SLB™ Branch Office Manager User Guide
Intellectual Property

© 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

*Lantronix* is a registered trademark of Lantronix, Inc. in the U.S. and certain other countries. *Lantronix Spider* is a registered trademark, and *SLB, SLC, and vSLM* are trademarks of Lantronix, Inc.


*Windows* and *Internet Explorer* are registered trademarks of Microsoft Corporation. *Mozilla* and *Firefox* are registered trademarks of the Mozilla Foundation. *Chrome* is a trademark of Google, Inc. All other trademarks and trade names are the property of their respective holders.

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license or the GNU General Public License (GPL) as published by the Free Software Foundation (FSF). Lantronix grants you no right to receive source code to the Open Source software; however, in some cases, rights and access to source code for certain Open Source software may be available directly from Lantronix’ licensors. Upon request, Lantronix will identify the Open Source components and the licenses that apply to them. Your use of each Open Source component or software is subject to the terms of the applicable license. The GNU General Public License is available at [http://www.gnu.org/licenses/gpl.html](http://www.gnu.org/licenses/gpl.html).

Open Source Software is distributed WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. See the GPL and BSD for details.

Warranty

For details on the Lantronix warranty policy, please go to our Web site at [https://www.lantronix.com/technical-support/warranty/](https://www.lantronix.com/technical-support/warranty/).

Contacts

**Lantronix, Inc.**

48 Discovery
Suite 250
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

**Technical Support**

Online: [https://www.lantronix.com/technical-support/](https://www.lantronix.com/technical-support/)

**Sales Offices**

For a current list of our domestic and international sales offices, go to the Lantronix web site at [https://www.lantronix.com/about-us/contact/](https://www.lantronix.com/about-us/contact/).
Disclaimer & Revisions

All information contained herein is provided “AS IS.” Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Note: This equipment has been tested and found to comply with the limits for 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 this user guide, may cause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Changes or modifications to this device not explicitly approved by Lantronix will void the user’s authority to operate this device.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Rev.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2013</td>
<td>A</td>
<td>Initial Release (6.0).</td>
</tr>
<tr>
<td>June 2014</td>
<td>B</td>
<td>Added the new 200-240 VAC SLB model.</td>
</tr>
<tr>
<td>August 2014</td>
<td>C</td>
<td>Updated for firmware release 6.1.</td>
</tr>
<tr>
<td>January 2015</td>
<td>D</td>
<td>Updated technical specification information.</td>
</tr>
<tr>
<td>May 2016</td>
<td>E</td>
<td>Updated safety information.</td>
</tr>
<tr>
<td>December 2016</td>
<td>F</td>
<td>Updated to firmware revision 6.3.0.0, which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Removal of java from the WebSSH and WebTelnet application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Addition of transport security layer (TLS) 1.1 and 1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Upgrade of web SSL certificate to 2048 bits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Option to disable SSH DSA keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Zero touch provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Custom SSL certificate for the web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Compliance information updates</td>
</tr>
<tr>
<td>June 2018</td>
<td>G</td>
<td>Updated to firmware revision 6.5.0.0RC19.</td>
</tr>
<tr>
<td>October 2018</td>
<td>H</td>
<td>Updated to firmware revision 6.6, which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✦ Sierra gateway LTE modem integration</td>
</tr>
<tr>
<td>Month</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>March 2019</td>
<td>J</td>
<td>Updated to firmware revision 6.7.0.0RC12, which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Support for custom Expect scripts that can be connected to the SLB CLI or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a device port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Web and SSH support for SHA2 and higher</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ConsoleFlow access timeout settings</td>
</tr>
<tr>
<td>April 2019</td>
<td>K</td>
<td>Updated to firmware revision 6.8.0.0RC8, which includes support for Tcl and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Python custom scripts.</td>
</tr>
<tr>
<td>November 2019</td>
<td>L</td>
<td>Updated to firmware revision 7.0.0.0, which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Support for CLI commands issued from ConsoleFlow in bulk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Newly manufactured SLB units that come installed with firmware 7.0.0.0 or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>later use a device-unique default password for local user sysadmin</td>
</tr>
<tr>
<td>November 2020</td>
<td>M</td>
<td>Updated to firmware revision 7.4.0.0 which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added an option to select cloud or on-premise version of ConsoleFlow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>clients.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added option to configure Eth2 network port settings from the LCD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added System Info page in Maintenance, which generates ZIP file with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added Passthrough Mode for cellular gateway configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for importing ECDSA and ED25519 SSH host keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added factory reset via external storage device</td>
</tr>
<tr>
<td>December 2021</td>
<td>N</td>
<td>Updated to firmware version 7.5.0.1, which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for modem access list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added USB serial support on front USB port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Removed MQTT security option from ConsoleFlow configuration settings</td>
</tr>
<tr>
<td>September 2022</td>
<td>P</td>
<td>Updated to firmware version 7.6.0.0, which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for G520 series cellular gateway as failover gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added a feature to only start a VPN tunnel in network failover mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated CLI syntax</td>
</tr>
<tr>
<td>December 2023</td>
<td>R</td>
<td>Updated to firmware 7.7.0.0, which includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for configuring the timeout when connecting to a TACACS+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for audit log messages option for ConsoleFlow client</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added one time password option to for firmware update and configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>restore/save to bypass saving the FTP/SFTP/TFTP server login and password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the maximum number of rules allowed in an IP filter ruleset to 256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the CLI “show power” output to improve readability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated CLI syntax</td>
</tr>
</tbody>
</table>
## Table of Contents

Intellectual Property ................................................. 2
Open Source Software .................................................. 2
Warranty .................................................................. 2
Contacts .................................................................. 2
Disclaimer & Revisions ................................................ 3
Revision History .......................................................... 3
List of Figures ................................................................ 14
List of Tables ................................................................ 17

1: About this Guide ....................................................... 18
Purpose and Audience .................................................... 18
Summary of Chapters ..................................................... 18
Additional Documentation .............................................. 19

2: Introduction ............................................................... 20
Features ..................................................................... 20
  Console Management .................................................. 20
  Power Management Outlets for Power Connectivity .......... 20
  Power Inlets ............................................................. 20
  Integration with Other Secure Lantronix Products .......... 20
  Internal Temperature Sensor ......................................... 21
  Designed for Branch Offices and Similar Environments .... 21
  Typical Equipment ..................................................... 22
  Types of Business ...................................................... 22
  Benefits ................................................................ 22
Models ..................................................................... 23
System Features ............................................................ 24
  Protocols Supported .................................................. 24
  Access Control .......................................................... 25
  Power Outlet Control .................................................. 25
  Device Port Buffer ....................................................... 25
  Configuration Options .................................................. 25
Application Example ...................................................... 26
Hardware Features ........................................................ 27
  Serial Connections ....................................................... 27
  Network Connections .................................................... 28
  USB Interface ............................................................ 28
  Modem Interface ........................................................ 29
3: Installation

What's in the Box
Product Information Label
Technical Specifications
Safety Precautions
Cover
Power Plug
Input Supply
Grounding
Fuses
Rack
Port Connections
Physical Installation
Connecting to a Device Port
Connecting to Network Ports
Connecting Terminals
Connecting to the Internal Modem
Power
AC Input
Connecting Devices to Power Outlets
Typical Installations

4: Quick Setup

Recommendations
IP Address
Method #1 Using the Front Panel Display
Front Panel LCD Display and Keypads
Navigating
Entering the Settings
Restoring Factory Defaults
Limiting Sysadmin User Access
Method #2 Quick Setup on the Web Page
Network Settings
Date & Time Settings
Administrator Settings
Method #3 Quick Setup on the Command Line Interface
Next Step

5: Web and Command Line Interfaces

Web Interface
Logging in
Logging Out
Web Page Help 54
Command Line Interface 54
Logging In 55
Logging Out 55
Command Syntax 55
Command Line Help 56
Tips 56
General CLI Commands 57

6: Basic Parameters 59

Requirements 59
Eth1 and Eth2 Settings 61
Hostname & Name Servers 62
DNS Servers 63
DHCP-Acquired DNS Servers 63
GPRS-Acquired DNS Servers 63
TCP Keepalive Parameters 63
Gateway 63
Fail-Over Settings 64
Fail-Over Cellular Gateway Configuration 65
Advanced Cellular Gateway Configuration 66
Fail-Over Cellular Gateway Firmware 67
Load Cellular Gateway Firmware Options 67
Ethernet Counters 68
Network Commands 68
IP Filter 68
Viewing IP Filters 68
Enabling IP Filters 69
Configuring IP Filters 69
Rule Parameters 70
Updating an IP Filter 72
Deleting an IP Filter 72
Mapping a Ruleset 72
IP Filter Commands 72
Routing 72
Dynamic Routing 73
Static Routing 73
Routing Commands 73
VPN 74
Performance Monitoring 77
Performance Monitoring - Add/Edit Probe 80
Performance Monitoring - Results 82
Performance Monitoring Commands 86
# 7: Services

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Logging and Other Services</td>
<td>87</td>
</tr>
<tr>
<td>SSH/Telnet/Logging</td>
<td>88</td>
</tr>
<tr>
<td>System Logging</td>
<td>88</td>
</tr>
<tr>
<td>Audit Log</td>
<td>89</td>
</tr>
<tr>
<td>SMTP</td>
<td>89</td>
</tr>
<tr>
<td>SSH</td>
<td>89</td>
</tr>
<tr>
<td>Telnet</td>
<td>90</td>
</tr>
<tr>
<td>Web SSH/Web Telnet Settings</td>
<td>90</td>
</tr>
<tr>
<td>Phone Home</td>
<td>90</td>
</tr>
<tr>
<td>SNMP</td>
<td>91</td>
</tr>
<tr>
<td>Communities</td>
<td>92</td>
</tr>
<tr>
<td>Version 3</td>
<td>93</td>
</tr>
<tr>
<td>V3 Read-Only User</td>
<td>93</td>
</tr>
<tr>
<td>V3 Read-Write User</td>
<td>93</td>
</tr>
<tr>
<td>SNMP, SSH, Telnet, and Logging Commands</td>
<td>93</td>
</tr>
<tr>
<td>NFS and SMB/CIFS</td>
<td>94</td>
</tr>
<tr>
<td>SMB/CIFS Share</td>
<td>95</td>
</tr>
<tr>
<td>NFS and SMB/CIFS Commands</td>
<td>95</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>95</td>
</tr>
<tr>
<td>Troubleshooting Browser Issues</td>
<td>99</td>
</tr>
<tr>
<td>Web SSH/Telnet Copy and Paste</td>
<td>101</td>
</tr>
<tr>
<td>Secure Lantronix Network Commands</td>
<td>101</td>
</tr>
<tr>
<td>Date and Time</td>
<td>102</td>
</tr>
<tr>
<td>Date and Time Commands</td>
<td>103</td>
</tr>
<tr>
<td>Web Server</td>
<td>103</td>
</tr>
<tr>
<td>Administrative Commands</td>
<td>105</td>
</tr>
<tr>
<td>Services - Web Sessions</td>
<td>105</td>
</tr>
<tr>
<td>Services - SSL Certificate</td>
<td>106</td>
</tr>
<tr>
<td>SSL Certificate Commands</td>
<td>108</td>
</tr>
<tr>
<td>ConsoleFlow</td>
<td>109</td>
</tr>
<tr>
<td>ConsoleFlow Commands</td>
<td>113</td>
</tr>
</tbody>
</table>

