.
<i>i-timer value</i>	<p>enter a period in seconds for which the idle timer will run. Use this timer to close a connection because of inactivity. When the idle timer expires, if there has been no exchange of data, the unit will end the connection. The default value is 0 (zero), meaning that the idle timer will not expire (the connection is open permanently). The maximum value is <math>2^{32}</math> seconds.</p> <p>The idle timer (here) will override the idle timer which you can configure for a line with the exception of reverse SSH or reverse Telnet sessions.</p>
<i>s-timer value</i>	<p>enter a period in seconds for which the session timer will run. Use this timer to forcibly close a user's session (connection). When the session timer expires the unit will end the connection. The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The maximum value is <math>2^{32}</math> seconds.</p> <p>The session timer (here) will override the session timer which you can configure for a line with the exception of reverse SSH or reverse Telnet sessions.</p>
<i>f-ip address</i>	use only when the user service field is set to 'slip' or 'ppp';
<i>f-netmask</i>	ignore this parameter; it is reserved for future use.
<i>f-mtu value</i>	use only when the user service field is set to 'slip' or 'ppp';
<i>f-compression value</i>	use only when the user service field is set to 'slip' or 'ppp';
<i>routing_value</i>	the routing parameter determine the routing mode used on the PPP and SLIP interfaces that are authenticated by the particular user. Values are <b>none</b> , <b>send</b> , <b>listen</b> and <b>send_and_listen</b> .

*access-value* enter a value for the line(s) that the user can have access or permission to connect to. The *access-value* can be entered in three different modes and be assigned to a specific line number or a range of line numbers.

*line-number-and-range*

The *access-value* can be set to the following:

**readwrite:** permits the user to have both read and write access to the line.

**readin:** permits the user to read data from the device into the serial port of the unit. Inbound data only.

**readout:** permits the user to read data to the device from the serial port of the unit. Outbound data only.

The *line-number-and-range* can be set to the following

**Specific Line format:** can specify certain lines that a user can have access rights to. For example, to allow user *abc* access to port 3, 4, 6, and 2 you can configure using **set user abc line\_access readwrite 3,4,6,2**. NOTE: specify a value of 0 for the user disables all line access right and the user is unable to connect to any lines on the CS9000.

**Range format:** can specify a range of lines which the user can have access to. For example, to allow the user *abc* access to ports 1 to 12 you can configure using **set user abc line\_access readwrite 1-12**.

Combination of formats can be also specified e.g **set user abc line\_access readwrite 1,5,10-15,17,20-23**.

*Notes* You can set all users to the same parameters by using the \* asterisk character, e.g.

```
set user * level normal
```

will set all users to this language value.

*Menu equivalent* Users - Change User/Set Password

Users - Line Access

*See also* [add user](#), [netload](#), [show timezone](#), [delete user](#), [show telnet](#)

## show ARP

This command is used to display the current ARP table. This is useful for diagnostic and debugging purposes.

This parameter is only accessible from the unit's CLI.

*Syntax*

```
show arp
```

*See also* [delete ARP](#)

## show date

*user levels:* This command enables you to show the date in the unit; e.g.

*admin, normal*            date 2/2/1999

*Syntax*                    show date

*Menu equivalent* Main Menu - hardware

*See also*                [set date](#), [set time](#), [show time](#), [show hardware](#)

## show gateways

*user levels:* Use this command to list the gateways you have defined. The list will be displayed in the following

*admin, normal* format:

```
CS_9000# show gateways
hostname      service  internet address  netmask      status
socrates      network 172.18.128.0   255.255.224.0 active
plato         host    192.168.23.45  active
router312     default
```

If you have not entered gateway information your command will be ignored; you will be presented with the unit prompt once more.

*Syntax*                    show gateways

*Menu equivalent* Network Configuration - Gateways - Change Gateway

*See also*                [add gateway](#), [delete gateway](#), [set gateway](#)

## show hardware

*user level:* This command displays the hardware configuration of your unit. An example display is:

*admin, normal*

```
CS_9000# show hardware
mac address      0080ba0000d4
ethernet i/f     RJ45 10/100Base-T
board id         CS4300076R2.1
processor        80386
uarts            2 * Serial ASIC
flash rom        1 x 1MB
ram              2 x 2MB
battery ram      32kB
serial ports     16
date             13/12/2001
time             15:03:44
CS_9000#
```

*Syntax*                    show hardware

*Menu equivalent* Main Menu - Hardware

*See also*                [set date](#), [set time](#), [show line](#)

## show hosts

*user levels:* Use this command to list the contents of the host table:  
*admin, normal*

```
CS_9000# show hosts
hostname      internet address
socrates      192.49.144.4
aristotle     192.50.123.76
plato         192.78.26.21
sophocles     192.111.89.2
homer         192.111.64.3
pythagoras    192.168.0.254
CS_9000#
```

*Syntax* show hosts  
*Menu equivalent* Network Configuration - Host Table - Change Host  
*See also* [add host](#), [delete host](#), [set host](#)

## show interface

This command will show all lines with active SLIP or PPP links. It is useful for monitoring the status of dial-up lines. This parameter is only accessible from the unit's CLI.

*Syntax* show interface

## show line

*user levels:* This command can be used to display the configuration of a single line or all lines, of the front-mounted serial RJ45 ports only. Admin users can show all lines, normal users can only display the configuration of their own line. The command does *not* show :

the Admin Port line configuration; this is fixed.

For a single line the display will look similar to this:

```
JS_8500# show line 2
line name      line_name_2
speed          9600
terminal       dumb
dial           none
flow           none
bits           8
parity         N
stop           1
phone number
modem name     none
idle timer     0
session timer  0
routing        none
service        rev raw
CS port        10002
security       on
JS_8500#
```

If you specify all lines, the display will look similar to this:

```

CS_9000# show line *
line   line name      speed  service
1      Accounting      9600   cslogin
2      Accounting      9600   rev tel  -/10002 security=on
3      Corporate       9600   rev ssh  -/10003
4      Corporate       9600   rev tel  -/10004 security=on
5      TFTP            9600   rev ssh  -/10005
6      TFTP            9600   rev tel  -/10006 security=on
7      TFTP            9600   rev tel  -/10007 security=on
8      Sales           9600   rev tel  -/10008 security=on
9      Sales           9600   rev tel  -/10009 security=on
10     Sales           9600   rev tel  -/10010 security=on
11     RAS             9600   rev tel  -/10011 security=on
12     RAS             9600   rev tel  -/10012 security=on
13     Engineering     9600   rev tel  -/10013 security=on
14     Engineering     9600   rev tel  -/10014 security=on
15     Engineering     9600   rev tel  -/10015 security=on
16     Engineering     9600   rev tel  -/10016 security=on
CS_9000#

```

Note that the user shown in the right-hand column is the 'current user' i.e. the user currently logged in on that line. 'Nouser' means there is not a user currently logged in. 'In use' means the line is in use but line security is off so no user can be identified. If a user is displayed followed by a + character this indicates that the displayed user was first to connect to the line and multiple users are connected to the particular line. To view the specific users connected to the line, see *show line <line number> users*.

The security status for individual lines can be determined from the show line display. "Security=on" indicates that security is enabled for the particular line and "Security=off" indicates security is disabled for the line.

*Syntax*            `show line line_number`

Where line\_number is :

- .                    the current line.
- n*                 a specific line number.
- \*                   all lines

*Menu equivalent*    Line Configuration - Line Settings

*See also*            [set line](#), [show timezone](#), [show line users](#)

## show line users

*user levels:* Use this command to show all users connected to a specific line.

*admin, normal*

*Syntax*                    show line <line number> users

If you specify to view the users connected to a specific line you will see a list of the users connected to the line:

```
CS_9000# show line 1 users
test
admin
CS_9000#
```

## show modems

*user levels:* Use this command to show modem details held by the unit.

*admin, normal*

*Syntax*                    show modem

This will show (for example):

name	initialisation string
Hayes	
US Robotics	
Courier	

*Menu equivalent* Line Configuration - Modems - Change Modem

*See also:* [add modem](#), [delete modem](#), [show line](#)

To change modem details in the cli you must 'delete' the modem, then 'add' it again, with the changed details.

## show port\_buffering

*user levels:* Use this command to show port buffering details held by the unit.

*admin, normal*

*Syntax*                    show port\_buffering

```
CS_9000# show port_buffering
mode local
view port buffer string ~view
time stamp on
nfs host linux
nfs directory /cs9000/portlogs
nfs encryption off
CS_9000#
```

*Menu equivalent* Main Menu-Port Buffering

*See also:*            [set port\\_buffering](#)

## show ppp line

*user levels:* Use this command to show the PPP configuration of a line. Admin users can show all lines; users with normal level privileges can only display the configuration of their own line.

*admin,*

*normal*

For example:

```
CS_9000# show ppp line 1
local address 0.0.0.0
remote address 0.0.0.0
subnet mask 0.0.0.0
accm 00000000
mru 1500
security chap
user
password *****
ruser
rpassword *****
ac comp on
proto_comp on
vj_comp on
magic_neg off
ipaddr_neg off
cr_timeout 3 seconds
tr_tmout 3 seconds
cr_retry 10
tr_retry 2
nak_retry 10
auth_tmout 1 minutes
roaming_callback off
challenge_interval 0 minutes
CS_9000#
```

*syntax*                    `show ppp line line_number`

where:

line\_number may also be specified as \* for all lines, or . for the current in-use line.

parameters are any from the list shown in the next table:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
accm	asynchronous character control map
mru	maximum receive unit
security	security
user	user
password	password
ruser	remote user
rpassword	remote password
ac_comp	address/control compression
proto_comp	protocol compression
vj_comp	VJ compression
magic_neg	magic number negotiation
ipaddr_neg	ip address negotiation
cr_tmout	'configure request' timeout
tr_tmout	'terminate request' timeout
cr_retry	'configure request' retries
tr_retry	'terminate request' retries
nak_retry	'configure nak' retries
auth_tmout	authentication timeout

The meanings and values of these parameters are explained in [Introduction to SLIP and PPP connections on page 75](#).

*Menu equivalent* Line Configuration - PPP

## show radius

*user levels:* Use this command to check the RADIUS settings of the unit:

*admin, normal*

*Syntax*                    show radius

The output of this command are the RADIUS settings of the unit (e.g.):

```
CS_9000# show radius
retry                5
timeout              3
auth_port            1645
acct_port            1646
acct_authenticator   on
accounting           off
session id           5000000
user level           normal
CS_9000#
```

For details of these parameters, see Perle CS9000, [RADIUS configuration on page 55](#).

*Menu equivalent* radius configuration - radius settings

*See also*            [add radius](#), [set radius](#), [set server](#)

## show rip

*user levels:* Use this command to check the RIP settings of the unit:

*admin, normal*

*Syntax*                    show rip

The output of this command are the RIP settings of the unit :

```
CS_9000# show rip
ethernet mode        send_and_listen
send                 rip_v2
receive              both
authentication       md5

md5 keys:
id   start                end                status
41   15/10/2003  2:00:00          15/1/2004   2:10:00    expired
12   15/1/2004    2:00:00          15/4/2004   2:10:00    active
125  15/4/2004    2:00:00          15/7/2004   2:10:00    pending
253  15/7/2004    2:00:00          15/10/2004  2:10:00    pending
CS_9000#
```

**Note**            *The MD5 keys are only displayed if the authentication is set to MD5.*

For details of these parameters, see Perle CS9000, [Configuring RIP on page 64](#).

*Menu equivalent* radius configuration - radius settings

*See also*            [add rip md5](#), [set rip](#)

## show rip peers

*user levels:* Use this command to display the contents of the current RIP peer table.

*admin, normal*

*Syntax*                    show rip peers

The output of this command are:

```
CS_9000# show rip peers
internet address last update ver auth seq number bad packets bad routes
172.16.1.7        28          1   1   0          0          0
172.16.43.50     16          1   1   0          0          0
172.16.4.43      16          1   1   0          0          0
172.16.1.9       18          1   1   0          0          0
CS_9000#
```

For details of these parameters, see Perle CS9000, [Configuring RIP on page 64](#).

*Menu equivalent* radius configuration - radius settings

*See also*            [add rip md5](#), [set rip](#), [show rip](#)

## show routes

*user levels:* Use this command to give you a better understanding of your network. It will also show a single passive gateway configured using bootp. Below is an example:

*admin, normal*

```
CS_9000# show routes
destination netmask gateway flags refs use iface
192.168.23.45 255.255.255.255 172.16.48.102 UGH 0 0 le0
192.168.0.0 255.255.255.0 172.16.1.9 UG 0 0 le0
172.18.128.0 255.255.224.0 172.16.48.101 UG 0 0 le0
172.16.0.0 255.255.0.0 172.16.48.9 U 1 1564 le0
172.17.0.0 255.255.0.0 172.16.53.11 UG 0 0 le0
0.0.0.0 0.0.0.0 172.16.1.7 UG 3 4464 le0
```

*Syntax*                    show routes

*Menu equivalent* there is no menu equivalent

**Note**            *this command is synonymous with the 'netstat -r' command on most Unix systems. See the manpages (type "man netstat" on your Unix system for more information).*

## show server

*user levels:*        This command displays the base configuration of the unit, for example:  
*admin, normal*

```
CS_9000# show server
servername                CS9000
internet address          172.16.33.220
subnet mask               255.255.0.0
broadcast address         172.16.255.255
domain name
tftp retry                5
tftp timeout              3
security                  off
authentication            local
services                  fffe
                          (SPCD+SNMPD+HTTPD+SSHD+TELNETD+ROUTED)
dhcp                      off
ssh protocol              both(ssh-1+ssh-2)
break                     off
ssh break string          ~break
session escape string     <026>s
line menu string          ~menu
reverse session limit     24
gui access                on
banner                    off
prompt with name          off
OEM_mode                  0000
< hit any key >
CS_9000#
```

Fields which are unconfigured will not appear in the list on your screen.

*Syntax*                `show server`

*Menu equivalent*    server configuration

network configuration - DNS

network configuration - WINS

*See also*            [set server](#), [show hardware](#)

## show slip line

*user levels:* Use this command to show the SLIP configuration of a line. Admin users can show all lines; users with *admin, normal* normal level privileges can only display the configuration of their own line.

For example:

```
CS_9000# show slip line 1
local address      0.0.0.0
remote address    0.0.0.0
subnet mask       0.0.0.0
mtu               256
icmp_suppress     off
priority          on
vj_comp          on
transmit_parameters on
CS_9000#
```

*syntax*                    show slip line *line\_number*

where

:*line\_number* may also be specified as \* for all lines, or . for the current in-use line.

parameters are any from the list below:

parameter syntax	parameter name
lipaddr	local ip address
ripaddr	remote ip address
subnet	subnet mask
mtu	maximum transmission unit
priority	interactive priority
transmit_parameters	transmit parameters
icmp_suppress	suppress icmp
vj_comp	VJ compression

The meanings and values of these parameters are explained in [Introduction to SLIP and PPP connections on page 75](#).

*Menu equivalent* Line Configuration - SLIP

*See also* [set slip line](#)

## show snmp

*user levels:* This command shows the configuration of the unit for SNMP support; for example:  
*admin, normal*

```
CS_9000# show snmp
snmp contact      John Smith
snmp location     IT Helpdesk x3423
snmp communities: 1. public      192.168.0.234  readonly
                  2. admin      192.168.0.10   readwrite
snmp traps:       1. local      192.168.0.35
CS_9000#
```

*Syntax*                    show snmp

*Menu equivalent* network configuration - snmp

*See also*                [add community](#), [add trap](#), [set contact](#), [set location](#)

## show sntp

*user levels:* This command shows the configuration of the unit for SNTP support; for example:  
*admin, normal*

```
CS_9000# show sntp
mode                unicast
version             4
server 1            linux
server 2            pc
CS_9000#
```

*Syntax*                    show sntp

*Menu equivalent* network configuration - Time Configuration - SNTP settings

*See also*                [set sntp mode](#)

## show sntp\_info

*user levels:* This command shows the latest status of SNTP network packet information, for example:  
*admin, normal*

```
CS_9000# show sntp_info
internet address      172.16.33.200
last update          7/1/2004 15:23:30 utc
leap indicator        0
version              4
mode                 4
stratum              4
reference identifier  ac103030
correction            0
CS_9000#
```

Where :

<i>internet address</i>	IP address of the last packet received from a server
<i>last update</i>	the time the last server packet was received
<i>leap indicator</i>	the value of the leap indicator in the last server packet received
<i>version</i>	the version number in the last server packet received
<i>mode</i>	the mode in the last server packet received
<i>stratum</i>	the clock stratum in the last server packet received
<i>reference ID</i>	the reference indicator in the last server packet received
<i>correction</i>	the correction applied to the clock from the last server packet received.

*Syntax*                    show sntp\_info

*Menu equivalent* network configuration - Time Configuration - SNTP settings

*See also*                [set sntp mode](#)

## show summertime

*user levels:* This command shows the configuration of the unit for daylight savings time (summertime); for example:  
*admin, normal*

```
CS_9000# show summertime
name          edt
offset        60
mode          recurring
start day     sunday
start week    1
start month   april
start time    2:00:00
end day       sunday
end week      last
end month     october
end time      2:00:00
CS_9000#
```

*Syntax* `show summertime`  
*Menu equivalent* network configuration - Time Configuration - Summertime Settings  
*See also* [set summertime mode](#)

## show telnet

*user levels:* Use this command to show telnet parameters on a line. Note that telnet parameters shown here apply only to line service types of:

[Direct telnet](#)  
[Silent telnet](#)

The command also shows telnet parameters entered using the command `set sntp mode`.

```
CS_9000# show telnet line 1
echo mapn mode intr quit eof erase break terminal
off off off 7f 1c 04 00 1d
CS_9000#
```

*Syntax* `show telnet line line_number`

Where:

*line\_number* is the serial line number connected

*Menu equivalent* not available in the text menus

*See also* [set sntp mode](#)

## show time

*user levels:* This command enables you to show the time as measured by the real-time clock in the unit; e.g.

*admin, normal*                   time11:04:32

*Syntax*                        show time

*Menu equivalent* Main Menu - hardware

*See also*                    [set date](#), [set time](#), [show date](#), [show hardware](#)

## show timezone

*user levels:* This command shows the configuration of the unit for timezone support; for example:

*admin, normal*

```
CS_9000# show timezone
name                est
offset              -5:00
CS_9000# █
```

*Syntax*                        show timezone

*Menu equivalent* network configuration - Time Configuration - Time Zone settings

*See also*                    [set timezone offset](#)

## show user

*user levels:* Use this command to display a user's setup, including predefined sessions. The admin user can show details of any user, a normal user can only view their own details:

```
CS_9000# show user johnd
username                johnd
screen switch           01
level                   normal
service                 csprompt
ip_host                 0.0.0.0
tcp port                23
callback                off
phone number
idle timer              0
session timer          0
framed ip               255.255.255.254
framed netmask          0.0.0.0
framed mtu              1500
framed compression     on
routing                 send_and_listen
line access readwrite  1-16
line access readin     0
line access readout    0
CS_9000#
```

*Syntax*            `show user ./username`

Where:

- `.` specifies the current user.
- `username` is the name of a specific user.

*Menu equivalent* Admin user: Users - Change User.  
Normal user: Sessions - Set Up User

*See also*        [set user](#)

## start

*all users* Use this command to start a predefined session. This is a particularly important command for restricted users who can only start sessions predefined for them by system administrator. If you are using telnet, the target host will prompt you for your login name. If you are using rlogin, the host will prompt you for your password. If you are using rlogin and your unit's login name is entered in the 'rhost' file of the target login directory, you will be logged straight in.

*Syntax*            `start n`

Where *n* is the predefined session that you want to start.

*Menu equivalent* Sessions - Start Predefined Session

*See also*        [resume](#)

## telnet

*user levels:* This command establishes a connection with another host on the network using the telnet protocol. You must specify the target host but the other arguments (such as echo, mapnl, mode, etc.) are optional. If you do not specify the other arguments the line telnet values will be used (values set/shown in `set sntp mode` or `show telnet`)

*admin, normal*

If you do specify arguments such as echo, mapnl, mode, etc. the values you enter will override the line telnet values. Note that your values (specified here using the `telnet` command) expire when your telnet session is finished; values set/shown in `set sntp mode` or `show telnet` can be saved permanently.

When the connection is made you will be prompted for your login name.

*Syntax*

```
telnet hostname/inetaddress port [termttype termttype] [echo on/off] [mapnl on/off] [mode on/off] [intr <hex>] [quit <hex>] [eof <hex>] [erase <hex>] [break <hex>]
```

Where:

*hostname/ inetaddress* is the name or internet address of the machine you want to log into

*termttype* is your terminal type. This argument enables you to pass your terminal type to the host. When connecting to a UNIX host, you must define the termttype in accordance with its UNIX TERM variable.

The termttype argument overrides a termttype value entered into the unit when using the `set line` or `set sntp mode` commands.

echo, mapnl, etc. these are telnet options. They set values once only, for the duration of a single telnet connection. See comments under [telnet on page 205](#) above.

*See also* [resume](#), [rlogin](#), [set sntp mode](#), [show telnet](#), [start](#)

## version

*user levels:* This command tells you what version of software your unit is running.

*admin, normal*

*Syntax* `version`

*Menu equivalent* Version of software is displayed at the top of any menu display, e.g.

```
+-----+
* user [admin ] CONSOLESERVER 9000 3.4.0.G telnet 1 *
+-----+
```



# Appendix C SNMP

*You need to read this appendix if you want information on the Perle CS9000 support of SNMP.*

*this appendix if you want to...* This appendix describes the Perle CS9000 support of SNMP.

This appendix includes the following sections;

- [Overview on page 208](#)
- [Configuring SNMP support on page 209](#)
- [Network management on page 210](#)

## Overview

The Simple Network Management Protocol (SNMP) is a protocol for access and control of network management information on TCP/IP networks. Perle CS9000 (the '*unit*') provides an SNMP agent, able to respond to SNMP requests generated by SNMP Managers. The unit's implementation of SNMP is compatible with MIB II (RFC 1213) as specified by the SNMP SMI document (RFC1155). For a full description of SNMP, refer to your SNMP documentation.

Enterprise-specific parameters are defined by the unit's Private MIB, known as the Perle CS9000 Private MIB. Configurable parameters for the CS9000 are available as read-only parameters through SNMP protocol. The corresponding MIB file is available on the CS9000 CDROM and on the Perle website.

# Configuring SNMP support

To configure for SNMP support proceed as follows;

1. From the Main Menu select 'network configuration' and then 'snmp'.
2. Select 'snmp contact information' to configure the SNMP sysContact and sysLocation objects; an example screen is shown below:

*cli syntax:*  
*set contact*  
*set location*

```

network configuration
reset
snmp
snmp
snmp
contact      location
[john smith  ][IT Helpdesk ]
security
reboot server
  
```

3. Select 'edit traps' to create up to four trap communities; an example screen is shown below:

*add trap*  
*delete trap*

```

network configuration
reset
traps
trap      internet address
[pink     ][192.168.0.1  ]
[turquoise][192.168.0.42 ]
[         ][           ]
[         ][           ]
reboot server
  
```

SNMP Trap messages generated by the unit will only be broadcast to hosts defined by SNMP Trap communities.( note that the unit generates no enterprise specific traps).