# 8: Device Ports

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Methods</td>
<td>114</td>
</tr>
<tr>
<td>Permissions</td>
<td>114</td>
</tr>
<tr>
<td>Device Status</td>
<td>115</td>
</tr>
<tr>
<td>Global Port Settings</td>
<td>115</td>
</tr>
<tr>
<td>Telnet/SSH/TCP in Port Numbers</td>
<td>116</td>
</tr>
<tr>
<td>Global Commands</td>
<td>117</td>
</tr>
<tr>
<td>Device Ports - Settings</td>
<td>117</td>
</tr>
<tr>
<td>Device Port Settings</td>
<td>119</td>
</tr>
</tbody>
</table>
# 12: Maintenance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware &amp; Configurations</td>
<td>237</td>
</tr>
<tr>
<td>Factory Reset with External Storage Device</td>
<td>237</td>
</tr>
<tr>
<td>Internal Temperature</td>
<td>239</td>
</tr>
<tr>
<td>Site Information</td>
<td>239</td>
</tr>
<tr>
<td>SLB Firmware</td>
<td>239</td>
</tr>
<tr>
<td>Boot Banks</td>
<td>240</td>
</tr>
<tr>
<td>Load Firmware Via Options</td>
<td>240</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>240</td>
</tr>
<tr>
<td>Zero Touch Provisioning Configuration Restore</td>
<td>241</td>
</tr>
<tr>
<td>Administrative Commands</td>
<td>242</td>
</tr>
<tr>
<td>System Logs</td>
<td>243</td>
</tr>
<tr>
<td>System Log Commands</td>
<td>244</td>
</tr>
<tr>
<td>Audit Log</td>
<td>245</td>
</tr>
<tr>
<td>Email Log</td>
<td>246</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>247</td>
</tr>
<tr>
<td>Diagnostic Commands</td>
<td>248</td>
</tr>
</tbody>
</table>
Status/Reports .........................................................................................................................249
View Report ............................................................................................................................250
Status Commands ....................................................................................................................251
Emailing Logs and Reports .......................................................................................................251
Events ......................................................................................................................................252
Events Commands ....................................................................................................................254
LCD/Keypad ..............................................................................................................................254
LCD/Keypad Commands ............................................................................................................256
Banners ....................................................................................................................................256
Banner Commands ....................................................................................................................257
System Info ...............................................................................................................................257

13: Application Examples ........................................................................................................259
Telnet/SSH to a Remote Device ...............................................................................................259
Dial-in (Text Mode) to a Remote Device ..................................................................................261
Local Serial Connection to Network Device via Telnet .............................................................262

14: Command Reference ..........................................................................................................264
Introduction to Commands .........................................................................................................264
Command Syntax .......................................................................................................................264
Command Line Help ...................................................................................................................265
Tips ..........................................................................................................................................265
Access List Commands ..............................................................................................................266
Administrative Commands .........................................................................................................267
Audit Log Commands .................................................................................................................278
Authentication Commands ..........................................................................................................278
Kerberos Commands ..................................................................................................................279
LDAP Commands ....................................................................................................................279
Local Users Commands .............................................................................................................280
NIS Commands ........................................................................................................................281
RADIUS Commands ................................................................................................................285
TACACS+ Commands ...............................................................................................................287
User Permissions Commands .....................................................................................................289
CLI Commands ..........................................................................................................................292
Connection Commands .............................................................................................................294
ConsoleFlow Commands ..........................................................................................................298
Console Port Commands ..........................................................................................................300
Custom User Menu Commands ...............................................................................................301
Date and Time Commands ........................................................................................................303
Device Commands .......................................................................................................................304
Device Port Commands .............................................................................................................305
Diagnostic Commands ..............................................................................................................309
End Device Commands ............................................................................................................311
List of Figures

Figure 2-1 Branch to Enterprise Integration Concept ..............................................................21
Figure 2-3 100-120 VAC SLB Unit ........................................................................................23
Figure 2-4 200-240 VAC SLB Unit ........................................................................................24
Figure 2-5 Example Deployment .........................................................................................26
Figure 2-6 Device Port Connections ....................................................................................28
Figure 2-7 Console Port Connection ....................................................................................28
Figure 2-8 Network Connection ............................................................................................28
Figure 2-9 USB Interface ........................................................................................................28
Figure 2-10 Modem Interface ...............................................................................................29
Figure 3-5 Inlet Pin Assignment ............................................................................................33
Figure 3-6 CAT 5 Cable Connection ....................................................................................35
Figure 3-7 AC Power Input .....................................................................................................37
Figure 3-8 100-120 VAC SLB - Branch Office Manager Power Outlets .........................37
Figure 3-9 200-240 VAC SLB - Branch Office Manager Power Outlets .........................38
Figure 3-10 100-120 VAC SLB Installation Diagram ............................................................38
Figure 3-11 200-240 VAC SLB Installation Diagram ............................................................39
Figure 4-2 Front Panel LCD Display and Five Button Keypads (Enter, Up, Down, Left, Right) 41
Figure 4-6 Quick Setup ........................................................................................................47
Figure 4-7 Beginning of Quick Setup Script .........................................................................49
Figure 4-8 Completed Quick Setup .......................................................................................50
Figure 5-1 Web Page Layout .................................................................................................52
Figure 6-1 Network > Network Settings (1 of 2) ..................................................................60
Figure 6-2 Network > Network Settings (2 of 2) ..................................................................61
Figure 6-3 Network > IP Filter ..............................................................................................69
Figure 6-4 Network > IP Filter Ruleset (Adding/Editing Rulesets) .........................................70
Figure 6-5 Network > Routing ..............................................................................................73
Figure 6-6 Network > VPN ....................................................................................................74
Figure 6-7 Network > Perf Monitoring ..................................................................................78
Figure 6-8 Performance Monitoring - Add/Edit Probe ............................................................80
Figure 6-10 Performance Monitoring - Operations .................................................................85
Figure 7-1 Services > SSH/Telnet/Logging ..........................................................................88
Figure 7-2 Services > SNMP .................................................................................................91
Figure 7-3 Services > NFS/CIFS ..........................................................................................94
Figure 7-4 Services > Secure Lantronix Network .................................................................96
Figure 7-5 IP Address Login Page .......................................................................................97
Figure 7-6 SSH or Telnet CLI Session ................................................................................97
Figure 11-3 User Authentication > Local/Remote User > Settings __________________________202
Figure 11-4 User Authentication > NIS ______________________________________________206
Figure 11-5 User Authentication > LDAP _____________________________________________209
Figure 11-6 User Authentication > RADIUS ___________________________________________213
Figure 11-7 User Authentication > Kerberos __________________________________________218
Figure 11-8 User Authentication > TACACS+ __________________________________________222
Figure 11-9 User Authentication > Group _____________________________________________226
Figure 11-10 User Authentication > SSH Keys _________________________________________229
Figure 11-11 Current Host Keys ____________________________________________________232
Figure 11-12 User Authentication > Custom Menus ____________________________________234
Figure 12-1 Maintenance > Firmware & Configurations _________________________________238
Figure 12-2 Manage Configuration Files _____________________________________________242
Figure 12-3 Maintenance > System Logs _____________________________________________243
Figure 12-4 System Logs __________________________________________________________244
Figure 12-5 Maintenance > Audit Log _______________________________________________245
Figure 12-6 Maintenance > Email Log _______________________________________________246
Figure 12-7 Maintenance > Diagnostics _____________________________________________247
Figure 12-8 Diagnostics Report ____________________________________________________248
Figure 12-9 Maintenance > Status/Reports __________________________________________249
Figure 12-10 Generated Status/Reports ____________________________________________250
Figure 12-11 Emailed Log or Report _______________________________________________252
Figure 12-12 Maintenance > Events _______________________________________________253
Figure 12-13 Maintenance > LCD/Keypad ___________________________________________255
Figure 12-14 Maintenance > Banners ______________________________________________256
Figure 12-15 System Info _________________________________________________________258
Figure 13-1 SLB - Branch Office Manager Configuration _______________________________259
Figure 13-2 Remote User Connected to a SUN Server via the SLB _________________________259
Figure 13-3 Dial-in (Text Mode) to a Remote Device _________________________________261
Figure 13-4 Local Serial Connection to Network Device via Telnet ______________________262
Figure C-1 RJ45 Receptacle to DB25M DCE Adapter for the SLB (PN 200.2066A) __________354
Figure C-2 RJ45 Receptacle to DB25F DCE Adapter for the SLB (PN 200.2067A) __________355
Figure C-3 RJ45 Receptacle to DB9M DCE Adapter for the SLB (PN 200.2069A) __________355
Figure C-4 RJ45 Receptacle to DB9F DCE Adapter for the SLB (PN 200.2070A) __________356
Figure C-5 RJ45 to RJ45 Adapter for Netra/Sun/Cisco and SLP (PNs 200.2225 and ADP010104-01)
List of Tables

Table 2-2 SLB Models .................................................................23
Table 3-1 Part Numbers and Descriptions for Adapters and Cables ..................30
Table 3-2 Part Numbers and Descriptions for Power Cords ................................30
Table 3-3 SLB Technical Specifications .............................................31
Table 3-4 Max Current per Power Cord Used .....................................32
Table 4-1 Methods of Assigning an IP Address .....................................40
Table 4-3 LCD Arrow Keypad Actions ...............................................42
Table 4-4 Front Panel Setup Options with Associated Parameters ................43
Table 4-5 Front Panel Options, continued .........................................43
Table 5-2 Actions and Category Options ...........................................56
Table 6-9 Error Conditions ............................................................84
Table 8-5 Port Status and Counters ..................................................124
Table 8-17 Definitions ................................................................147
Table 8-18 Primary Commands .........................................................148
Table 8-19 Secondary Commands ....................................................149
Table 8-20 Control Flow Commands ................................................150
Table 14-1 Actions and Category Options .........................................264
Table A-1 User Commands ............................................................351
Table A-2 Administrator Commands ................................................352
1: About this Guide

Purpose and Audience

This guide provides the information needed to install, configure, and use the Lantronix® SLB™ branch office manager. The SLB unit is for IT professionals who must remotely and securely configure and administer servers, routers, switches, telephone equipment, or other devices equipped with a serial port for facilities that are typically remote branch offices or “distributed” IT locations.

Summary of Chapters

The remaining chapters in this guide include:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 2: Introduction</strong></td>
<td>Describes the SLB models, their main features, and the protocols they support.</td>
</tr>
<tr>
<td><strong>Chapter 3: Installation</strong></td>
<td>Provides technical specifications; describes connection formats and power supplies; provides instructions for installing the SLB unit in a rack.</td>
</tr>
<tr>
<td><strong>Chapter 4: Quick Setup</strong></td>
<td>Provides instructions for getting your SLB unit up and running and for configuring required settings.</td>
</tr>
<tr>
<td><strong>Chapter 5: Web and Command Line Interfaces</strong></td>
<td>Describes the web and command line interfaces available for configuring the SLB branch office manager. The configuration chapters (6-12) provide detailed instructions for using the web interface and include equivalent command line interface commands.</td>
</tr>
<tr>
<td><strong>Chapter 6: Basic Parameters</strong></td>
<td>Provides instructions for configuring network ports, firewall and routing settings, and the date and time.</td>
</tr>
<tr>
<td><strong>Chapter 7: Services</strong></td>
<td>Provides instructions for enabling and disabling system logging, SSH and Telnet logins, SNMP, SMTP, and the date and time.</td>
</tr>
<tr>
<td><strong>Chapter 8: Device Ports</strong></td>
<td>Provides instructions for configuring global device port settings, individual device port settings, and console port settings.</td>
</tr>
<tr>
<td><strong>Chapter 9: USB Port</strong></td>
<td>Provides instructions for using the USB port.</td>
</tr>
<tr>
<td><strong>Chapter 10: Connections</strong></td>
<td>Provides instructions for configuring connections and viewing, updating, or disconnecting a connection.</td>
</tr>
<tr>
<td><strong>Chapter 11: User Authentication</strong></td>
<td>Provides instructions for enabling or disabling methods that authenticate users who attempt to log in via SSH, Telnet, or the console port. Provides instructions for creating custom menus.</td>
</tr>
<tr>
<td><strong>Chapter 12: Maintenance</strong></td>
<td>Provides instructions for upgrading firmware, viewing system logs and diagnostics, generating reports, and defining events. Includes information about web pages and commands used to shut down and reboot the SLB unit.</td>
</tr>
<tr>
<td><strong>Chapter 13: Application Examples</strong></td>
<td>Shows how to set up and use the SLB branch office manager in three different configurations.</td>
</tr>
<tr>
<td><strong>Chapter 14: Command Reference</strong></td>
<td>Lists and describes all of the commands available on the SLB command line interface</td>
</tr>
</tbody>
</table>
Additional Documentation

Visit the Lantronix Web site at www.lantronix.com/support/documentation for the latest documentation and the following additional documentation.

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLB Branch Office Manager Quick Start</td>
<td>Describes the steps for getting the SLB unit up and running.</td>
</tr>
<tr>
<td>SLB Branch Office Manager Online Help for the Command Line Reference</td>
<td>Provides online help for configuring the SLB unit using commands.</td>
</tr>
<tr>
<td>SLB Branch Office Manager Online Help for the Web Interface</td>
<td>Provides online help for configuring the SLB unit using the web page.</td>
</tr>
</tbody>
</table>
2: **Introduction**

The SLB branch office manager enables IT system administrators to manage remote servers and IT infrastructure equipment securely over the Internet. This innovative hybrid device combines the capabilities of the award-winning secure console manager with an 8-port remote power management solution into a compact, 1U rack-mountable appliance.

**Features**

**Console Management**
- 8 serial ports for console connectivity
- Enables system administrators to remotely manage devices with serial console ports, e.g., Linux, Unix, and recent versions of Windows servers, routers, switches, telecom, and building access equipment.
- Provides data logging, monitoring, and secure access control via the Internet

**Power Management Outlets for Power Connectivity**
- 8 outlets for power connectivity
- Provides ability to control power individually to all attached equipment
- Provides on/off/reboot control
- Per port power consumption monitoring
- SLB882KIT-15P and SLB882KIT-20P outlets support NEMA 5-15P & 5-20P plugs
- SLB8824KIT-AP and SLB8824KIT-EU outlets support C14 plugs
- Ensures safe power distribution and reduces in-rush current overload

**Power Inlets**
- SLB882KIT-xx Dual 100-120 VAC power inlets
- SLB8824KIT-xx Dual 200-240 VAC power inlets
- Provides automatic power switch-over when both primary and secondary power inlet sources are used

**Integration with Other Secure Lantronix Products**
- Can integrate seamlessly with the ConsoleFlow™ software for a complete end-to-end Out-of-Band (OOB) management solution.
Internal Temperature Sensor

- System administrators can be alerted if temperature goes out of range.

**Figure 2-1 Branch to Enterprise Integration Concept**

**Designed for Branch Offices and Similar Environments**

Designed to meet the specific needs of the remote branch offices and environments alike, the SLB branch office manager conserves rack space and reduces costs by enabling system administrators at a main corporate facility to manage the IT equipment distributed among branch offices simply and cost-effectively.

Branch offices are facilities that are typically remote or "distributed IT" locations, likely located off-site of corporate headquarters or large-scale enterprise facilities. These distributed facilities typically do not have an on-site maintenance staff or IT System Administrator.

Typically, the branch office environment has some of the following characteristics:

- Space is limited to 1U rack space or shelf mounted desktop unit
- Closet-mounted or wall-attached rack
- Limited air and power conditioning
- Limited number of network devices and servers
- No on-site maintenance staff
- Ethernet or dial-up modem access is required
**Typical Equipment**
You can configure, administer, and manage IT equipment in a variety of ways, but most devices have one method in common: an RS-232 serial port, sometimes called a console, auxiliary, or management port. These ports are often accessed directly by connecting a terminal or laptop to them, meaning that the user typically must be in the same physical location as the equipment. Eliminating the need for a physical presence, the Lantronix SLB unit provides remote access to the equipment from anywhere there is a network or modem connection.

The SLB branch office manager can access and administer many types of equipment, such as:

- Servers: Unix, Linux, Windows Server 2003 or higher, and others
- Networking equipment: Routers, switches, storage networking
- Telecom: PBX, voice switches
- Other systems with serial interfaces: Heating/cooling systems, security/building access systems, UPS, medical device.

**Types of Business**
The SLB unit is used in many types of environments, for example:

- Banking and finance
- Insurance companies
- Healthcare
- Retail Sales
- Information Technology
- Education and campus style facilities
- Hospitality
- Manufacturing Facilities
- Base Station Control and Management

**Benefits**
The key benefits of using the SLB branch office manager:

- Saves space: Compact design merges the functionality of two solutions into a 1U rack solution, reducing required rack space and total cost of ownership.
- Saves money: Enables remote management and troubleshooting without sending a technician onsite, resulting in reduced travel costs and increased network uptime.
- Saves time: Provides instant access and reduces response time, improving efficiency.
- Simplifies access: Enables 24/7 access to your equipment securely and remotely after hours and on weekends and holidays-without having to schedule visits or arrange for off-hour access.
- Protects assets: Provides the highest levels of encryption and security features (authentication, authorization, and IP filters) to ensure that your IT infrastructure and data assets are protected.

The SLB unit also provides features such as convenient text menu systems, break-safe operation, port buffering (logging), remote authentication, and Secure Shell (SSH) access. Dial-up modem support ensures access when the network is not available.
Models

The SLB branch office manager has the following hardware components:

- The 100-120 VAC SLB model is available in 100-120 VAC (50-60 Hz) NEMA 5-20R type outlets. This model also includes a USB port.
- The 200-240 VAC SLB model is available in 200-240 VAC (50-60 Hz) IEC C13 type outlets. This model also includes a USB port.
  
  **Note:** This model is EU style with one switched hot line, not a US style with two hot lines. It is intended for use on power systems where the 200-240VAC is provided on a single hot line.

- **Chassis:** The SLB unit has a 1U tall, self-contained rack-mountable chassis.
- **Power Outlets:** Eight outlets allow power management and control (on/off/reboot) of the attached equipment using a simple web or command line interface.
- **Serial Device Ports:** Eight serial RS-232C (EIA-232) device ports are for remote console management of the attached equipment. These match the RJ45 pin-outs of the console ports of many popular devices found in a network environment, and where different can be converted using Lantronix adapters. See the appendix, Appendix C: Adapters and Pinouts for more information on serial adapters and pin-outs.
- **Ports and Modem:** The SLB branch office manager has two 10/100 Ethernet ports (referred to in this user guide as Eth1 and Eth2) in the back and a front panel serial console port (RJ45). The SLB unit also includes a USB type A port in the front panel and an internal v.92 modem.

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100-120 VAC SLB</td>
<td>Branch Office Manager, 8 device ports, 8 power outlets (100-120 VAC, NEMA 5-20R type), 2 AC power inlets</td>
</tr>
<tr>
<td>200-240 VAC SLB</td>
<td>Branch Office Manager, 8 device ports, 8 power outlets (200-240 VAC, IEC C13 type), 2 AC power inlets</td>
</tr>
</tbody>
</table>

Figure 2-3 100-120 VAC SLB Unit
System Features

The SLB firmware has the following basic capabilities:

- Connects up to eight RS-232 serial consoles
- Controls power (on/off/reboot) of up to eight attached devices
- Per port current consumption monitoring
- Dual power inlets for failover. Both power inlets must be on the same phase.
- Dual 10Base-T/100Base-TX Ethernet network compatibility
- Buffer logging to file
- Email and SNMP notification
- ID/Password security, configurable access rights
- Secure shell (SSH) security; supports numerous other security protocols
- Network File System (NFS) and Common Internet File System (CIFS) support for configuration files
- TCP, Telnet or SSH to a serial port by IP address per port or by IP address and TCP port number
- Configurable user rights for local and remotely authenticated users
- Built-in internal modem
- External USB modem and Flash Storage supported
- Sun break-safe (no unintentional break ever sent to attached servers)
- Simultaneous access on the same port-- "listen" and "direct" connect mode
- Local access through a console port
- Web administration (using most browsers)

Protocols Supported

The SLB branch office manager supports the TCP/IP network protocol as well as:

- TCP, SSH, Telnet, PPP and NFS for connections in and out of, and CIFS for incoming connections to the `\\<hostname>\public\config` directory of the SLB unit
- SMTP for mail transfer
- DNS for text-to-IP address name resolution
SNMP with custom traps for remote monitoring and management
FTP and SFTP for file transfers and firmware upgrades
TFTP and HTTPS for firmware upgrades
DHCP and BOOTP for IP address assignment
HTTPS (SSL) for secure browser-based configuration
NTP for time synchronization
LDAP, NIS, RADIUS, CHAP, PAP, Kerberos, and TACACS+ for user authentication
IPsec for VPN access

For brief descriptions of these protocols, see Appendix D: Protocol Glossary.

Access Control
The system administrator controls access to attached servers or devices by assigning access rights to up to 128 user profiles. Each user has an assigned ID, password, and access rights. Other user profile access options may include externally configured authentication methods such as RADIUS, TACACS+, NIS, and LDAP. Groups are supported in LDAP, RADIUS (via VSA), and TACACS+ (using priv_lvl).

Power Outlet Control
With the SLB unit's built-in power management capability, system administrators can remotely control the power (on/off/reboot) individually to all IT equipment in the branch office, ensure safe power distribution, and reduce "in-rush" current overload. If SNMP traps are enabled, a trap (alarm) is sent if the total current for all outlets exceeds a threshold.

Device Port Buffer
The SLB branch office manager supports real-time data logging for each device port. The port can save the data log to a file, send an email notification of an issue, or take no action.

You can define the path for logged data on a port-by-port basis, configure file size and number of files per port for each logging event, and configure the device log to send an email alert message automatically to the appropriate parties indicating a particular error.

Configuration Options
You may use the backlit front-panel LCD display for initial setup and configuration and to view current network, console, and date/time settings, and get power outlet status.

Both a web interface viewed through a standard browser and a command line interface (CLI) are available for configuring the SLB settings and monitoring performance.
Application Example

The figure below is an example deployment. An SLB unit is deployed in each branch office and an (optional) vSLM management appliance at the main office. The branch offices are interconnected (always on) by VPN routers overlaid on the Internet, and also interconnected (on demand) through the analog phone system.

The SLB unit provides remotely controlled and monitored AC power (orange), console management (green), and traditional, wired telephone network (PSTN) access (yellow).