4. Select 'edit communities' to create up to four communities; an example screen is shown below:

*add community*  
*delete community*

```

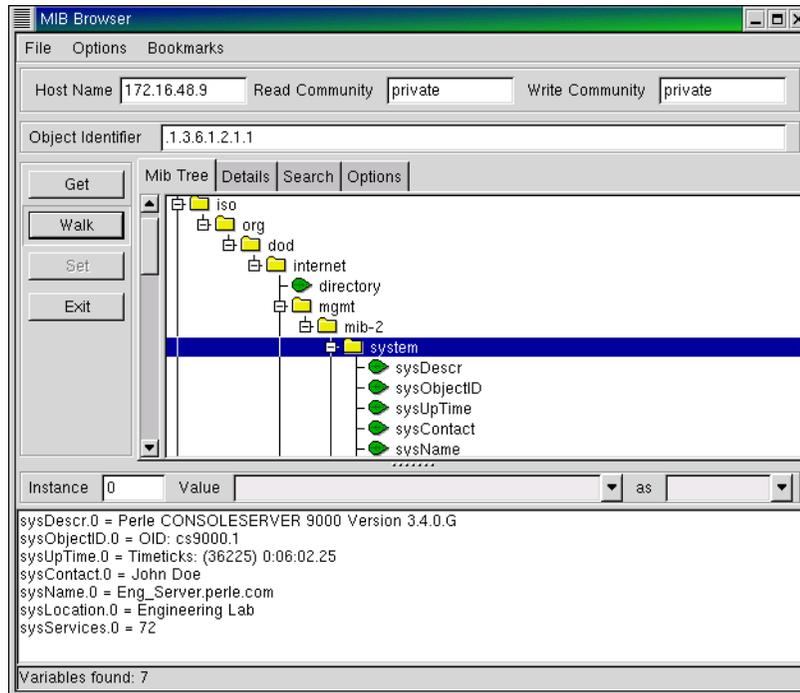
network configuration
reset
communities
community  internet address  permissions
[public    ][192.168.0.65  ] [none  ]
[          ][           ] [none  ]
[          ][           ] [none  ]
[          ][           ] [none  ]
reboot server
  
```

The unit's SNMP Agent will only provide information to hosts defined by an SNMP community.

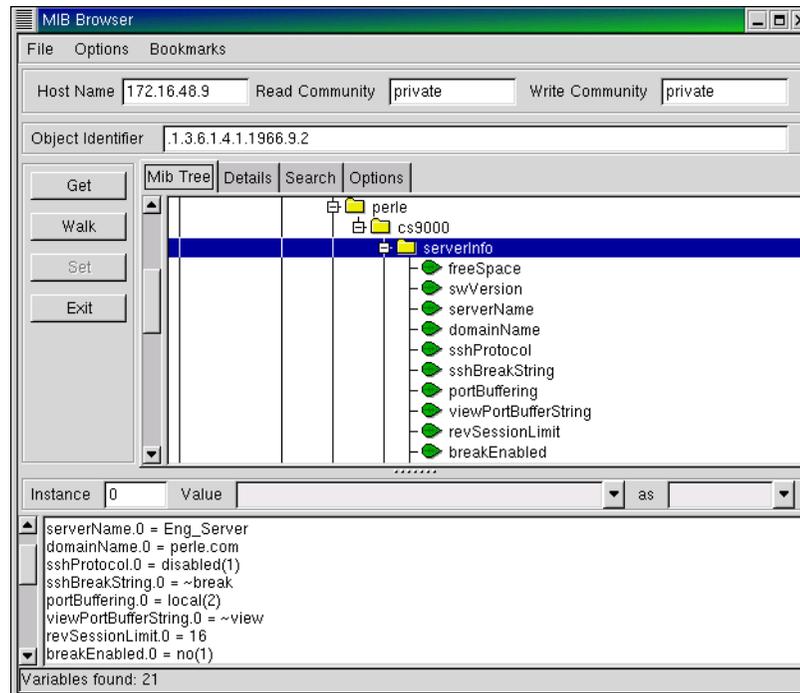
# Network management

If you have separate network management software you can interrogate and configure the unit using SNMP. For example, using MBrowse SNMP application, by Aaron Hodgen, running on a Linux host, configuration screens you might see are shown below:

*Viewing the  
RFC1213 MIB*



Viewing the  
CS9000 MIB





# Appendix D Upgrading your firmware

*You need to read this appendix if you want information on upgrading the Perle CS9000 firmware.*  
*this appendix if you want to...* This appendix provides task orientated information on upgrading the Perle CS9000 firmware.

This appendix includes the following sections;

- [Introduction on page 214](#)
- [Saving your existing Configuration on page 215](#)
- [Using BOOTP from a boothost on page 218](#)
- [Upgrade using JETset, the web browser interface on page 219](#)
- [Enabling BOOTP/DHCP after upgrading software on page 219](#)
- [Disable BOOTP/DHCP on page 219](#)

# Introduction

If you have been supplied with a software upgrade this appendix shows you how to install it.

To check the version of software your unit is running see the information displayed at the top of any menu display, that is:

```
user [admin]          xxxxxx 1.0          telnet 1
```

Compare this with the version number of software which you have obtained. If you have a more recent version of software, you should install it.

There are three methods for upgrading the software in the unit:

- Using the administrative Command Line Interface (CLI) on the unit (see [Using TFTP from a host on page 215](#)).
- Using a BOOTP server (see [Using BOOTP from a boothost on page 218](#))
- Using the JETset web configuration tool (see [Upgrade using JETset, the web browser interface on page 219](#)).

The method you choose will depend on how you operate your unit.

Before you upgrade the software on your Perle CS9000 unit we recommend you save the existing configuration information to a network file server.

In all cases the software upgrade process requires that the software has been installed to a readable directory on a network fileserver and that the TFTP service has been enabled.

## Saving your existing Configuration

Saving the existing configuration will allow the configuration information in the unit to be restored at a later date.

*Note* Upgrading the software on the unit does not alter the stored configuration information which will be preserved during the upgrade.

The procedure requires the presence of a write enabled empty file on a suitable network fileserver. The fileserver must have the TFTP (Trivial File Transport Protocol) service enabled and running.

## Example of saving a configuration file

The following is an example of how to save the configuration of a Perle CS9000 on a UNIX fileserver called **BIGSERVER**, the file will be saved to the file **/home/cs9000/cs9000.cfg**.

In this example the administrator issues the CLI command:

```
netsave configuration BIGSERVER /home/cs9000/cs9000.cfg
```

## Using TFTP from a host

1. Place the new software file on a host machine. Ensure the file has global read/execute permissions for its entire path.
2. Exit the menus and go into the CLI. Type:  
*cli syntax:*  
*netload software*            `netload software <hostname> <filename>`
3. Press <return>. The Perle CS9000 will download the new software file using TFTP.

## TFTP configuration

*cli syntax:* You can configure TFTP in the Perle CS9000 (the 'unit'). It is used for transferring files to/from a host; the files could be, for example, configuration, new software or custom language files. From the Network Configuration Menu, select 'tftp'; you should see the following:

```
tftp
retry [5 ]
timeout[3 ]
```

**retry** should tftp fail, retry is the number of retries the unit will make to transfer a file to/from a host. Enter a value between 0 and 255. The default value is 5. A value of 0 means that the unit will not attempt a retry.

**timeout** is the time in seconds the unit will wait for successful transmit or receipt of tftp packets before retrying a transfer. Enter a value between 1 and 255. The default value is 3.

## Writing to FLASH memory

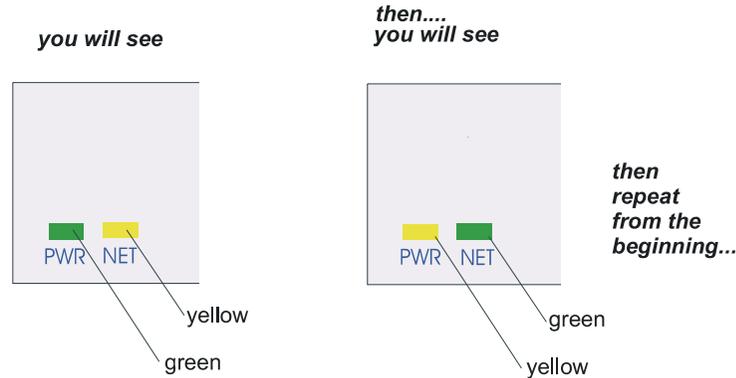
The Perle CS9000 will load the software into RAM, perform checks, and then write the software into FLASH memory. The writing to FLASH will take a few minutes and during this time the unit will not respond to user input. While the new software is being loaded into FLASH memory, the power and network LEDs on the front of the unit display a pattern.

---

### WARNING

do not turn the power off/on while the unit is writing to FLASH memory

*pattern of Perle CS9000 LEDs during load of software into FLASH*



This pattern is repeated approximately once per second.

The Network LED flickers green if network traffic is identified on the network ports.

The pattern on each LED is repeated approximately once per second.

*reboot*

When the software has finished downloading you must reboot the unit. To do this, type the command:

```
reboot
```

## Using BOOTP from a boothost

When installing with BOOTP, the SW\_FILE parameter in your BOOTFILE will need to be changed to point to the new software image. We recommend that you keep the name of the image file as supplied as this will guarantee that the software is recognised as a new version by the existing software installation.

Reboot your unit. The new software will download and write to FLASH memory, see [Writing to FLASH memory](#) on page 217. You can monitor the progress of this operation with a terminal (or terminal emulation) connected to the Admin port at the rear of the unit.

---

**WARNING**

---

**DO NOT SWITCH OFF THE UNIT** whilst the unit is programming the FLASH memory.

You can use BOOTP to compare a software version placed on the boot host and one loaded in the Perle CS9000; if there is a newer version on the host, it will be downloaded to the unit.

For a full description of how to use BOOTP to download a new software file from a host, see [Perle CS9000, Section Appendix F BOOTP](#).

## Upgrade using JETset, the web browser interface

1. Start JETset by pointing your network browser at the Internet Address of your the unit.
2. Log in as the Admin user and select file transfer from the main menu.
3. Complete the file transfer form by selecting software download from the pull-down menu, and completing the internet address of the TFTP server and the download software image filename.
4. Select save from the main menu to start the download process. Your browser may ask you to confirm this action before the download will start.

The new software will download and written to FLASH memory, see Writing to FLASH memory on page 217. You can monitor the progress of this operation with a terminal (or terminal emulation) connected to the Admin port at the rear of the unit.

---

**WARNING**

DO NOT SWITCH OFF THE UNIT whilst the unit is programming the FLASH memory.

## Enabling BOOTP/DHCP after upgrading software

If you require automatic BOOTP/DHCP configuration, be sure to set the server DHCP parameter to ON:

```
set server dhcp on
```

Save the configuration:

```
Save
```

## Disable BOOTP/DHCP

The server parameter DHCP is used to disable BOOTP/DHCP (set server dhcp on/off ). Setting DHCP to OFF prevents the unit from initiating a BOOTP/DHCP request. This parameter is only accessible from the CLI.

RARP is unaffected by this parameter.

After any software upgrade you should always check that DHCP is set to ON if you require BOOTP/DHCP to configure your unit.



# Appendix E Summary of Line Service Types

*You need to read this appendix if you want to...* You need to read this appendix if you want a summary of line service types for the Perle CS9000.  
This appendix provides a list of line service types for the Perle CS9000.

This appendix includes the following sections;

- [List of line service types on page 222.](#)

## List of line service types

When you are configuring a line on the Perle CS9000 (the 'unit') you will find a parameter for a line called 'service'. The detail of types of line service available are shown below.