A system administrator, upon losing IP connectivity to a server, takes the following steps:

1. Views the server's Ethernet interface state information provided by the SLB branch office manager.
2. If the Ethernet interface is faulty, connects to the server's console port by means of the SLB web page or CLI (optionally via the vSLM management appliance) and checks the server's system parameters.
3. If the server is not responsive on the console port, commands the SLB to reboot the server's power.
4. If the entire branch office loses IP connectivity, dial in to the SLB to perform the diagnostic functions.
Hardware Features

**Caution:** *To avoid physical and electrical hazards, please read Safety Precautions before installing the SLB unit.*

The SLB hardware includes the following:
- 1U-tall (1.75 inch) rack-mountable appliance
- Two 10Base-T/100Base-TX network ports
- One front panel serial console port for VT100 terminal or PC with emulation
- One USB Port
- Front panel LCD display and keypad
- One RJ-11 Internal Modem Port
- 256 KB-per-port buffer memory for serial device ports
- Eight RS-232 serial device ports connected via Category 5 (RJ45) wiring

**Note:** Max input/output is rated at 80% of the circuit max, per typical electrical codes.

- Dual AC Power Input

| 100-120 VAC SLB Model | Dual IEC-60320/C20 inlets, 100-120 VAC, 50/60Hz  
(20A Branch Circuit) 16A max input current |
|-----------------------|--------------------------------------------------------------------------------------------------|
| 200-240 VAC SLB Model | Dual IEC-60320/C20 inlets, 200-240 VAC, 50/60Hz  
(20A Branch Circuit) 16A max input current |

- Power Outlets (Total Switched Power)

| 100-120 VAC SLB Model | (8) NEMA 5-20R outlets, 100-120 VAC, 50/60Hz  
16A max per outlet, 16A total for SLB |
|-----------------------|--------------------------------------------------------------------------------------------------|
| 200-240 VAC SLB Model | (8) IEC C13 outlets, 200-240 VAC, 50/60Hz  
10A max per outlet, 16A total for SLB  
(15.9A max total for China CCC) |

**Note:** The outlet voltage equals the input voltage.

- Convection cooled, silent operation, low power consumption

**Note:** For more detailed information, see Technical Specifications (on page 31).

Serial Connections

All devices attached to the device ports and the console port must support the RS-232C (EIA-232) standard. Category 5 cabling with RJ45 connections is used for the device port connections and for the console port. (For pinout information, see Adapters and Pinouts on page 354.)

**Note:** RJ45 to DB9/DB25 adapters are available from Lantronix.

Device ports and the console port support the following baud-rate options: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, and 230400 baud.
Network Connections

The SLB network interfaces are 10Base-T/100Base-TX connectors for use with a conventional Ethernet network. Use standard RJ45-terminated Category 5 cables. Network parameters must be configured before the SLB branch office manager can be accessed over the network.

**Note:** One possible use for the two Ethernet ports is to have one port on a private, secure network and the other on a public, unsecured network.

USB Interface

The SLB unit has a USB port. Lantronix qualifies USB devices continuously.
Modem Interface

The SLB branch office manager has one v92 modem RJ11 interface to allow configuration and control of the unit via dialing into the unit.

**Caution:** *To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.*

**Attention:** *Pour réduire les risques d’incendie, utiliser uniquement des conducteurs de télécommunications 26 AWG au de section supérieure.*

Figure 2-10 Modem Interface
3: **Installation**

This chapter provides a high-level procedure for installing the SLB branch office manager followed by more detailed information about the SLB connections and power supplies.

**What's in the Box**

In addition to the SLB branch office manager, the following table lists components in the box and their corresponding part numbers.

<table>
<thead>
<tr>
<th>Table 3-1 Part Numbers and Descriptions for Adapters and Cables</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Part #</strong></td>
</tr>
<tr>
<td><strong>Adapters:</strong></td>
</tr>
<tr>
<td>200.2066A</td>
</tr>
<tr>
<td>200.2067A</td>
</tr>
<tr>
<td>200.2069A</td>
</tr>
<tr>
<td>200.2070A</td>
</tr>
<tr>
<td>ADP010104-01</td>
</tr>
</tbody>
</table>

*Note: The following optional adapters are available from Lantronix:
200.2073 Adapter: DB25M (DTE) to RJ45, external modems.
200.2071 Adapter: DB9M (DTE) to convert the RJ45 serial connector to a PC style D-sub serial port*

| **Cables:** | |
| 200.0063 | Cable: RJ45 to RJ45, Cat-5, 6.6 ft (2 m) |
| 500-153 | Cable: RJ45 Loopback |

<table>
<thead>
<tr>
<th>Table 3-2 Part Numbers and Descriptions for Power Cords</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model</strong></td>
</tr>
<tr>
<td>100-120 VAC SLB*</td>
</tr>
<tr>
<td>200-240 VAC SLB*</td>
</tr>
<tr>
<td>200-240 VAC SLB*</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>200-240 VAC SLB*</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

* Included power cords vary for kit purchased. Please see [www.lantronix.com](http://www.lantronix.com) for additional inlet power cords available.

Verify and inspect the contents of the SLB package using the enclosed packing slip or the table above. If any item is missing or damaged, contact your place of purchase immediately.
Product Information Label

The product information label on the underside of the SLB branch office manager contains the following information about each SLB unit:

- Part Number
- Serial Number Bar Code
- Serial Number and Date Code
- Regulatory Certifications and Statements

Technical Specifications

Note: The SLB branch office manager is intended for use in Single Phase systems.

Table 3-3  SLB Technical Specifications

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Interface (Device)</td>
<td>(8) RJ45-type 8-conductor connector (DTE)</td>
</tr>
<tr>
<td></td>
<td>Speed software selectable (300 to 230,400 baud)</td>
</tr>
<tr>
<td>Serial Interface (Console)</td>
<td>(1) RJ45-type 8-pin connector (DTE)</td>
</tr>
<tr>
<td></td>
<td>Speed software selectable (300 to 230,400 baud)</td>
</tr>
<tr>
<td>Power Input</td>
<td>100-120 VAC SLB Model</td>
</tr>
<tr>
<td></td>
<td>◆ (2) IEC-60320/C20 inlet, 100-120 VAC, 50/60Hz</td>
</tr>
<tr>
<td></td>
<td>◆ (20A Branch Circuit) 16A max input current</td>
</tr>
<tr>
<td></td>
<td>200-240 VAC SLB Model</td>
</tr>
<tr>
<td></td>
<td>◆ (2) IEC-60320/C20 inlet, 200-240 VAC, 50/60Hz</td>
</tr>
<tr>
<td></td>
<td>◆ (20A Branch Circuit) 16A max input current</td>
</tr>
</tbody>
</table>

Note: The max input current is de-rated to figures listed in Table 3-4 when using specified power cords.

| Power Outlets               | 100-120 VAC SLB Model                                                       |
|                            | ◆ (8) NEMA5-20R outlets, 100-120 VAC, 50/60Hz                               |
|                            | ◆ (20A Branch Circuit) 16A max per outlet, 16A total                         |
|                            | Individual current sensor for monitoring power draw on each outlet           |
|                            | Output power switchable via independent relay for each outlet               |
|                            | 200-240 VAC SLB Model                                                       |
|                            | ◆ (8) IEC C13 outlets, 200-240 VAC, 50/60Hz                                 |
|                            | ◆ (20A Branch Circuit) 10A max per outlet, 16A total                         |
|                            | (15.9A max total for China CCC)                                             |
|                            | Individual current sensor for monitoring power draw on each outlet           |
|                            | Output power switchable via independent relay for each outlet               |
|                            | Single pole only. Not suitable for two hot line power systems.              |
| Modem Interface            | RJ11 Jack for connection to internal v92 dial up modem.                    |
|                            | Note: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord. |
| Network Interface          | Dual 10Base-T/100Base-TX RJ45 Ethernet                                      |
| Power Consumption          | Less than 30 watts. Applies only to the operation of the SLB branch office manager and not to the current it is switching. |
3: Installation

Safety Precautions

Please follow the safety precautions described below when installing and operating the SLB branch office manager.

**Cover**
- Do not remove the cover of the chassis. There are no user-serviceable parts inside. Opening or removing the cover may expose you to dangerous voltage that could cause fire or electric shock.
- Refer all servicing to Lantronix.

**Power Plug**
- When disconnecting the power cable from the socket, pull on the plug, not the cord.
- Always connect the power cord to a properly wired and grounded power source. Do not use adapter plugs or remove the grounding prong from the cord.
- Only use a power cord with a voltage and current rating greater than the voltage and current rating marked on the SLB.
- Install the SLB unit near an AC outlet that is easily accessible.
- Always connect any equipment used with the product to properly wired and grounded power sources.

### Table 3-4 Max Current per Power Cord Used

<table>
<thead>
<tr>
<th>Power Cord Used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLPP12310-01</td>
<td>Inlet cord: IEC60320/C19 to NEMA 5-15P (15A)</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Unit input current is de-rated to 12A maximum when using this cable.</td>
</tr>
<tr>
<td>SLPP12410-01</td>
<td>Inlet cord: IEC60320/C19 to NEMA 5-20P (20A)</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Unit input current is de-rated to 16A maximum when using this cable.</td>
</tr>
<tr>
<td>SLPP12810-01</td>
<td>Inlet cord: IEC60320/C19 to Schuko (EU/16A)</td>
</tr>
<tr>
<td>SLPP12910-01</td>
<td>Inlet cord: IEC60320/C19 to BS1363 (UK/13A)</td>
</tr>
<tr>
<td>SLPP12A08-01</td>
<td>Inlet cord: IEC60320/C19 to AS/NZS 3112 (AU/NZ/15A)</td>
</tr>
<tr>
<td>SLPP12C08-01</td>
<td>Inlet cord: IEC60320/C19 to CHINA/GB (CN/16A)</td>
</tr>
</tbody>
</table>

Component (continued)

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>1U, 1.7 in x 18.9 in x 12.4 in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>10 lb.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Operating: 0 to 50 °C (32 to 122 °F)</td>
</tr>
<tr>
<td></td>
<td>Storage: -20 to 70 °C (-4 to 158 °F)</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>Operating: 10% to 90% non-condensing</td>
</tr>
<tr>
<td></td>
<td>Storage: 10% to 90% non-condensing</td>
</tr>
<tr>
<td>Current measurement accuracy</td>
<td>1A to 16A</td>
</tr>
</tbody>
</table>
Always connect the unit with the proper polarity at the inlet connector. See Figure 3-5. Failure to do so may cause downstream hazards on connected devices.

Figure 3-5 Inlet Pin Assignment

To help protect the product from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).

Do not connect or disconnect this product during an electrical storm.

Input Supply

Caution: This SLB unit may have more than one power supply source. Disconnect all power supply sources before servicing to avoid electric shock. Disconnect downstream device power cables prior to servicing the downstream device.

Note: The SLB branch office manager is intended for use in Single Phase systems.

Check nameplate ratings to assure there is no overloading of supply circuits that could affect over current protection and supply wiring.

Grounding

1. Maintain reliable grounding of this product.
2. Pay particular attention to supply connections when connecting to power strips, rather than directly to the branch circuit.

Fuses

For protection against fire, replace the power-input-module fuse with the same type and rating.

Rack

If rack mounted SLB branch office managers are installed in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. The following items must be considered:
3: Installation

Do not install the SLB unit in a rack in such a way that a hazardous stability condition results because of uneven loading. A drop or fall could cause injury.

The ambient temperature (Tma) inside the rack may be greater than the room ambient temperature. Make sure to install the SLB branch office manager in an environment with an ambient temperature less than the maximum operating temperature of the SLB unit. (See Technical Specifications on page 31.)

Install the equipment in a rack in such a way that the amount of airflow required for safe operation of the equipment is not compromised.

Mount the equipment in the rack so that a hazardous condition is not achieved due to uneven mechanical loading.

Maintain reliable earthing of rack-mounted equipment. Give particular attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Before operating the SLB branch office manager, make sure the SLB unit is secured to the rack.

Port Connections

Only connect the network port to an Ethernet network that supports 10Base-T/100Base-T.

Only connect device ports to equipment with serial ports that support EIA-232 (formerly RS-232C).

Only connect the console port to equipment with serial ports that support EIA-232 (formerly RS-232C).

Physical Installation

To install the SLB branch office manager in a rack:

1. Place the SLB unit in a 19-inch rack.

Warning: Do not block the air vents on the sides of the SLB unit. If you mount the SLB branch office manager in an enclosed rack, we recommended that the rack have a ventilation fan to provide adequate airflow through the SLB unit.