*Note do not confuse line 'service' with user 'service'. User 'service' is a completely different parameter from line 'service' and is used by the unit in different ways.*

Line Service Type	Description/Uses	Example
<b>Bidir</b>	Allows a bidirectional modem connection on a port	A UUCP connection for batch file transfer and printing.
<b>Direct telnet or rlogin</b>	When using the unit as a Serial Server, to bypass the unit and allow users to login straight into a specific host. <i>These are non-permanent connections</i>	Users on terminals.
<b>Direct Raw</b>	Enables external non-login devices to access TCP/IP servers via the unit. No authentication will take place. The connection is set up from the unit to a TCP/IP network host (the opposite of <a href="#">Reverse Raw</a> ). <i>These connections are established by pressing &lt;return&gt;.</i>	On dialin connections: user applications for devices such as bar code readers and smart cards.
<b>cslogin</b>	The unit presents a login on that line.	a) System administrator to do unit configuration b) Users to starting the unit's sessions to hosts. c) Providing authentication of a user before starting a user 'service' of SLIP
<b>PPP</b>	a) Remote access connection b) Using the unit as a router (two units back-to-back)	A mobile employee  Joining together two networks
<b>Reverse Raw</b>	Simple pipe between a TCP/IP host and a machine/device attached to a port on the unit. The connection is set up from the TCP/IP host on the local network to the unit (the opposite of <a href="#">Direct Raw</a> and <a href="#">Silent Raw</a> ).	To access printers or dialout modems (with separate host-based print/modem handling software).

Line Service Type	Description/Uses	Example
<b>Reverse Telnet (Default)</b>	Enables a TCP/IP host to establish a login connection on an external machine attached to a port	To access machines like routers, firewalls, servers and so on.
<b>Silent telnet or rlogin</b>	When using the unit as a Terminal Server, to bypass the unit and allow users to login straight into a specific host. <i>These are permanent connections, therefore consume system resources</i>	Users on terminals.
<b>Reverse SSH</b>	Enables a SSH secure connection to establish a login connection on an external machine attached to a port.	Secure remote connection to access machines like servers, routers, firewalls etc.
<b>Silent Raw</b>	Enables external non-login devices to access TCP/IP hosts via the unit. The connection is set up from the unit to a TCP/IP network host on the local network (the opposite of <a href="#">Reverse Raw</a> ). <i>These connections are established automatically; they are suitable for computer to computer communications.</i>	Dialin connection from an external host machine.
<b>SLIP</b>	a) Remote access connection b) Using the unit as a router (two units back-to-back)	A mobile employee Joining together two networks



# Appendix F BOOTP

*You need to read this appendix if you want to...* You need to read this appendix if you require information about BOOTP for the Perle CS9000. This appendix provides information about BOOTP for the Perle CS9000.

This appendix includes the following sections;

- [Introduction on page 226](#)
- [How BOOTP works on page 227](#)
- [How to setup BOOTP on page 229](#)
- [BOOTP messages output to screen on page 233](#)
- [Disabling the BOOTP reply on page 233](#)
- [Booting multiple units on page 234](#)
- [Multiple BOOTP servers on page 235](#)
- [Example of BOOTP on page 235.](#)

## Introduction

You can use BOOTP to perform the following actions on a single or multiple Perle CS9000 (the '*unit(s)*')s on its/their boot-up:

- auto-configure with minimal information; e.g. only an ip address
- auto-configure with basic setup information (ip address, subnet mask, broadcast address, etc.)
- download a new version of software
- download a full configuration profile (saved from another unit)

BOOTP is particularly useful for multiple installations: you can do all the unit's configuration in one BOOTP file, rather than configure each unit manually.

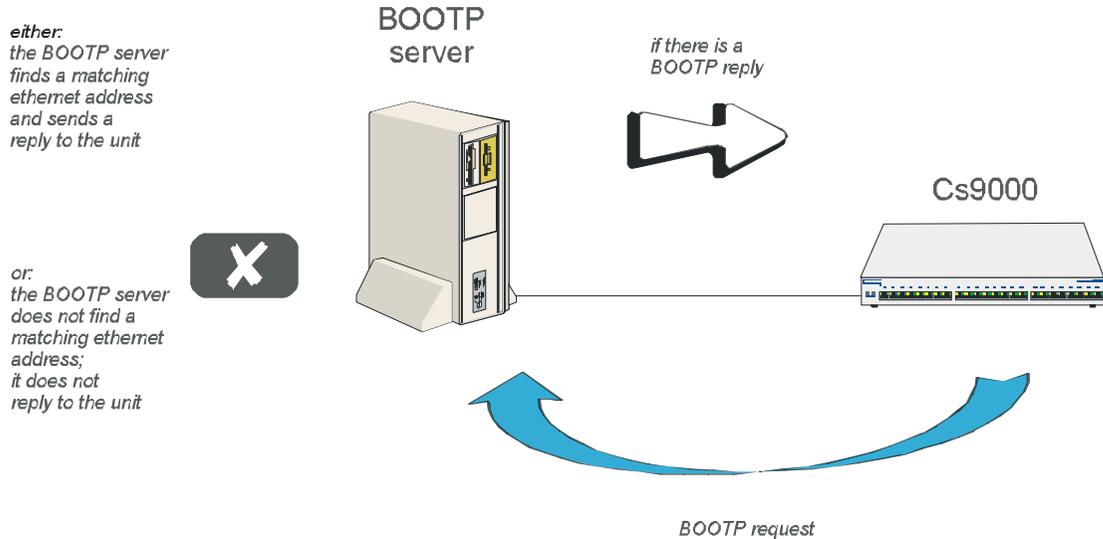
Another advantage of BOOTP is that you can connect a unit to the network, turn on its power and let auto-configuration take place. All the configuration is carried out for you during the BOOTP process.

The the unit's implementation of BOOTP is compatible with RFC 951.

## How BOOTP works

On bootup or power-up, the unit will send a broadcast request to the BOOTP server(s) on the network. The request contains the ethernet address of the unit; it asks for network configuration details (internet address, subnet mask, etc.). This process is shown on [page 227](#). You can stop the BOOTP server from replying to the unit; see [page 233](#).

### BOOTP request and response



The BOOTP server checks the ethernet address and looks for a matching address in its bootptab file:

If a matching ethernet address is found the BOOTP server will reply to the unit; the reply will contain network configuration information. This information is listed in the bootptab file for that particular unit (identified by its hardware address). The unit then boots using the information sent to it. If no matching ethernet address is found the BOOTP server does not reply; the unit boots from internal memory.

The BOOTP response contains network configuration information; e.g. ip address, subnet mask, broadcast address. It may also contain details of a bootfile (not mandatory).

A bootfile (if you specify one) contains a unit's specific boot information; e.g. authentication method of users, access permission for the GUI. It may also contain details of other files (not mandatory); e.g. software version, language files and a general configuration file.

A configuration file (if you specify one) contains general configuration parameters; these parameters will have been created from another unit and saved to a file.

In the bootp response the minimum parameters to specify are **:ht** and **:ha**

There is no minimum number of parameters to specify in the bootfile or configuration file; unspecified parameters will remain unchanged in the unit's memory.

After processing the BOOTP response the unit will download additional files. If a bootfile is specified, the unit will then download that bootfile (using tftp). If the bootfile specifies other files e.g. a software file, the unit will compare that filename with the filename in its memory; if it has changed the unit will then download that other file using tftp. If the filename has not changed the unit will not download it.

**Note**     *In the bootp response you do not have to specify a bootfile. In the bootfile you do not have to specify other files, such as the software file. If you wish, you can make an entry in the bootptab file only.*

## How to setup BOOTP

Your nominated BOOTP server should be on the same network as the unit(s). The BOOTP server can also be on a different segment of the same network, provided that segment is connected by a bridge.

You can locate your BOOTP server on another network to the unit; this means that the bootp request and replies have to pass through a router or gateway. You must configure your router or gateway:

- to pass through BOOTP requests and replies
- for RIP

Note that if you have an existing unit, you do *not* have to enter the details of the gateway or router into the unit before using bootp. Details of gateways or routers pre-configured in the unit will be ignored during the bootp process.

## The bootptab file entry

Find the bootptab file on the host; on UNIX systems the bootptab file is usually file /etc/bootptab. Make an entry for the unit; an example for a single unit is shown at bootptab file entry for a single unit on page 229 on page 229. An example for multiple units is shown at bootptab file entry for multiple units on page 234.

*bootptab file  
entry for a single  
unit*

```
cs9000_blue:\n\n:ht=1:\n:ha=0080ba000057:\n:ip=192.101.34.211:\n:ds=192.65.144.44:\n:sm=255.255.255.224:\n:hn:\n:bf=/tmp/cs9000p.bfc:\n:dn=xxxx.co.uk:\n:gw=192.101.35.254
```

This entry should include the ethernet address of the unit. Other standard BOOTP tags which the unit supports are listed below, together with the unit's interpretation:

- ht** (hardware type) set to 1 (=10Mb ethernet).
- ha** (hardware address) the ethernet address of the unit.
- ip** (internet address) enter the ip address to assign to the unit.
- sm** (subnet mask) enter the subnet mask of the unit.
- hn** (host name) enter as :hn:\ which causes the name at the start of the **file** (cs9000\_blue) to be allocated to this unit.
- bf** (bootfile name) enter the name of the file containing specific configuration information; see An example bootfile on page 231.

**ds** (domain servers) enter the ip address of up to two nameservers.  
**gw** (gateway) enter the ip address of a single passive gateway

Caution

*use the 'gw' flag only in very specific circumstances; see Note 5. below.*

Notes on the above BOOTP tags:

1. Specify the fields that you wish; you do not have to specify all of them. E.g. if you wish to download only the internet address to the unit, specify the **ip** field (you must specify - as a minimum - the **ha** and **ht** fields).
2. If the subnet mask (**sm**) has not been explicitly specified by a BOOTPREPLY packet, it will be derived from the class of internet address.
3. If domain name servers are specified their port number will always be set to the default for a name server (53).
4. If you require a bootfile (**bf**) it must be on the same host as the bootptab file entry.
5. include the **gw** (gateway) flag only if your BOOTP server is on a different network and your gateway (or router) is *not* configured to support RIP.

The effect of using the '**gw**' field is:

- to make only this gateway available in the unit; it will be a passive gateway. You can view the details of the gateway only in the cli, using the 'show rip peers' command.
- to turn off RIP in the unit; i.e. the unit will ignore RIP messages broadcast on the network
- the unit will ignore gateways pre-configured in the unit or added after boot-up. It will respond only to the single gateway.
- you delete the gateway as follows: omit the '**gw**' field in the bootptab file entry and re-boot the unit. You can now add/configure active and passive gateways into the unit.

Gateways are detailed in Section Chapter 2 Installation.

## The bootfile

If you wish to download basic configuration information to the unit you must create a bootfile. This file is a text file formatted in a particular style; an example is shown at An example bootfile on page 231.