2. Connect the serial device(s) to the SLB device ports. See the section, Connecting to a Device Port (on page 35).

3. Choose one of the following options:
   - To configure the SLB branch office manager using the network, or to monitor serial devices on the network, connect at least one SLB network port to a network. See Connecting to Network Ports (on page 35).
   - To configure the SLB branch office manager using a dumb terminal or a computer with terminal emulation, connect the terminal or PC to the SLB console port. See Connecting Terminals (on page 36).

4. Connect the power cord, and apply power. See Power (on page 36).

5. Wait approximately a minute and a half for the boot process to complete. If a terminal is connected to the front panel serial console port the boot messages will be displayed on the
terminal.

When the boot process ends, the SLB host name and the clock or the power supply status appear on the LCD display. Now you are ready to configure the network settings as described in Chapter 4: Quick Setup on page 40.

Connecting to a Device Port

You can connect almost any device that has a serial console port to a device port on the SLB unit for remote administration. The console port must support the RS-232C interface.

Note: Many servers must either have the serial port enabled as a console or the keyboard and mouse detached. Consult the server hardware and/or software documentation for more information.

To connect to a device port:

1. Connect one end of the Cat 5 cable to a device port on the SLB unit front panel.
2. Connect the other end of the Cat 5 cable to a Lantronix serial console adapter.

Note: To connect a device port to a Lantronix SLP™ power management, use the ADP010104 adapter and a Cat5 patch cable between the adapter and the connected equipment. See the appendix, Adapters and Pinouts on page 354 for more information about Lantronix adapters.

3. Connect the adapter to the serial console port on the serial device.

Connecting to Network Ports

The SLB branch office manager’s network ports, 10Base-T/100Base-TX, allow remote access to the attached devices and the system administrative functions. Use a standard RJ45-terminated Category 5 cable to connect to the network port.
Note: One possible use for the two Ethernet ports is to have one port on a private, secure network, and the other on an unsecured network. Ethernet bonding is also supported.

Connecting Terminals
The console port is for local access to the SLB unit and the attached devices. You may attach a dumb terminal or a computer with terminal emulation to the console port. The SLB console port uses RS-232C protocol and supports VT100 emulation. The default baud rate is 9600.

To connect the console port to a terminal or computer with terminal emulation, Lantronix offers optional adapters that provide a connection between an RJ45 jack and a DB9 or DB25 connector. The console port is configured as DTE. For more information, see the appendix, Adapters and Pinouts on page 354 and our Web site at www.lantronix.com/support and click Cable/Adapter Lookup on the Support menu.

To connect a terminal:

1. Attach the Lantronix adapter to your terminal (use PN 200.2066A adapter) or your PC’s serial port (use PN 200.2070A adapter).
2. Connect the Cat 5 cable to the adapter, and connect the other end to the SLB console port.
3. Turn on the terminal or start your computer’s communication program (e.g., HyperTerminal for Windows XP or lower. For recent versions of Windows use a free terminal emulator such as PuTTY or TeraTerm Pro).
4. Once the SLB branch office manager is running, press Enter to establish connection. You should see the model name and a login prompt on your terminal. You are connected.
5. On a factory default SLB you may log in using sysadmin as the user name and the last 8 characters of the Device ID (for newly manufactured devices that come installed with SLB firmware 7.0.0.0 or later) or PASS (for older devices) as the password.

Connecting to the Internal Modem
1. Connect an RJ11 telecommunication cable to the modem port on the front of the unit.
2. Connect the other end of the cable to an analog phone connector on your telephone network.

Caution: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.

Power
The SLB unit consumes less than 30W of electrical power.

Note: Switched currents may be 30W or greater.

AC Input
The SLB branch office manager has a universal auto-switching dual AC inlet power supply. The power supply for the 100-120 VAC SLB controller accepts AC input voltage between 100 and 120 VAC with a frequency of 50 or 60 Hz. The power supply for the 200-240 VAC SLB controller accepts AC input voltage between 200 and 240 VAC with a frequency of 50 or 60 Hz. Rear-mounted IEC-type AC power connectors are provided for universal AC power input on a single hot line. US style two hot line 200-240VAC power is not supported. (See What’s in the Box on page 30.)
Caution: This unit may have more than one power supply source. Disconnect all power supply sources before servicing to avoid electric shock.

Figure 3-7 AC Power Input

One of the SLB dual AC power inputs is the designated primary power source and the other is designated as the secondary source. If both are used, the power will be drawn by the primary power source. If the primary power source should fail, power will be drawn through the secondary power source. Once power is restored to the primary power source, the power will be switched back from the secondary power source to the primary power source. Both power sources must be on the same phase. Using power from different phases will cause the relay to malfunction and possibly cause damage to the SLB.

Connecting Devices to Power Outlets

To avoid the possibility of noise due to arcing:

1. Keep the device's on/off switch in the off position until after it is plugged into the outlet, or log in to the SLB branch office manager and turn the outlets off before connecting the devices.
2. Connect devices to the outlets.
The default screen under **Maintenance->LCD/Keypad** can be modified, but by default, the status of the power outlets displays on the front panel LCD.

**Typical Installations**

Following are illustrations showing some typical ways to install the SLB branch office manager. In **Figure 3-10**, three serial devices (a server, a Cisco switch, and a firewall) connect to the SLB unit’s serial ports and power outlets. This setup enables the SLB branch office manager to manage the devices and provide power to the devices. In addition, the SLB unit includes a built-in modem for out-of-band dial-up access.
The SLB unit controls up to eight serial devices and provides power to them. The devices use a separate user supplied Ethernet switch to connect to the network.
4: Quick Setup

This chapter helps get the IP network port up and running quickly, so you can administer the SLB branch office manager using your network. The setup procedures assume you are starting with a factory default SLB unit.

Recommendations

To set up the network connections quickly, we suggest you do one of the following:

- Use the front panel LCD display and keypads.
- Complete the Quick Setup on the web interface.
- SSH to the command line interface and follow the Quick Setup script on the command line interface.
- Connect to the console port and follow the Quick Setup script on the command line interface.

Note: The first time you power up the SLB unit, Eth1 tries to obtain its IP address via DHCP. If you have connected Eth1 to the network, and Eth1 is able to acquire an IP address, you can view this IP address on the LCD or by running the Lantronix® Provisioning Manager application. If Eth1 cannot acquire an IP address, you cannot use Telnet, SSH, or the web interface to run Quick Setup.

IP Address

Your SLB unit must have a unique IP address on your network. The system administrator generally provides the IP address and corresponding subnet mask and gateway. The IP address must be within a valid range, unique to your network. If a valid gateway address has not been assigned, the IP address must be on the same subnet as workstations connecting to the SLB over the network.

The following table lists the options for assigning an IP address to your SLB branch office manager.

Table 4-1 Methods of Assigning an IP Address

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>A DHCP server automatically assigns the IP address and network settings.</td>
</tr>
<tr>
<td></td>
<td>The SLB unit is DHCP-enabled by default.</td>
</tr>
<tr>
<td></td>
<td>With the Eth1 network port connected to the network, and the SLB unit</td>
</tr>
<tr>
<td></td>
<td>powered up, Eth1 acquires an IP address, viewable on the LCD.</td>
</tr>
<tr>
<td></td>
<td>At this point, you can use SSH or Telnet to connect to the SLB branch office</td>
</tr>
<tr>
<td></td>
<td>manager, or use the web interface.</td>
</tr>
<tr>
<td>BOOTP</td>
<td>Similar to DHCP but for smaller networks.</td>
</tr>
<tr>
<td>Front panel LCD display</td>
<td>You manually assign the IP address and other basic network, console, and</td>
</tr>
<tr>
<td>and keypads</td>
<td>date/time settings. If desired, you can restore the factory defaults.</td>
</tr>
</tbody>
</table>
Method #1 Using the Front Panel Display

**Before you begin, ensure that you have:**

- Unique IP address that is valid on your network (unless automatically assigned)
- Subnet mask (unless automatically assigned)
- Gateway
- DNS settings
- Date, time, and time zone
- Console port settings: baud rate, data bits, stop bits, parity, and flow control

Make sure the SLB branch office manager is plugged into power and turned on.

**Front Panel LCD Display and Keypads**

With the SLB unit powered up, you can use the front panel display and keypad buttons to set up the basic parameters.

![Figure 4-2 Front Panel LCD Display and Five Button Keypads (Enter, Up, Down, Left, Right)](image)

The front panel display initially shows the hostname (abbreviated to 14 letters), total current level, and state of the power supply.

When you click the right-arrow keypad buttons, the SLB network settings display. Using the five keypad buttons, you can change the network, console port, and date/time settings and view the firmware release version. If desired, you can restore the factory defaults.

**Note:** Have your information handy as the display times out without accepting any unsaved changes if you take more than 30 seconds between entries.

Any changes made to the network, console port, and date/time settings take effect immediately.

**Navigating**

The front panel keypad has one **Enter** button (in the center) and four arrow buttons (up, left, right, and down). Press the arrow buttons to navigate from one option to another, or to increment or decrement values.
decrement a numerical entry of the selected option. Use the **Enter** button to select an option to change or to save your settings.

The following table lists the SLB navigation actions, buttons, and options.

**Table 4-3 LCD Arrow Keypad Actions**

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right arrow</td>
<td>To move to the next option (e.g., from Network Settings to Console Settings)</td>
</tr>
<tr>
<td>Left arrow</td>
<td>To return to the previous option</td>
</tr>
<tr>
<td>Enter (center button)</td>
<td>To enter edit mode</td>
</tr>
<tr>
<td>Up and down arrows</td>
<td>Within edit mode, to increase or decrease a numerical entry</td>
</tr>
<tr>
<td>Right or left arrows</td>
<td>Within edit mode, to move the cursor right or left</td>
</tr>
<tr>
<td>Enter</td>
<td>To exit edit mode</td>
</tr>
<tr>
<td>Up and down arrows</td>
<td>To scroll up or down the list of parameters within an option (e.g., from IP Address to Mask)</td>
</tr>
</tbody>
</table>

The following two tables list the SLB settings and parameters displayed on the LCD.
### Table 4-4 Front Panel Setup Options with Associated Parameters

<table>
<thead>
<tr>
<th>Power</th>
<th>Network Settings</th>
<th>Console Port Settings</th>
<th>Date / Time Settings</th>
<th>Release</th>
<th>Current Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Inlets</td>
<td>Eth1 IP Address</td>
<td>Baud Rate</td>
<td>Data Bits</td>
<td>Stop Bits</td>
<td>Parity</td>
</tr>
<tr>
<td>Outlet 1 - 8 On/Off Status</td>
<td>Eth1 Subnet Mask</td>
<td>Date/Time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outlet 1 - 8 Reading</td>
<td>Eth2 IP Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth2 Subnet Mask</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 4-5 Front Panel Options, continued

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>ID</th>
<th>Internal Temperature</th>
<th>User Strings</th>
<th>Location</th>
<th>Device Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLB Serial Number (display only)</td>
<td>Device ID (display only)</td>
<td>Reading in Celsius &amp; Fahrenheit</td>
<td>Displays configured user string(s), if any.</td>
<td>Indicates the Rack (RK), Row (RW) &amp; Cluster (CW) locations.</td>
<td>Detects the connection state of each port: 0=No serial connection 1=Serial connection detected.</td>
</tr>
</tbody>
</table>

**Note:** The individual screens listed from left to right in Table 4-4 and Table 4-5 can be enabled or disabled for display on the SLB LCD screen. The order of appearance of the screens, if enabled, along with the elected “Home Page” may vary on the LCD screen according to configuration. See LCD/Keypad (on page 254) for instructions on enabling and disabling screens.
**Entering the Settings**

To enter setup information:

1. From the normal display (host name, date and time or power supply status), press the right arrow button to display Network Settings. The IP address for Eth1 displays.

*Note:* If you have connected Eth1 to the network, and Eth1 is able to acquire an IP address through DHCP, this IP address displays, followed by the letter [D]. Otherwise, the IP address displays as all zeros (000.000.000.000).

2. Press the **Enter** button on the keypad to enter edit mode. A cursor displays below one character of the existing IP address setting.

3. To enter values:
   - Use the left or right arrow to move the cursor to the left or to the right position.
   - Use the up or down arrow to increment or decrement the numerical value.

4. When you have the set IP address as you want it, press **Enter** to exit edit mode, and then press the down arrow button. The Subnet Mask parameter displays.

*Note:* You must edit the IP address and the Subnet Mask together for a valid IP address combination.

5. To save your entries for one or more parameters in the group, press the right arrow button. The Save Settings? Yes/No prompt displays.

*Note:* If the prompt does not display, make sure you are no longer in edit mode.

6. Use the left/right arrow buttons to select **Yes**, and press the **Enter** button.

7. Press the right arrow button to move to the next option, **Console Settings**.

8. Repeat steps 2-7 for each setting.

9. Press the right arrow button to move to the next option, **Date/Time Settings**, and click **Enter** to edit the time zone.
   - To enter a US time zone, use the up/down arrow buttons to scroll through the US time zones, and then press **Enter** to select the correct one.
   - To enter a time zone outside the US, press the left arrow button to move up to the top level of time zones. Press the up/down arrow button to scroll through the top level.

   A time zone with a trailing slash (such as Africa/) has sub-time zones. Use the right arrow button to select the Africa time zones, and then the up/down arrows to scroll through them.

   Press **Enter** to select the correct time zone. To move back to the top-level time zone at any time, press the left arrow.

10. To save your entries, press the right arrow button. The **Save Settings? Yes/No** prompt displays.

*Note:* If the prompt does not display, make sure you are no longer in edit mode.

11. Use the left/right arrow buttons to select **Yes**, and press the **Enter** button.

12. To review the saved settings, press the up or down arrows to step through the current settings.
When you are done, the front panel returns to the clock display. The network port resets to the new settings, and you can connect to your IP network for further administration. You should be able to SSH to the SLB branch office manager through your network connection, or access the Web interface through a Web browser.

Restoring Factory Defaults

To use the LCD display to restore factory default settings:

1. Press the right arrow button to move to the Release option.
2. Use the down arrow to move to the Restore Factory Defaults option. A prompt for the 6-digit Restore Factory Defaults password displays.
3. Press Enter to enter edit mode.
4. Using the left and right arrows to move between digits and the up and down arrows to change digits, enter the password (the default password is 999999).

Note: The Restore Factory Defaults password is only for the LCD. You can change it at the command line interface using the CLI admin keypad password command.

5. Press Enter to exit edit mode. If the password is valid, a Save Settings? Yes/No prompt displays.
6. To initiate the process for restoring factory defaults, select Yes. When the process is complete, the SLB branch office manager reboots.

Limiting Sysadmin User Access

For security purposes, full administrative access to the SLC or SLB via the default sysadmin local user account can be limited to only the front console port of the SLC or SLB unit.

To configure this:

1. Enable the Sysadmin access limited to Console Port option on the Local/Remote Users web page.
2. Enable a remote authentication method (such as TACACS+ or LDAP) and configure the remote authentication method to be first in the order of methods used.
3. Create a remote user account with full administrative rights.
4. Uncheck the Attempt next method on authentication rejection checkbox on the Authentication Methods web page.

These steps will prevent any local users from logging in, restrict the default sysadmin local user to the front console port, and allow a user with administrative rights to login, as long as remote authentication is working.
To use DHCP to restore a configuration to a factory defaulted SLB:

Utilize the Zero Touch Provisioning Configuration Restore feature, to acquire a default configuration from a DHCP server and TFTP server when it is booted.

1. At boot time, before the normal startup process, a unit will attempt to acquire network parameters and a configuration file, first over Eth1.
2. A unit will then attempt to acquire network parameters and a configuration file over Eth2.
3. See Firmware & Configurations (on page 237) for more information.

Method #2 Quick Setup on the Web Page

After the unit has an IP address, you can use the Quick Setup page to configure the remaining network settings. This page displays the first time you log into the SLB unit only. Otherwise, the SLB Home Page displays.

To complete the Quick Setup page:

1. Open a web browser (Firefox, Chrome or Internet Explorer with JavaScript enabled).
2. In the URL field, type https:// followed by the IP address of your SLB.

Note: The web server listens for requests on the unencrypted (HTTP) port (port 80) and redirects all requests to the encrypted (HTTPS) port (port 443).

3. Log in using sysadmin as the user name and the last 8 characters of the Device ID (for newly manufactured devices that come installed with SLB firmware 7.0.0.0 or later) or PASS (for older devices) as the password. The first time you log in to the SLB, the Quick Setup page automatically displays. Otherwise, the Home page displays.

Note: If the Device ID is not set, the default sysadmin password is the last 8 characters of the serial number.
4. To accept the defaults, select the **Accept** default Quick Setup settings checkbox in the top portion of the page and click the **Apply** button at the bottom of the page. Otherwise, continue with step 5.

*Note:* Once you click the **Apply** button on the Quick Setup page, you can continue using the web interface to configure the SLB branch office manager further.

5. Enter the following settings:
Network Settings

*Note:* Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Eth 1 Settings** | ▶️ Obtain from DHCP: Acquires IP address, subnet mask, hostname and gateway from the DHCP server. (The DHCP server may not provide the hostname gateway, depending on its setup.) This is the default setting. If you select this option, skip to Gateway.  
▶️ Obtain from BOOTP: Lets a network node request configuration information from a BOOTP "server" node. If you select this option, skip to Gateway.  
▶️ Specify: Lets you manually assign a static IP address, generally provided by the system administrator. |

| IP Address (if specifying) | Enter an IP address that is unique and valid on your network. There is no default. Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment. |

*Note:* Currently, the SLB unit does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).

| Subnet Mask | If specifying an IP address, enter the subnet mask for the network on which the SLB unit resides. There is no default. |
| Default Gateway | The IP address of the router for this network. There is no default. |
| Hostname | The default host name is slbXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). The host name becomes the prompt in the command line interface. |
| Domain | If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLB unit. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the SLB branch office manager attempts to resolve abcd.mydomain.com for the SMTP server. |

Date & Time Settings

<table>
<thead>
<tr>
<th>Date &amp; Time Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Date/Time</td>
<td>Select the checkbox to manually enter the date and time at the SLB’s location.</td>
</tr>
<tr>
<td>Date</td>
<td>From the drop-down lists, select the current month, day, and year.</td>
</tr>
<tr>
<td>Time</td>
<td>From the drop-down lists, select the current hour and minute.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>From the drop-down list, select the appropriate time zone.</td>
</tr>
</tbody>
</table>

Administrator Settings

<table>
<thead>
<tr>
<th>Administrator Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysadmin Password</td>
<td>To change the password (e.g., from the default) enter a Sysadmin Password of up to 64 characters.</td>
</tr>
<tr>
<td>Retype Password</td>
<td>Re-enter the Sysadmin Password above in this field as a confirmation.</td>
</tr>
</tbody>
</table>

6. Click the **Apply** button to save your entries.
Method #3 Quick Setup on the Command Line Interface

If the SLB branch office manager does not have an IP address, you can connect a dumb terminal or a PC running a terminal emulation program (VT100) to access the command line interface. (See Connecting Terminals on page 36.) If the unit has an IP address, you can use SSH or Telnet to connect to the SLB.

**Note:** By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the Services > SSH/Telnet/Logging page (see Chapter 7: Services on page 87), a serial terminal connection, or an SSH connection.

To complete the command line interface Quick Setup script:

1. Do one of the following:
   - With a serial terminal connection, power up, and when the command line displays, press Enter.
   - With a network connection, use an SSH program or Telnet program (if Telnet has been enabled) to connect to `xx.xx.xx.xx` (the IP address in dot quad notation), and press Enter. You should be at the login prompt.

2. Enter `sysadmin` as the user name and press Enter.

3. Enter the last 8 characters of the Device ID (for newly manufactured devices that come installed with SLB firmware 7.0.0.0 or later) or `PASS` (for older devices) as the password and press Enter. The first time you log in, the Quick Setup script runs automatically. Normally, the command prompt displays.

   **Note:** If the Device ID is not set, the default sysadmin password is the last 8 characters of the serial number.

Figure 4-7  Beginning of Quick Setup Script

Quick Setup will now step you through configuring a few basic settings.

The current settings are shown in brackets (`[]`). You can accept the current setting for each question by pressing <return>.

4. Enter the following information at the prompts:

   **Note:** To accept a default or to skip an entry that is not required, press Enter.

<table>
<thead>
<tr>
<th>CLI Quick Setup Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Eth1</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>◆ &lt;1&gt; obtain IP Address from DHCP: The unit will acquire the IP address, subnet mask, hostname, and gateway from the DHCP server. (The DHCP server may or may not provide the gateway and hostname, depending on its setup.) This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>◆ &lt;2&gt; obtain IP Address from BOOTP: Permits a network node to request configuration information from a BOOTP &quot;server&quot; node.</td>
</tr>
<tr>
<td></td>
<td>◆ &lt;3&gt; static IP Address: Allows you to assign a static IP address manually. The IP address is generally provided by the system administrator.</td>
</tr>
</tbody>
</table>
Quick Setup will now step you through configuring a few basic settings.

The current settings are shown in brackets (\'[]\').
You can accept the current setting for each question by pressing <return>.

**Ethernet Port and Default Gateway**
The SLB88 has two ethernet ports, Eth1 and Eth2.
By default, both ports are configured for DHCP.
Configure Eth1:  (1) obtain IP Address from DHCP
              (2) obtain IP Address from BOOTP
              (3) static IP Address
Enter 1-3: [1]

The SLB88 can be configured to use a default gateway.

<table>
<thead>
<tr>
<th>CLI Quick Setup Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address (if specifying)</td>
<td>An IP address that is unique and valid on your network and in the same subnet as your PC. There is no default.</td>
</tr>
<tr>
<td></td>
<td>If you selected DHCP or BOOTP, this prompt does not display. Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask specifies the network segment on which the SLB branch office manager resides. There is no default. If you selected DHCP or BOOTP, this prompt does not display.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>IP address of the router for this network. There is no default.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The default host name is slbXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The host name becomes the prompt in the command line interface.</td>
</tr>
<tr>
<td>Domain</td>
<td>If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLB. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the SLB branch office manager attempts to resolve abcd.mydomain.com for the SMTP server.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>If the time zone displayed is incorrect, enter the correct time zone and press Enter. If the entry is not a valid time zone, the system guides you through selecting a time zone. A list of valid regions and countries displays. At the prompts, enter the correct region and country.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>If the date and time displayed are correct, type n and continue. If the date and time are incorrect, type y and enter the correct date and time in the formats shown at the prompts.</td>
</tr>
<tr>
<td>Sysadmin password</td>
<td>Enter a new sysadmin password.</td>
</tr>
</tbody>
</table>
Enter gateway IP Address: [none]

Hostname
The current hostname is 'slb882/8824', and the current domain is '<undefined>'.
The hostname will be shown in the CLI prompt.
Specify a hostname: [slb882/8824]
Specify a domain: [<undefined>]

Time Zone
The current time zone is 'UTC'.
Enter time zone: [UTC]

Date/Time
The current time is Mon April 30 02:33:17 2018
Change the current time? [n]

Sysadmin Password
Enter new password: [<current password>]

Quick Setup is now complete.

Next Step

After completing quick setup on the SLB, you may want to configure other settings. You can use the web page or the command line interface for configuration.