**Note** *The bootfile must be located on the same host as the boottab file*  
*An example bootfile*

```
# cat cs9000p.bfc

SW_FILE192.65.144.95:/src/pscx/sw/cs9000.bin
CONFIG_FILE192.65.144.95:/src/pscx/cfg/jconfig.0183
GUI_ACCESSYes
AUTH_TYPE0
IP_HOST192.101.34.199
SECURITYno
TFTP_RETRY3
TFTP_TMOUT21
EXTRA_TERM1192.65.144.95:/src/pscx/et/et1.0183
EXTRA_TERM2192.65.144.95:/src/pscx/et/et2.0183
EXTRA_TERM3192.65.144.95:/src/pscx/et/et3.0183

#
```

Notes on the above example:

1. The bootfile can have line entries for other files, e.g. a software or configuration file. The unit will download these files only if the filename has changed (excludes the pathname).
2. The format of each line entry in the file is:  
PARAMETER\_NAME <white space> parameter value  
<carriage return/line feed>
3. The parameter name must be in UPPER CASE and match exactly the strings shown in An example bootfile on page 231; e.g. AUTH\_TYPE.
4. An explanation of these parameters is shown in Bootfile parameters on page 232.
5. Include only those parameters which you want to configure. For example you may not wish to download a configuration file, so omit the line beginning CONFIG\_FILE (or precede the line with a hash # character).
6. If a domain name and nameserver are configured, either in the boottab entry or in the unit's memory, you can replace ip addresses with hostnames in lines specifying additional files; e.g.

```
SW_FILESophocles:/src/pscx/sw/cs9000.bin
```

Table 2 Bootfile parameters

Parameter	Value	Brief Meaning	Fuller explanation
SW_FILE	a filename and a full pathname - all pre-fixed by hostname/ip address	a version of software	<a href="#">Appendix D Upgrading your firmware</a>
CONFIG_FILE	a filename and full pathname - all pre-fixed by hostname/ip address	a set of saved configuration parameters from an existing unit. Note: these parameters include user passwords.	configuration parameters which are not listed in the BOOTPTAB file entry or in the bootfile. The parameters will not overwrite network configuration parameters specified in your bootfile.
GUI_ACCESS	on, off	access to the unit from a web browser	<a href="#">Chapter 2 Installation</a>
AUTH_TYPE	0 = both(local+RADIUS) 1 = local only 2 = RADIUS only 3 = both(RADIUS+local)	authentication method employed by the unit for all users	<a href="#">Chapter 2 Installation</a>
IP_HOST	ip address in dot decimal notation	default ip host for a user when user service is set to 'telnet' 'rlogin' or 'tcp clear'	
SECURITY	on, off	'reverse Telnet' line types, and remote configuration - all restricted to devices listed in the the unit's host table	
TFTP_RETRY	numeric; e.g. 5	number of tftp attempts before aborting	<a href="#">TFTP configuration on page 216</a>
TFTP_TMOU	numeric; e.g. 3	period in seconds before retrying a download/upload	<a href="#">TFTP configuration on page 216</a>
EXTRA_TERM1 (or 2, or 3)	a filename and full pathname - all prefixed by a hostname/ip address	termcap files for specific terminal types	

## BOOTP messages output to screen

The unit will output BOOTP messages to your screen during bootup, provided you are connected to the unit via its Admin Port.

On bootup the unit will always send a BOOTP request to BOOTP servers, so you will see the message:

```
INIT: attempting BOOTP
```

If the unit does not receive a BOOTP reply you will see the message:

```
INIT: no bootphost/server found on this network
```

If you want the unit to boot from a BOOT server then this message means BOOTP is not working. Consult [Appendix I Troubleshooting](#) for help.

## Disabling the BOOTP reply

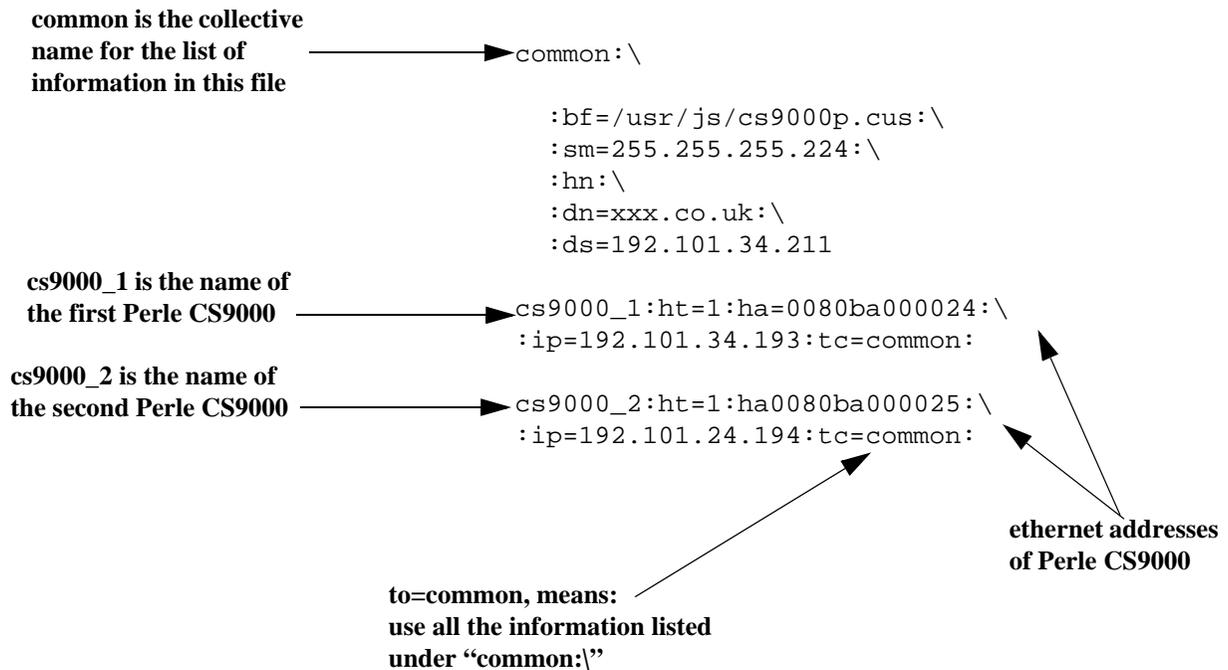
You cannot disable BOOTP in the unit; however, you can stop the BOOTP host from sending a BOOTP reply to the unit. You stop the reply by placing a hash # character in the bootptab file entry as follows:

- in bootptab file entry for a single unit on page 229 on page 229, place a hash before all the lines, e.g.  
# :ht=1:\  
# :ha=0080ba000057:\  
..  
# :gw=192.101.35.254:\
- in bootptab file entry for multiple units on page 234 you would place a hash before the line referring to each unit; e.g:  
# cs9000\_2:ht=1:ha=0080ba000025:\  
# ip=192.101.34.194:tc=common:

# Booting multiple units

You can boot multiple unit's simultaneously using BOOTP; we recommend you alter the format of your bootptab file entry, as shown in bootptab file entry for multiple units on page 234. You make one set of parameters in a single area (in this example 'common') and point each unit's entry to this area called 'common'.

*bootptab file  
entry for multiple  
units*



Notes on the above figure:

1. The example shown is for the Perle CS9000.
2. List each unit at the bottom of the file.
3. So that all units use the same BOOTP information, terminate each unit's entry with the same syntax, using the format `tc=name` (in the example above `tc=common`).
4. You will see that all the unit's are being directed towards the same bootfile (as listed in the 'bf' field in the area 'common'). This is acceptable - however all your the unit's will have the same configuration parameters.
5. The bootfile must be on the same host as the bootptab file entry.

## Multiple BOOTP servers

You may well wish to have a secondary BOOTP server as a back-up to the primary BOOTP server.

The unit will operate with BOOTP when you have a second, third or more BOOTP servers on your network. During a reboot the unit processes the first BOOTP reply received and ignores subsequent replies. If the bootptab file entries are identical on all your BOOTP servers the first reply received by the unit will be the same as the other replies.

The rules for multiple BOOTP servers are:

- we recommend they are located on the same network; however if they are on different network see the advice at How to setup BOOTP on page 229
- if you specify a bootfile (**bf**), each BOOTP server must contain an identical copy of this bootfile
- the software file (**SW\_FILE**) and/or configuration file (**CONFIG\_FILE**) can be located on any host; they do not have to be on the BOOTP server machines

## Example of BOOTP

Here is a working example of BOOTP, used to download a new version of software. We are using tftp with the 'secure' option:

1. If possible choose a BOOTP server which is located on the same network as the unit. Our BOOTP server was located like this.
2. Enable BOOTP on the machine you have chosen as the BOOTP server. E.g. on our SCO Open Server 5 machine we modified file /etc/inetd.conf, as follows:

```
tftp dgram udp wait root /etc/tftpd tftpd -s /tftpboot
bootps dgram udp wait root /etc/bootpd bootpd -c/tftpboot
```
3. Reboot the BOOTP server to ensure that BOOTP is operating.
4. Make an entry in file /etc/bootptab for your unit; e.g.

*Our example  
entry in a  
BOOTPTAB file*

```
cs9000_3:\  
  
:ht=1:\  
:ha=0080BA00004b:\  
:ip=192.65.146.120:\  
:ds=192.165.144.6:\  
:sm=255.255.255.0:\  
:hn:\  
:bf=/test:\  
:dn=xxxx.co.uk
```

5. Create the bootfile specified in the above entry; i.e. file 'test':

*Our example  
bootfile*

```
# cat test  
  
SW_FILE192.65.146.71:/cs9000.fl5  
GUI_ACCESSyes  
AUTH_TYPE0  
IP_HOST192.65.146.71  
SECURITYno  
TFTP_RETRY3  
EXTRA_TERM1homer:/src/pscx/et/et1.0183  
EXTRA_TERM2homer:/src/pscx/et/et2.0183  
EXTRA_TERM3homer:/src/pscx/et/et3.0183  
  
#
```

6. In the bootfile (above) we specified the software file(SW\_FILE). Specify the pathname for the file; in our example we placed the software file in the same directory as the bootfile.
7. Reboot the unit. After receiving details from the bootptab file, the unit should download the bootfile and the software file. The unit should then place the new software file into FLASH memory.

# Appendix G JETset

*You need to read this appendix if you want information on the Perle CS9000 JETset utility.*  
*this appendix if* This appendix provides task orientated information on using the CS9000 JETset utility.  
*you want to...*

This appendix includes the following sections;

- [Introduction to JETset on page 238](#)
- [Using JETset on page 240](#)
- [JETset program summary on page 243](#)

# Introduction to JETset

Once you have allocated an ip address, you can use the Graphical User Interface, named 'JETset'. This is a web-based program which you access from the web browser on your networked PC/computer. See [JETset home page on page 238](#). A summary of the program is in [JETset program summary on page 243](#).

*JETset home page*

Product logo will display the name of your product



**CS9000**

<u>line</u>	<u>user</u>
<u>server</u>	<u>line access</u>
<u>gateway</u>	<u>host</u>
<u>radius</u>	<u>nameserver</u>
<u>ppp</u>	<u>modem</u>
<u>snmp</u>	<u>slip</u>
<u>admin</u>	<u>file transfer</u>

Copyright © 2003 Perle.  
All Rights Reserved.

**server configuration**

---

servername	<input type="text" value="Eng_Server"/>
domain name	<input type="text" value="perle.com"/>
internet address	<input type="text" value="172.16.48.9"/>
subnet mask	<input type="text" value="255.255.0.0"/>
broadcast address	<input type="text" value="172.16.255.255"/>
authentication	<input type="text" value="local"/>
ssh protocol	<input type="text" value="ssh-1"/>
ssh break string	<input type="text" value="^break"/>
port buffering	<input type="text" value="local"/>
view port buffer string	<input type="text" value="^view"/>
nfs host	<input type="text" value="log_system"/>
nfs directory	<input type="text" value="/cs9000/portlogs"/>
nfs encryption	<input type="text" value="off"/>
line menu string	<input type="text" value="^menu"/>
reverse session limit	<input type="text" value="16"/>
dhcp	<input type="text" value="off"/>
services	<input type="text" value="fffc"/>
break	<input type="text" value="off"/>
banner	<input type="text" value="off"/>
security	<input type="text" value="off"/>
prompt with name	<input type="text" value="off"/>

To access JETset



Address  http://192.168.0.101/

## Perle JETset

The web based configuration utility for **CONSOLESERVER 9000**

Enter the password for the **admin** user then click the login button

**password**

1. Make sure you set 'gui\_access' to 'on', see [Chapter 2 Installation](#)
2. Open your web browser and enter the ip address of your Perle CS9000; e.g.

`http://192.101.34.211`

You should be presented with the login page:

The program prompts you for a password (for user of name 'admin').