- For information about the web and the command line interfaces, go to *Chapter 5: Web and Command Line Interfaces*.
- To continue configuring the SLB, go to *Chapter 6: Basic Parameters*. 
5: Web and Command Line Interfaces

The SLB branch office manager offers three interfaces for configuring the SLB command line interface (CLI), a web interface, and an LCD with keypads on the front panel. This chapter discusses the web and command line interfaces. (Chapter 4: Quick Setup on page 40 includes instructions for using the LCD to configure basic network settings.)

Web Interface

A web interface allows the system administrator and other authorized users to configure and manage the SLB unit using most web browsers (Firefox, Chrome or Internet Explorer with JavaScript enabled). The SLB branch office manager provides a secure, encrypted web interface over SSL (secure sockets layer).

Note: The web server listens for requests on the unencrypted (HTTP) port (port 80) and redirects all requests to the encrypted (HTTPS) port (port 443).

The following figure shows a typical web page:

![Figure 5-1 Web Page Layout](image)
The web page has the following components:

- **Tabs**: Groups of settings to configure.
- **Options**: Below each tab are options for specific types of settings.

**Note**: Only those options for which the currently logged-in user has rights display.

- **Port and Power Outlet Bar**:
  - The light green **LCD** button allows you to configure the front panel LCD.
  - The gray **U1** button allows you to configure the USB device (flash drive or modem) plugged into the front panel USB connector. The gray **U2** button allows you to configure the internal USB dial-up modem.
  - The blue **E1** and **E2** buttons display the Network > Network Settings (1 of 2) page.
  - The eight green number buttons allow you to select a port and display its settings. Only ports to which the currently logged-in user has rights are enabled.

  Below the bar are three options for use with the port buttons. Selecting a port and the Configuration option takes you to the Device Ports > Settings page. Selecting a port and the WebSSH option displays the WebSSH window for the device port if Web SSH is enabled, and if SSH is enabled for the device port. Selecting the port and the Connected Device button allows access to supported devices such as SLP power managers and/or SensorSoft temperature and humidity probes connected to the device port.
  - The red **P1 - P8** buttons enable you to select a power outlet and display the Devices > Power Outlets page with the selected outlet’s information highlighted.
  - The yellow **A** and **B** buttons display the status of the power supplies.

- **Entry Fields and Options**: Allow you to enter data and select options for the settings.

**Note**: For specific instructions on completing the fields on the web pages, see Chapters 5 through 12.

- **Apply Button**: Apply on each web page makes the changes immediately and saves them so they will be there when the SLB branch office manager is rebooted.
- **Icons**: The icon bar above the Main Menu has icons that display the following:
  - Home page.
  - Information about the SLB unit and Lantronix contact information.
  - Configuration site map.
  - Status of the SLB unit.
- **Help Button**: Provides online Help for the specific web page.
Logging in
Only the system administrator or users with web access rights can log into the web page. More than one user at a time can log in, but the same user cannot login more than once.

To log in to the SLB web interface:
1. Open a web browser.
2. In the URL field, type https:// followed by the IP address of your SLB branch office manager.
3. To configure the SLB unit, use sysadmin as the user name and the last 8 characters of the Device ID (for newly manufactured devices that come installed with SLB firmware 7.0.0.0 or later) or PASS (for older devices) as the password.

Note: The system administrator may have changed the password using one of the Quick Setup methods in the previous chapter.

The Lantronix SLB Quick Setup page displays automatically the first time you log in. Subsequently, the Lantronix SLB Home page displays. (If you want to display the Quick Setup page again, click Quick Setup on the main menu.)

Logging Out
To log off the SLB web interface:
1. Click the Logout button located on the upper left part of any user interface page. You are brought back to the login screen when logout is complete.

Web Page Help
To view detailed information about an SLB web page:
1. Click the Help button to the right of any user interface page. Online Help contents will appear in a new browser.

Command Line Interface
A command line interface (CLI) is available for entering all the commands you can use with the SLB. In this User Guide, after each section of instructions for using the web interface, you will find the equivalent CLI commands. You can access the command line interface using Telnet, SSH, or a serial terminal connection.

Note: By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the Services > SSH/Telnet/Logging web page, a serial terminal connection, or an SSH connection. (See Chapter 7: Services.)

The sysadmin user and users with who have full administrative rights have access to the complete command set, while all other users have access to a reduced command set based on their permissions.
Logging In

To log in to the SLB command line interface:

1. Do one of the following:
   
   - With a serial terminal connection, power up, and when the command line displays, press Enter.
   - If the SLB branch office manager already has an IP address (assigned previously or assigned by DHCP), Telnet (if Telnet has been enabled) or SSH to xx.xx.xx.xx (the IP address in dot quad notation) and press Enter. The login prompt displays.

2. To log in as the system administrator for setup and configuration, enter sysadmin as the user name and press Enter.

3. Enter the last 8 characters of the Device ID (for newly manufactured devices that come installed with SLB firmware 7.0.0.0 or later) or PASS (for older devices) as the password and press Enter. The first time you log in, the Quick Setup script runs automatically. Normally, the command prompt displays. (If you want to display the Quick Setup script again, use the admin quicksetup command.)

   Note: The system administrator may have changed the password using one of the Quick Setup methods in the previous chapter.

To log in any other user:

1. Enter your SLB user name and press Enter.

2. Enter your SLB password and press Enter.

Logging Out

To log out of the SLB command line interface, type logout and press Enter.

Command Syntax

Commands have the following format:

```
<action> <category> <parameter(s)>
```

where

- `<action>` is set, show, connect, admin, diag, or logout.
- `<category>` is a group of related parameters whose settings you want to configure or view. Examples are ntp, deviceport, and network.
- `<parameter(s)>` is one or more name-value pairs in one of the following formats:

| `<parameter name>` <aa|bb> | User must specify one of the values (aa or bb) separated by a vertical line ( | ). The values are in all lowercase and must be entered exactly as shown. Bold indicates a default value. |
|--------------------------|---------------------------------------------------------------------------------------------------|
| `<parameter name>` <Value> | User must specify an appropriate value, for example, an IP address. The parameter values are in mixed case. Square brackets [ ] indicate optional parameters. |
Table 5-2 Actions and Category Options

<table>
<thead>
<tr>
<th>Action</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>auth</td>
</tr>
<tr>
<td>show</td>
<td>auth</td>
</tr>
<tr>
<td>connect</td>
<td>bidirection</td>
</tr>
<tr>
<td>diag</td>
<td>arp</td>
</tr>
<tr>
<td>admin</td>
<td>banner</td>
</tr>
<tr>
<td>logout</td>
<td>Terminates CLI session.</td>
</tr>
</tbody>
</table>

Command Line Help

- For general Help and to display the commands to which you have rights, type: help
- For general command line Help, type: help command line
- For more information about a specific command, type help followed by the command. For example: help set network or help admin firmware

Tips

- Type enough characters to identify the action, category, or parameter name uniquely. For parameter values, type the entire value. For example, you can shorten:
  set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0 to
  se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
- Use the Tab key to automatically complete action, category, or parameter names. Type a partial name and press Tab either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, Tab displays all possible names.
- Should you make a mistake while typing, backspace by pressing the Backspace key and/or the Delete key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the left and right arrow keys to move within a command.
- Use the up and down arrows to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- To clear an IP address, type 0.0.0.0, or to clear a non-IP address value, type CLEAR.
When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until the user is ready to continue. To display the next line, press Enter, and to display the page, press the space bar. You can override the number of lines (or disable the feature altogether) with the set cli command.

### General CLI Commands

The following commands relate to the CLI itself.

**To configure the current command line session:**

```
set cli scscommands <enable|disable>
```

Allows you to use SCS-compatible commands as shortcuts for executing commands:

**Note:** Settings are retained between CLI sessions for local users and users listed in the remote users list.

<table>
<thead>
<tr>
<th>SCS Commands</th>
<th>SLB Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td>'show sysstatus'</td>
</tr>
<tr>
<td>version</td>
<td>'admin version'</td>
</tr>
<tr>
<td>reboot</td>
<td>'admin reboot'</td>
</tr>
<tr>
<td>poweroff</td>
<td>'admin shutdown'</td>
</tr>
<tr>
<td>listdev</td>
<td>'show deviceport names'</td>
</tr>
<tr>
<td>direct</td>
<td>'connect direct deviceport'</td>
</tr>
<tr>
<td>listen</td>
<td>'connect listen deviceport'</td>
</tr>
<tr>
<td>clear</td>
<td>'set locallog clear'</td>
</tr>
<tr>
<td>telnet</td>
<td>'connect direct telnet'</td>
</tr>
<tr>
<td>ssh</td>
<td>'connect direct ssh'</td>
</tr>
</tbody>
</table>

**To set the number of lines displayed by a command:**

```
set cli terminallines <disable|Number of lines>
```

Sets the number of lines in the terminal emulation (screen) for paging through text one screenful at a time, if the SLB branch office manager cannot detect the size of the terminal automatically.

**To show current CLI settings:**

```
show cli
```

**To view the last 100 commands entered in the session:**

```
show history
```
To clear the command history:

set history clear

To view the rights of the currently logged-in user:

show user

Note: For information about user rights, see Chapter 11: User Authentication.
6: Basic Parameters

This chapter explains how to set the following basic configuration settings for the SLB branch office manager using the SLB web interface or the CLI:

- Network parameters that determine how the SLB branch office manager interacts with the attached network
- Firewall and routing
- Date and time

Note: If you entered some of these settings using a Quick Setup procedure, you may update them here.

Requirements

If you assign a different IP address from the current one, it must be within a valid range, unique to your network, and with the same subnet mask as your workstation.

To configure the unit, you need the following information:

Eth1
- IP address: ________ - ________ - ________ - ________
- Subnet mask: ________ - ________ - ________ - ________

Eth2
- IP address (optional): ________ - ________ - ________ - ________
- Subnet mask (optional): ________ - ________ - ________ - ________

Gateway: ________ - ________ - ________ - ________
DNS: ________ - ________ - ________ - ________
To enter settings for one or both network ports:

1. Click the **Network** tab and select the **Network Settings** option. *Figure 6-1* and *Figure 6-2* show the page that displays:
2. Enter the following information:

**Eth1 and Eth2 Settings**

*Note:* Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.

| Eth1 Settings or Eth2 Settings | **Disabled:** If selected, disables the network port.  
|                               | **Obtain from DHCP:** Acquires IP address, subnet mask, hostname and gateway from the DHCP server. (The DHCP server may not provide the hostname gateway, depending on its setup.) This is the default setting. If you select this option, skip to Gateway.  
|                               | **Obtain from BOOTP:** Lets a network node request configuration information from a BOOTP "server" node. If you select this option, skip to Gateway.  
|                               | **Specify:** Lets you manually assign a static IP address, generally provided by the system administrator.  
| IP Address (if specifying)    | **Enter an IP address that will be unique and valid on your network. There is no default.**  
|                               | **Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment.**  

*Note:* Currently, the SLB branch office manager does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).
### Subnet Mask
If specifying an IP address, enter the network segment on which the SLB unit resides. There is no default.

### IPv6 Address
Address of the port in IPv6 format.

**Note:** The SLB branch office manager supports IPv6 connections for a limited set of services: the web, SSH, and Telnet.

IPv6 addresses are written as 8 sets of 4-digit hexadecimal numbers separated by colons. There are several rules for modifying the address. For example:


### IPv6 Address (Link Local)
An IPv6 address that is intended only for communications within the segment of a local network.

### Mode
Select the direction (full duplex or half-duplex) and speed (10 or 100Mbit) of data transmission. The default is Auto, which allows the Ethernet port to auto-negotiate the speed and duplex with the hardware endpoint to which it is connected.