---

**Caution**

---

*the only access permitted is username 'admin'. Perle CS9000 assumes this username and so prompts you for the password for this user.*

On successful login you will be presented with the JETset home page ([JETset home page on page 238](#) on page 238). From the home page you can now configure your unit.

# Using JETset

using JETset

Navigate by selecting these buttons



If you have made changes, remember to save them before moving to another option





**CS9000**

line	user
<a href="#">server</a>	<a href="#">line access</a>
<a href="#">gateway</a>	<a href="#">host</a>
<a href="#">radius</a>	<a href="#">nameserver</a>
<a href="#">ppp</a>	<a href="#">modem</a>
<a href="#">snmp</a>	<a href="#">slip</a>
<a href="#">admin</a>	<a href="#">file transfer</a>

Copyright © 2003 Perle  
All Rights Reserved.

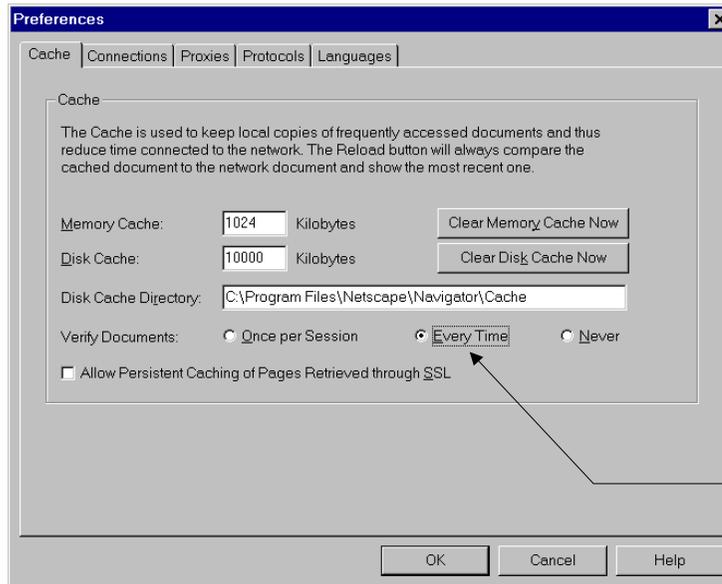
**server configuration**

servername	<input type="text" value="Eng_Server"/>
domain name	<input type="text" value="perle.com"/>
internet address	<input type="text" value="172.16.48.9"/>
subnet mask	<input type="text" value="255.255.0.0"/>
broadcast address	<input type="text" value="172.16.255.255"/>
authentication	<input type="text" value="local"/>
ssh protocol	<input type="text" value="ssh-1"/>
ssh break string	<input type="text" value="^break"/>
port buffering	<input type="text" value="local"/>
view port buffer string	<input type="text" value="^view"/>
nfs host	<input type="text" value="log_system"/>
nfs directory	<input type="text" value="/cs9000/portlogs"/>
nfs encryption	<input type="text" value="off"/>
line menu string	<input type="text" value="^menu"/>
reverse session limit	<input type="text" value="16"/>
dhcp	<input type="text" value="off"/>
services	<input type="text" value="fffc"/>
break	<input type="text" value="off"/>
banner	<input type="text" value="off"/>
security	<input type="text" value="off"/>
prompt with name	<input type="text" value="off"/>

Note the following guidelines about JETset:

- JETset uses the 'Frames' feature of HTML, which allows you to see four different 'windows' simultaneously inside your main browser window. This viewing method will make configuration easier. However, in common with all programs which use Frames there are particular ways of using JETset:
  - navigate using the main JETset buttons (see [using JETset on page 240](#)); we do not recommend using the 'Forward' or 'Backward' buttons of your Browser
  - set your browser to always check if there is a newer version of the page than the version stored in cache. This action will ensure that JETset will display the most up-to-date information; see [Netscape Navigator - configuration on page 240](#) and [Internet Explorer - configuration on page 241](#).

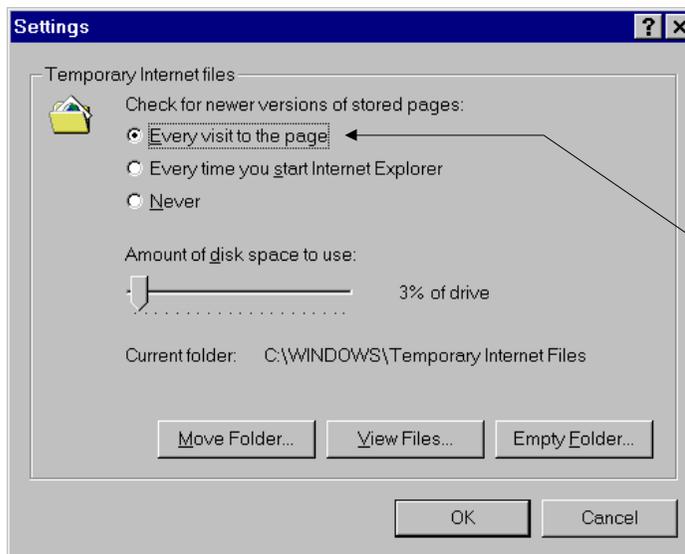
*Netscape  
Navigator -  
configuration*



in the 'Preferences' dialog box, click on the 'every time' radio button

- press the JETset 'Save' button before moving from one area, e.g. 'line' to another area, e.g. 'user'; see [using JETset on page 240](#). This action will save your changes in volatile memory (RAM); the saving process is instantaneous.
- to save your configuration changes to non-volatile memory, press the 'Admin' button and then select the 'Save to FLASH' button. The unit will spend a few seconds writing to FLASH memory, so we suggest you save to FLASH periodically (e.g. once every thirty minutes)

### Internet Explorer - configuration



in the 'Settings' dialog box, click on the 'every visit to the page' radio button

- if you visit another URL (address on the World Wide Web) and then wish to return to JETset you can either:
  - use the 'JETset' bookmark/favourite entry (the JETset home page), or
  - use the 'Go' feature of your browser (if 'JETset' is listed - this is the JETset home page), or
  - re-type the ip address of the unit in your 'location' field; e.g.  
`http://192.101.34.211`  
the login page will be displayed; you will need to login again.

## JETset program summary

- compatible with Microsoft Internet Explorer® or Netscape Navigator®, both at version 3 or more recent versions
- you can configure most Perle CS9000 parameters
- access is restricted to the person with username 'admin'
- you can use the 'bookmark/add to favourites' feature of your browser only with the login and home pages
- you can use the 'Go' navigation method of your browser (history file) of your browser only with the login and home pages



# Appendix H Radius Attributes

*You need to read this appendix if you want to...* You need to read this appendix if you want information regarding the RADIUS attributes supported on the Perle CS9000.

This appendix provides the specific attributes communicated between the CS9000 and the designated RADIUS host.

This appendix includes the following sections:

- [Access Request Messages on page 246](#)
- [Access-Accept Message on page 247](#)
- [Accounting Message on page 249](#)
- [Perle Specific RADIUS Attributes on page 251](#)

## Access Request Messages

This section describes the attributes which will be included by the CS9000 when requesting authentication from a RADIUS server.

*Access Request  
Message  
attributes*

<b>Number</b>	<b>Name</b>	<b>Description</b>
1	User Name	The name of the user to be authenticated
2	User Password	The password of the user to be authenticated
4	NAS IP Address	IP Address of the Console Server LAN interface
5	NAS Port	Line number of Console Server
6	Service Type	Indicates the service to use to connect the user to the Console Server

# Access-Accept Message

This section describes the attributes which will be accepted by the CS9000 from a RADIUS server in response to an authentication request.

*Access-Accept  
Message  
attributes*

Number	Name	Description
1	User Name	The name of the user to be authenticated
2	User Password	The password of the user to be authenticated
6	Service Type	Indicates the service to use to connect the user to the Console Server. A value of 6 indicates administrative access to the Console Server
7	Framed-Protocol	The link layer protocol to be used by this user.
8	Framed-IP-Address	The IP Address to be assigned to this user.
9	Framed-IP-Netmask	The subnet to be assigned to this user.
12	Framed MTU	Attribute indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means such as PPP.
13	Framed-Compression	Indicates a compression protocol to be used for PPP or SLIP link
14	Login IP Host	Indicates the host with which the user can connect to when the Login Service is included
15	Login Service	Indicates the service to sue to connect the user a host
16	Login TCP Port	Indicates the TCP port with which the user is to be connected when the Login Service is also present

Number	Name	Description
26	Vendor Specific	<p>Perle self defined attributes for line access rights and user level. See example <a href="#">Perle Specific RADIUS Attributes on page 251</a></p> <p>Line Access Rights for port n (1-24):  <i>Name: <b>Perle:Line-Access-Right-n</b> (where n is the line number)</i>  <i>Type: <b>100 +n</b></i>  <i>Data Type: <b>integer</b></i>  <i>Value: <b>Disabled (0), ReadWrite(1), ReadInput(2), ReadInputWrite (3), ReadOutput (4), ReadOutputWrite (5), ReadOutputInput (6), ReadOutputInputWrite (7),</b></i>            User Level:  <i>Name: <b>Perle:User-Level</b></i>  <i>Type: <b>100</b></i>  <i>Data Type: <b>integer</b></i>  <i>Value: <b>Admin(1), Normal(2), Restricted(3), Menu(4)</b></i></p>
27	Session-Timeout	Maximum number of seconds the user will be allowed to stay logged on.
28	Idle Timeout	Maximum number of consecutive seconds with no link activity before the connection is terminated.

# Accounting Message

This section describes the attributes which will be included by the CS9000 when sending an accounting message to the RADIUS server.

*Accounting  
Message  
attributes*

Number	Name	Description
1	User Name	The name of the user to be authenticated
4	NAS IP Address	IP Address of CS9000 LAN interface
5	NAS Port	Line number of CS9000
6	Service Type	Indicates the service to use to connect the user to the Console Server. A value of 6 indicates administrative access to the Console Server
40	Acct-Status-Type	Indicates if this is the beginning or end of a session. Supported values are: 1 = Start 2 = Stop
42	Acct-Input-Octets	Number of bytes which were received from the user during this session.
43	Acct-Output-Octets	Number of bytes where were transmitted to the user during this session.
44	Acct-Session-ID	A string which identifies the session. The same string must be used in the start and stop messages.
45	Acct-Authentic	Indicates how the user was authenticated. Supported values are: 1 = Local 2 = RADIUS
46	Acct-Session-Time	Number of seconds for which the user has been connected to a specific session.
47	Acct-Input-Packets	Number of packets which were received from the user during this session.
48	Acct-Output Packets	Number of packets which were transmitted to the user during this session.

Number	Name	Description
49	Acct-Terminate-Cause	Indicates how the session was terminated: Supported values include: 1 = User Request 2= Lost Carrier 3=Lost Service 4= Idle Timeout 5= Session Timeout 14 = Port Suspended 16 = Callback

## Perle Specific RADIUS Attributes

The CS9000 has defined Vendor Specific RADIUS attributes in order for the RADIUS server to be configured to support the Console Server features of Line Access Rights and User Level. These attributes have been defined in [Access-Accept Message on page 247](#) to allow the RADIUS server to be configured for RADIUS users to have this level of configuration.

See below for an example of the Perle defined attributes for the RADIUS server for a 24 Port Console Server:

```
#
# Perle dictionary.
#
#           Perle Systems Ltd.
#           http://www.perle.com/
#
#           Enable by putting the line "$INCLUDE dictionary.perle" into
#           the main dictionary file.
#
# Version:      1.00 17-Jul-2003 contributed by Tianxin Li
#

VENDOR      Perle      1966

#           Perle Extensions

ATTRIBUTE   Perle-User-Level      100      integer Perle
ATTRIBUTE   Perle-Line-Access-Port-1  101      integer Perle
ATTRIBUTE   Perle-Line-Access-Port-2  102      integer Perle
ATTRIBUTE   Perle-Line-Access-Port-3  103      integer Perle
ATTRIBUTE   Perle-Line-Access-Port-4  104      integer Perle
ATTRIBUTE   Perle-Line-Access-Port-5  105      integer Perle
ATTRIBUTE   Perle-Line-Access-Port-6  106      integer Perle
ATTRIBUTE   Perle-Line-Access-Port-7  107      integer Perle
```

ATTRIBUTE	Perle-Line-Access-Port-8	108	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-9	109	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-10	110	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-11	111	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-12	112	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-13	113	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-14	114	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-15	115	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-16	116	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-17	117	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-18	118	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-19	119	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-20	120	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-21	121	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-22	122	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-23	123	integer Perle
ATTRIBUTE	Perle-Line-Access-Port-24	124	integer Perle

# Perle User Level Values

VALUE	Perle-User-Level	
VALUE	Perle-User-Level Restricted	3
VALUE	Perle-User-Level Menu	4

# Perle Line Access Right Values

VALUE	Perle-Line-Access-Port-1	Disabled	0
VALUE	Perle-Line-Access-Port-1	Read-Write	1

VALUE	Perle-Line-Access-Port-2	Disabled	0
VALUE	Perle-Line-Access-Port-2	Read-Write	1
VALUE	Perle-Line-Access-Port-3	Disabled	0
VALUE	Perle-Line-Access-Port-3	Read-Write	1
VALUE	Perle-Line-Access-Port-4	Disabled	0
VALUE	Perle-Line-Access-Port-4	Read-Write	1
VALUE	Perle-Line-Access-Port-5	Disabled	0
VALUE	Perle-Line-Access-Port-5	Read-Write	1
VALUE	Perle-Line-Access-Port-6	Disabled	0
VALUE	Perle-Line-Access-Port-6	Read-Write	1
VALUE	Perle-Line-Access-Port-7	Disabled	0
VALUE	Perle-Line-Access-Port-7	Read-Write	1
VALUE	Perle-Line-Access-Port-8	Disabled	0
VALUE	Perle-Line-Access-Port-8	Read-Write	1
VALUE	Perle-Line-Access-Port-9	Disabled	0
VALUE	Perle-Line-Access-Port-9	Read-Write	1
VALUE	Perle-Line-Access-Port-10	Disabled	0
VALUE	Perle-Line-Access-Port-10	Read-Write	1
VALUE	Perle-Line-Access-Port-11	Disabled	0

VALUE	Perle-Line-Access-Port-11	Read-Write	1
VALUE	Perle-Line-Access-Port-12	Disabled	0
VALUE	Perle-Line-Access-Port-12	Read-Write	1
VALUE	Perle-Line-Access-Port-13	Disabled	0
VALUE	Perle-Line-Access-Port-13	Read-Write	1
VALUE	Perle-Line-Access-Port-14	Disabled	0
VALUE	Perle-Line-Access-Port-14	Read-Write	1
VALUE	Perle-Line-Access-Port-15	Disabled	0
VALUE	Perle-Line-Access-Port-15	Read-Write	1
VALUE	Perle-Line-Access-Port-16	Disabled	0
VALUE	Perle-Line-Access-Port-16	Read-Write	1
VALUE	Perle-Line-Access-Port-17	Disabled	0
VALUE	Perle-Line-Access-Port-17	Read-Write	1
VALUE	Perle-Line-Access-Port-18	Disabled	0
VALUE	Perle-Line-Access-Port-18	Read-Write	1
VALUE	Perle-Line-Access-Port-19	Disabled	0
VALUE	Perle-Line-Access-Port-19	Read-Write	1
VALUE	Perle-Line-Access-Port-20	Disabled	0
VALUE	Perle-Line-Access-Port-20	Read-Write	1

VALUE	Perle-Line-Access-Port-21	Disabled	0
VALUE	Perle-Line-Access-Port-21	Read-Write	1
VALUE	Perle-Line-Access-Port-22	Disabled	0
VALUE	Perle-Line-Access-Port-22	Read-Write	1
VALUE	Perle-Line-Access-Port-23	Disabled	0
VALUE	Perle-Line-Access-Port-23	Read-Write	1
VALUE	Perle-Line-Access-Port-24	Disabled	0
VALUE	Perle-Line-Access-Port-24	Read-Write	1



# Appendix I Troubleshooting

*You need to read this appendix if you want information on troubleshooting the Perle CS9000.*  
*this appendix if* This appendix provides information on troubleshooting the Perle CS9000.  
*you want to...*

This appendix includes the following sections;

- [Introduction on page 258](#)
- [General communication matters on page 258](#)
- [Host problems on page 259](#)
- [JETset problems on page 260](#)
- [Login problems on page 261](#)
- [Problems with terminals on page 262](#)
- [Emergency recovery on page 263](#)
- [Problems with framed Routing on page 263](#)

## Introduction

This appendix contains solutions for problems that may arise while Perle CS9000 (the 'unit').

- if you bought your unit from a registered Perle Supplier, you must contact their Technical Support department; they are qualified to deal with your problem.
- if you are a registered Perle Supplier, and bought your unit from Perle, please contact the Technical Support department of your nearest Perle office. The addresses and telephone numbers of your nearest Perle office are contained in [Appendix J Contacting Perle](#).

## General communication matters

General communication checks and practices are as follows:

- ping your host; if you cannot ping at all, check the cabling between the unit and your network. If you can ping but packet loss is reported, ping another host/device on the same network. You will appreciate whether the problem is specific to a host/device or general to the network. If there is a problem with the network check the state of the network, including number of nodes.
- after entering or changing ip information for your unit (internet address, broadcast address, subnet mask) *reboot the unit* (does not apply when using BOOTP or DHCP). Once the unit has rebooted other network devices can communicate with it (ping, telnet, etc.). Also, protocols such as ARP and proxy-ARP will work properly  
  
If you don't reboot unit the ip information you have entered/changed will not be recognised by other network devices.
- use the *show routes* command (command line only). See if there a route to the host?
- implement load-balancing in your network by distributing the processing. For example, try not to cluster on the unit devices which require high throughput.
- ensure routes to/from your host are as direct as possible; e.g. ensure the unit is on the same network as your host so that bridges/routers do not act as bottlenecks.
- if your network is congested, subnet it with a bridge; however, bear in mind the recommendations in the previous paragraph.

## Host problems

### Cannot access a host by name

- if using DNS or if DNS is required, ensure a nameserver is configured on your unit and is accessible (ping it).
- if not using DNS, ensure the host is configured in the host table. Check access to the host by pinging it using the host's IP address.

### Cannot access a host on a local network

ensure:

- the network address is correct.
- the subnet mask is set correctly and reflects the network configuration.
- the broadcast address is set correctly and reflects the network configuration.

### Cannot access a host on a remote network

- use the *show route* command to verify that there is a route to the remote host. If no gateway is specified, ensure a default gateway is specified. Ping the default gateway to check if it is working.
- Consider the situation beyond the gateway; e.g. are intermediate gateways and the remote host available? Also, check the messages returned by the *show route* command; e.g. that a particular host or gateway is unreachable.

### Gateways added into the gateway table are ignored by the unit

- have you used BOOTP and entered a single static gateway in the bootptab file entry? If yes, the other gateways will be ignored. See [Appendix F BOOTP](#) for more information

### Access to host lost after a few minutes

- If the route to this host goes through routers, make sure those routers are all sending RIP packets across the networks.

### You see a message saying your host is in use.

- delete your host as either, a DNS or WINS host, or a gateway, then retry the 'delete host' command/menu item. You may have configured your host as a DNS or WINS host, or a gateway.

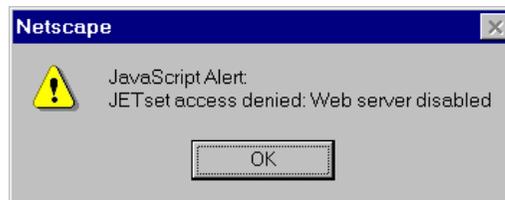
The connection fails when the user 'ip\_host' parameter is set to 0.0.0.0

other factors: several hosts are entered in the unit's host table

- check the host ip address entered in the server configuration; it is this ip address - and not hosts in the host table - which the unit will use when a user's ip\_host is set to 0.0.0.0

## JETset problems

Trying to access JETSET you see an 'alert' dialog box, e.g. :



- change the parameter 'gui\_access' to 'on'.

# Login problems

## User is waiting up to 60 seconds before login is accepted or denied

other factors: authentication is set to 'both' or 'RADIUS'. User has entered username and password, and has pressed <return> key.

- check RADIUS configuration of primary and secondary authentication/accounting hosts specified, and you have retry and timeout values greater than the default, the unit will be spending time trying each of these hosts and keeping the user waiting.
- adjust RADIUS configuration: specify just one host, reduce timeout and retry values to the default or less than default.
- when connecting using a reverse ssh connection, a delay of about 10 seconds for SSH version 1 will be experienced. A delay of 20 seconds for SSH version 2 will be experienced. These delays are due to the negotiation of a secure LAN connection. This involves the exchanging of encryption messages to establish a secure communication.

## You cannot progress beyond the 'login' and 'password' prompts (when authentication is set to either 'both' or 'RADIUS')

- check the setting of 'account\_authenticator' flag is the same in the unit and the RADIUS host; either they should both check or both ignore the authenticator field. If you are not sure, change the setting in the unit; see if this fixes the problem.
- on the RADIUS host check the secret (password); you should see it displayed in clear text in the RADIUS clients file. If you are unsure whether it is the same secret which you entered in the unit, go to the unit and re-enter a new secret.
- on the RADIUS host check there is only one entry for a particular user; do not have multiple entries of the same username (although passwords may be different).

## You cannot obtain a login on *any* of the front-mounted ports

- Connect via the Admin port and check the settings of the front-mounted ports; they have probably been set to 'direct' or 'silent' telnet/rlogin.

## You have lost or don't know your password (as 'admin' user)

- You must reset the unit to its factory default settings. The configuration will be erased and the default setting will be applied when you Jetload the firmware to the CS9000.

## at the remote end the client software locks up

other factors: security (CHAP) is enabled on the line.

- disable CHAP re-challenge parameter (challenge\_interval) in the unit. Some PPP client software does not work when receiving CHAP re-challenges.

## Problems with terminals

*see also:* [Login problems on page 261](#).

The following section concerns problems with the appearance of data on your terminal screen:

### The unit logs me out after a few minutes

- Change the idle timeout value set for the user. The idle timeout for all users is set to 0 seconds by default so that the ports will never timeout, because the unit is designed for remote access connections (using SLIP or PPP).

### Corrupt data

- check your line settings (baud rate, stop bits, etc.)

### Missing data

- ensure the same type of flow control is set in both your terminal and on the unit's port.

### Error message 'not permitted on a dumb terminal' after typing the cli command 'screen'

- set your line to 'termtype' VT100, ansi or Wyse60 (or other form of terminal emulation, if you have downloaded one). The default line type in the unit is 'dumb' which does not support the graphics characters necessary to view the text-based menus.

### Screen corruption when using the text-based menu system

- check that the terminal setup in the unit matches your terminal.
- check that entries in the term file match your terminal setup.
- if using a PC/computer, ensure the type of terminal emulation selected in your application matches those supported by the unit. If you still have the problem, you may be suffering with poorly written terminal emulation in your application. Instead use the command line mode; if you have a web browser use JETset.

## Emergency recovery

**Problem:**

You have a unit already configured and,

- you do know your password, but
- have lost, misconfigured or don't know the IP address of the unit, and
- you cannot obtain a login on any port (including the console port)

The emergency recovery method is to use BOOTP (see [Appendix F BOOTP](#)).

- Setup a host machine on your network to run BOOTP. Using the ethernet address of the unit (printed on the base of the product) BOOTP will assign the unit a known IP address.
- Now, you should be able to telnet into the unit and change its IP address.

Using BOOTP to recover access to your unit in this manner will preserve all configuration settings - apart from the IP address.

## Problems with framed Routing

**Problem:** My SLIP/PPP link is running but I am not seeing any routing information propagated to my dial up clients.

**Check:** Make sure that SLIP/PPP links are configured for route broadcasts, see section 9.1. Wait for 30 seconds before checking again for new routes, routes are broadcast every 30 seconds.

**Problem:** I can talk to my dial-up clients, but not any other machine on the network it is attached to.

**Check:** Make sure that your dial-up client is configured to pass on RIP ( routing ) packets to it's other network interfaces. This may involve installing additional routing software on some operating systems.

**Problem:** I have configured framed routing for a SLIP/PPP link but routing does not work.

**Check:** Both Remote IP Address and Local IP Address need to be configured with valid IP addresses for framed routing to remote clients to operate.



## Appendix J Contacting Perle

*You need to read this appendix if you want to contact Perle for technical support or any other queries about this product.*

*you want to...*

This appendix includes the following sections;

- [Making a technical support query on page 266](#)
- [Repair procedure on page 269](#)
- [Perle support centres worldwide on page 270](#)
- [Perle support centres worldwide on page 270](#)

*Internet access*

[Click here to access the our website at the following URL:  
http://www.perle.com](http://www.perle.com)

*Email*

[Click here to email Perle at the following address;  
Email: ptac@perle.com](mailto:ptac@perle.com)

## Making a technical support query

This section contains the following information about making a query;

- [Who to contact on page 266](#)
- [Information needed when making a query on page 267](#)
- [Making a support query via the Perle web page on page 268](#)

## Who to contact

If you bought your product from a registered Perle supplier, you must contact their Technical Support department; they are qualified to deal with your problem.

If you are a registered Perle supplier, and bought your product from Perle, contact Perle Technical Support at the offices listed below.

## Information needed when making a query

When you make a technical support enquiry please have the following information ready;

**Hint**  
Print out this page and fill in the table provided with the basic information you need.

Item	Write details here
Product name and version	
Problem description	
Operating system version	
Driver version	
Details of any other cards installed in your system	
Your name	
Company Name	
Country	
Phone number	
Fax number	
Email address (if available)	

## Making a support query via the Perle web page

If you have an internet connection, please send details of your problem to Technical Support using the email links provided on the Perle web site in the 'Support' area.

See also [Perle support centres worldwide on page 270](#) for email links and other contact details for the Perle technical support centres.

[Click here to access our website at the following URL:  
http://www.perle.com](http://www.perle.com)

## Repair procedure

Before sending a unit for repair, you must contact your Perle supplier. If, however, you bought your product directly from Perle you can contact directly. See [Perle support centres worldwide on page 270](#) for contact information.

Customers who are In Europe, Africa or Middle East can submit repair details via a website form shown in the next picture. This form is on the Perle website, [www.perle.com](http://www.perle.com), in the **Support** area.

[Click here to access our web site at the following URL:  
http://www.perle.com/support\\_services/rma\\_form.asp](http://www.perle.com/support_services/rma_form.asp)

In the USA and Asia contact the office shown in the Technical Support section.

## Perle support centres worldwide

**Note**

Perle offers free technical support to Perle Authorised Distributors and Registered Perle Resellers.

To access technical support please visit the Perle website at [www.perle.com/support\\_services/index.shtml](http://www.perle.com/support_services/index.shtml).

If you are unable to find the information you require, please feel free to contact our technical support teams by email using the addresses shown in the next table.

<b>Country</b>	<b>Address</b>	<b>Email</b>
<b>North America</b>	Perle Systems Ltd. 60 Renfrew Drive Markham Ontario Canada L3R OE1	<i>Email: <a href="mailto:ptac@perle.com">ptac@perle.com</a></i>
<b>Europe</b>	Perle Systems Europe Ltd. 3 Wintersells Road Byfleet Surrey KT14 7LF UK	<i>Email: <a href="mailto:ptac@perle.com">ptac@perle.com</a></i>
<b>Asia</b>	Perle Asia Pacific (Pte) Ltd. 190 Middle Road #19-05 Fortune Centre Singapore 188979	<i>Email: <a href="mailto:ptac@perle.com">ptac@perle.com</a></i>
<b>Worldwide</b>	Perle Systems Ltd. 60 Renfrew Drive Markham Ontario Canada L3R OE1	<i>Email: <a href="mailto:ptac@perle.com">ptac@perle.com</a></i>

## Index

### Numerics

9016 [22](#)  
9024 [22](#)  
9032 [22](#)  
9048 [22](#)

### A

accessing devices  
    using modems  
        on a dial in link [122](#), [125](#)  
        with dumb device [126](#)  
    using Telnet [115](#)  
add community [152](#)  
add DNS command [152](#)  
add gateway command [153](#)  
add host command [153](#)  
add modem command [154](#)  
add radius command [154](#), [159](#)  
add rip md5 command [155](#)  
add sntp server command [155](#)  
add trap command [155](#)  
add user command [156](#)  
add WINS command [156](#)  
admin command [156](#)  
AUI connector [135](#)

### B

BOOTP [225](#)

### C

cabling [133](#)  
CLI prompts [104](#)  
command  
    set sntp mode [183](#)  
    set summertime mode [184](#)  
commands [158](#)  
    add community [152](#)  
    add DNS [152](#)  
    add gateway [153](#)  
    add host [153](#)  
    add modem [154](#)  
    add radius [154](#), [159](#)  
    add rip md5 [155](#)  
    add sntp server [155](#)  
    add trap [155](#)  
    add user [156](#)  
    add WINS [156](#)  
admin [156](#)  
debug [156](#)  
delete community [157](#)  
delete DNS [157](#)  
delete gateway [157](#)  
delete host [158](#)  
delete radius [158](#)  
delete rip md5 [159](#)  
delete sntp [159](#)  
delete trap [159](#)  
delete user [159](#)  
delete WINS [160](#)  
heap [160](#)  
help [160](#)  
kill line [160](#)

## # A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- logout 161
- netload 162
- netsave 163
- ping 164
- reboot 165
- reset factory 165
- reset line 165
- reset user 166
- restart 166
- resume 166
- rlogin 167
- save 167
- screen 167
- set contact 168
- set date 168
- set gateway 169
- set host 169
- set line 170
- set location 172
- set port\_buffering 173
- set radius 175
- set rip 175
- set server 176
- set sntp mode 183
- set summertime mode 184
- set telnet 185
- set time 186
- set timezone offset 186
- set user 187
- show date 190
- show gateways 190
- show hardware 190
- show hosts 191
- show interfaces 191
- show line 191
- show modem 193
- show port\_buffering 194
- show radius 196
- show rip 196
- show rip peers 197
- show routes 197
- show server 198
- show snmp 200, 203
- show sntp 200
- show sntp\_info 201
- show summertime 202
- show telnet 202, 205
- show time 203
- show timezone 203
- show user 204
- start 204
- version 205
- connector pinouts 133
- console server
  - accessing devices using modems
    - on a dial in link 122, 125
    - using dumb device 126
  - accessing devices using Telnet 115
  - introduction to 114
- contacting Perle Systems
  - email 265
  - for technical support 266
  - internet 265
- CS9000
  - 9016 variant 22
  - 9024 variant 22
  - 9032 variant 22
  - 9048 variant 22
  - introduction to 21
  - using as console server 113
  - variants 22

## # A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

### D

date and time, setting [67](#)  
date, setting [67](#)  
debug command [156](#)  
delete community command [157](#)  
delete DNS command [157](#)  
delete gateway command [157](#)  
delete host command [158](#)  
delete modem [158](#)  
delete modem command [158](#)  
delete radius command [158](#)  
delete rip md5 command [159](#)  
delete snmp command [159](#)  
delete trap command [159](#)  
delete user command [159](#)  
delete WINS command [160](#)  
desk mounting [34](#)  
DHCP, setting up IP address with [39](#)  
dial in line, configuring [75](#)  
DNS, configuring [59](#)

### E

Easy Port Access [116](#)  
email [265](#)

### F

factory defaults, restoring [69](#)  
    using software [69](#)  
firmware, upgrading [213](#)  
FLASH memory [167](#)

### H

heap command [160](#)  
help command [160](#)  
host table, setting up [51](#)

### I

installation [31](#)  
installation, general procedure for [32](#)  
IP address  
    setting up  
        automatically using DHCP [39](#)  
        manually [43](#)  
IP address setting up [39](#)

### J

JETset [237](#)

### K

kill line command [160](#)

### L

LEDs, guide to [36](#)  
line  
    resetting to default [111](#)  
    settings, viewing and editing [73](#)  
Line Access Rights [103](#)  
line service types [221](#)  
Local Port Buffer [127](#)  
logging on [46](#)  
logout command [161](#)

## # A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

### M

mounting

desk [34](#)

rack [33](#)

multiple units, stacking [35](#)

multisession [122](#)

### N

netload command [162](#)

netsave command [163](#)

network gateways, configuring [61](#)

network installation verifying [65](#)

network parameters, host table [51](#)

network parameters, setting up [51](#)

### P

ping command [164](#)

Ports

AUI [135](#)

product repair form [269](#)

### R

rack mounting [33](#)

RADIUS, configuring [55](#)

reboot command [165](#)

rebooting, soft [68](#)

Remote Port Buffer [130](#)

repair procedure [269](#)

product repair form [269](#)

RMA form [269](#)

reset factory command [165](#)

reset line command [165](#)

reset user commands [166](#)

restart command [166](#)

resume command [166](#)

rlogin command [167](#)

RMA form [269](#)

### S

save command [167](#)

screen command [167](#)

set contact command [168](#)

set date command [168](#)

set gateway command [169](#)

set host command [169](#)

set line command [170](#)

set location command [172](#)

set port\_buffering command [173](#)

set ppp line [174](#)

set radius command [175](#)

set rip command [175](#)

set server command [176](#)

set sntp mode [183](#)

set sntp mode command [183](#)

set summertime mode command [184](#)

set telnet command [185](#)

set time command [186](#)

set timezone offset command [186](#)

set user commands [187](#)

settings, saving [112](#)

show [200](#), [201](#)

show date command [190](#)

show gateways command [190](#)

show hardware command [190](#)

show hosts command [191](#)

show interfaces command [191](#)

show line commands [191](#)

show modem command [193](#)

show port\_buffering command [194](#)

## # A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

show radius command [196](#)  
show rip command [196](#)  
show rip peers command [197](#)  
show routes command [197](#)  
show server command [198](#)  
show snmp command [200](#), [203](#)  
show sntp command [200](#)  
show sntp\_info command [201](#)  
show summertime command [202](#)  
show telnet command [202](#), [205](#)  
show time command [203](#)  
show timezone command [203](#)  
show user command [204](#)  
SNMP [207](#)  
    add community [152](#)  
    add trap [155](#)  
    delete community [157](#)  
    delete trap [159](#)  
soft reboot [68](#)  
SSH Setup [117](#)  
stacking multiple units [35](#)  
start command [204](#)  
system administration [71](#)

## T

technical support [266](#)  
    centres worldwide [270](#)  
    queries, information needed for [267](#)  
    via the internet [268](#)  
    who to contact [266](#)  
time, setting [67](#)  
troubleshooting [257](#)

## U

upgrading firmware [213](#)  
users  
    configuring [91](#)

## V

variants  
    9016 [22](#)  
    9024 [22](#)  
    9032 [22](#)  
    9048 [22](#)  
variants, CS9000 [22](#)  
version command [205](#)

## W

WINS, configuring [60](#)

# A B C D E F G H I J K L M N O P Q R S T U V W X Y Z