### MTU
Displays the multicast address of the Ethernet port.

### Enable IPv6
Select this box to enable the IPv6 protocol. Disabled by default.

### Ethernet Bonding
Ethernet 1 and Ethernet 2 can be bonded to support redundancy (Active Backup), aggregation (802.3ad), and load balancing. Disabled by default. Note that if Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported.

### Enable IP Forwarding
IP forwarding enables network traffic received on one interface (Eth1, Eth2, or an external/USB modem attached to the SLB branch office manager with an active PPP connection) to be transferred out another interface (any of the above). The default behavior (if IP forwarding is disabled) is for network traffic to be received but not routed to another destination. Enabling IP forwarding is required if you enable Network Address Translation (NAT) for any device port modem or USB/ISDN modem. IP forwarding allows a user accessing the SLB unit over a modem to access the network connected to Eth1 or Eth2.

**Note:** Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.

### Hostname & Name Servers

#### Hostname
The default host name is slbXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). The host name becomes the prompt in the command line interface.

#### Domain
If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLB. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the SLB branch office manager attempts to resolve abcd.mydomain.com for the SMTP server.
DNS Servers

| DNS Servers | Configure up to three name servers. #1 is required if you choose to configure DNS (Domain Name Server) servers. The first three DNS servers acquired via DHCP through Eth1 and/or Eth2 display automatically. |

DHCP-Acquired DNS Servers

| #1 - #3 | Displays the IP address of the name servers if automatically assigned by DHCP. |

GPRS-Acquired DNS Servers

| #1 - #3 | Displays the IP address of the name servers if automatically assigned by General Packet Radio Service (GPRS). |

TCP Keepalive Parameters

| Start Probes | Number of seconds the SLB branch office manager waits after the last transmission before sending the first probe to determine whether a TCP session is still alive. The default is 600 seconds (10 minutes). |
| Number of Probes | Number of probes the SLB unit sends before closing a session. The default is 5. |
| Interval | The number of seconds the SLB unit waits between probes. The default is 60 seconds. |

Gateway

| Default | IP address of the router for this network. If this has not been set manually, any gateway acquired by DHCP for Eth1 or Eth2 displays. All network traffic that matches the Eth1 IP address and subnet mask is sent out Eth1. All network traffic that matches the Eth2 IP address and subnet mask is sent out Eth2. If you set a default gateway, any network traffic that does not match Eth1 or Eth2 is sent to the default gateway for routing. |
| DHCP-Acquired | Gateway acquired by DHCP for Eth1 or Eth2. View only. |
| GPRS-Acquired | Displays the IP address of the router if it has been automatically assigned by General Packet Radio Service (GPRS). View only. |
| Precedence | Indicates whether the gateway acquired by DHCP, GPRS or the default gateway takes precedence. The default is DHCP Gateway. If the DHCP Gateway is selected and both Eth1 and Eth2 are configured for DHCP, the SLB unit gives precedence to the Eth1 gateway. |
| Enable IP Forwarding | IP forwarding enables network traffic received on one interface (Eth1, Eth2, or an external/USB modem attached to the SLB branch office manager with an active PPP connection) to be transferred out another interface (any of the above). The default behavior (if IP forwarding is disabled) is for network traffic to be received but not routed to another destination. Enabling IP forwarding is required if you enable Network Address Translation (NAT) for any device port modem or USB/ISDN modem. IP forwarding allows a user accessing the SLB unit over a modem to access the network connected to Eth1 or Eth2. |
Fail-Over Settings

| **Fail-Over Gateway IP Address** | An alternate IP address of the router for this network, to be used if an IP address usually accessible through the default gateway fails to return one or more pings. A fail-over event happens when the IP Address to Ping to Trigger Fail-Over reachable via Ethernet Port for Ping and the default gateway, becomes unreachable. Fail-back is when the IP Address to Ping becomes reachable again, causing the primary default route to be restored.  

*Note: The fail-over gateway is not supported when DHCP is used.* |
| **IP Address to Ping to Trigger Fail-over** | IP address to ping to determine whether to use the fail-over gateway. |
| **Ethernet Port to Ping** | Ethernet port to use for the ping. |
| **Delay between Pings** | Number of seconds between pings. |
| **Number of Failed Pings** | Number of pings that fail before the SLB branch office manager uses the fail-over gateway. |
## Fail-Over Cellular Gateway Configuration

| Fail-over Device | Select an integrated external device to be used as the fail-over gateway. Currently the **Sierra Wireless ES450** Cellular Gateway and the **Lantronix G520 Series (G52x)** Cellular Gateway are supported. The Sierra gateway must be properly provisioned before first use by initializing the APN of the installed SIM card. This is done by connecting the Sierra gateway to the second ethernet port of the SLB, and assigning a static IP address to the SLB port so that it is in the same subnet as the IP address of the Sierra gateway. Use the console CLI or web GUI to set the APN of the SIM card. After setting the APN, power cycle the Sierra gateway and allow it to reboot completely. The Lantronix G520 Series (G52x) gateway must be configured before it can be used as the fail-over gateway. The default **admin** user password must be changed to a new password, and the DHCP server must be disabled. For factory reset device, you need to first login as root and default password as **L@ntr0n1x**. Please note after factory reset, the G52x WebGUI will show the default user as **admin**; you need to delete it and enter the username as **root**. Once you login as **root** with default password as **L@ntr0n1x**, you can change the password for **root** user and set a password for **admin** user. After you save and apply, the G52x WebGUI will re-direct to login page where you can login as **admin** or **root**. Default IP Address:  
Lantronix G52x Series: 192.168.1.1  
Sierra Wireless ES450: 192.168.13.31  
The failover feature requires that both Ethernet ports be configured with a static IP address. Using DHCP on one of the Ethernet ports may overwrite the default route, interfering with fail-over and fail-back.  

**Note:** The commands sent to the fail-over device to retrieve status and update the configuration are shown in the syslog (messages may be displayed under Network syslog; at the Debug level). If there are errors retrieving status or updating the configuration, check messages in the Network syslog, the device administrator login/password, connectivity to the device and the firmware version of the fail-over device (the minimum required firmware version for Sierra Wireless ES450 is 4.9.2 and for the Lantronix G520 Series (G52x) gateway is 1.8.0.0). When the SLB sends an updated configuration to the fail-over device, it is recommended to check the SLB syslog, even if the SLB indicates that the update was successful. Responses from the fail-over device indicating that the device needs to be rebooted for configuration changes to take effect may also be in the syslog. The configuration will be resent to the device if any of the fail-over device settings are changed, or the selected fail-over device is changed from None to one of the supported fail-over device types. When a fail-over or fail-back occurs, running applications such as VPN tunnel and ConsoleFlow will be restarted.  

| APN of Mobile Carrier | For the Sierra and Lantronix G520 Series (G52x) gateways, configure the Access Point Name for the mobile carrier. May have up to 80 characters. |
6: Basic Parameters

Admin Login and Password/Retype
For the selected Fail-over Device, the administrator login and password used to retrieve status from the device and send configuration updates to the device. The login may have up to 32 characters, and the password may have up to 64 characters. The Admin Password displays the current password masked.

Default login credentials of the Sierra Wireless ES450:
Admin login name: user
Admin password: 12345

Default login credentials of the Lantronix G520 Series (G52x):
Admin login name: admin
Admin password: No default password, Current G52x working password.

Change Admin Password (check box)
Select this check box if you wish to update the admin password for the selected gateway Fail-over Device.

New Admin Password/Retype
For the selected Fail-over Device, the administrator password can be changed on the gateway. The password may have up to 64 characters.

Reboot Gateway When Making Changes (check box)
For the selected Fail-over Device, the administrator can reboot the gateway.

Fail-Over Cellular Gateway Status (link)
Clicking the link opens the Fail-Over Cellular Gateway status window, showing status and statistics about the fail-over gateway. Click Back to Network Settings to return to the Network Settings page.

Advanced Cellular Gateway Configuration

SIM Card PIN Lock (check box)
For the Sierra and Lantronix G520 Series (G52x) gateways, enable a lock so that the SIM card used by the gateway cannot be used by anyone who does not have the PIN.

Pin # for SIM Card/Retype
For the Sierra and Lantronix G520 Series (G52x) gateways, the PIN number for the SIM card used by the gateway. May have up to 8 characters.

SIM PUK/Retype
For the Lantronix G520 Series (G52x) gateway, the SIM Personal Unblocking Key. May have up to 16 characters. The Sierra gateway does not have this feature. SIM status in case of Lantronix G520 Series (G52x) gateway is not verified in SLB, SLB directly forwards the request to Lantronix G520 Series (G52x) gateway.

SIM Username
For the Lantronix G520 Series (G52x) gateway, enter the username for dial up to the cellular carrier, if required. May have up to 64 characters. The Sierra gateway does not have this feature.

SIM Password
For the Lantronix G520 Series (G52x) gateway, enter the password for dial up to the cellular carrier, if required. May have up to 64 characters. The Sierra gateway does not have this feature.

Dial-up String
For the Lantronix G520 Series (G52x) gateway, enter the modem string used for making a connection to the carrier. May have up to 64 characters. The Sierra gateway does not have this feature. The Lantronix G520 Series (G52x) gateway supports only three values pap, chap or none.
**6: Basic Parameters**

**Passthrough Mode**

For the Sierra and Lantronix G520 Series (G52x) gateways, enable or disable the IP Passthrough Mode. This mode allows the Sierra ES450 gateway to pass its WAN IP address to the selected ethernet interface of the console manager. The Sierra ES450 gateway will be rebooted on enabling or disabling this option.

When Passthrough is enabled, cellular DHCP will be automatically enabled. The IP Passthrough Mode is also supported in fail-over/fail-back scenario for a consistent IP and gateway. The fail-over feature does not handle changes in the fail-over gateway IP address for IP passthrough configurations.

If there is a communication failure with the Sierra ES450 on setting or unset operation Passthrough related parameters (such as Passthrough Mode, Cellular DHCP or Ethernet IP) with Eth2 set to DHCP, to work around this issue: first retry the configuration with a static IP setting for Eth2 and then subsequently change the Eth2 mode to DHCP. The Lantronix G520 Series (G52x) gateway does not support this feature.

*Note:* We recommend you wait till Sierra ES450 completes the rebooting process before you configure any other network parameter, or else, an error appears indicating that Sierra ES450 could not respond to the request.

**Ethernet IP**

Ethernet IP address of the Sierra ES450 gateway. This will mainly be used in conjunction with Passthrough Mode to remotely configure the Sierra ES450 options. If IP Passthrough Mode is disabled then this IP address will be ignored and IP address of the Alternate Gateway field will be used to configure Sierra ES450. The Lantronix G520 Series (G52x) gateway does not support this feature.

**Cellular DHCP**

For the Sierra ES450 gateway, enable or disable the DHCP server. This will mainly be used in conjunction with Passthrough Mode. The Sierra ES450 Gateway will get rebooted on enabling or disabling this option.

*Note:* We recommend you wait till Sierra ES450 completes the rebooting process before you configure any other network parameter, or else, an error appears indicating that Sierra ES450 could not respond to the request.

**Fail-Over Cellular Gateway Firmware**

*Note:* The Sierra fail-over device must be selected in order for you to be able to update the firmware.

**Update Firmware (check box)**

Select this option to update firmware on the Sierra gateway or on the Lantronix G520 Series (G52x) gateway. The Functional Firmware file and the Radio Firmware file will be transferred to the SLB using the method selected by the Load Firmware via option. Once the files have been transferred to the SLB, the SLB will initiate the firmware update on the gateway. The Lantronix G520 Series (G52x) gateway firmware upgrade may take 3 to 6 minutes.

**Firmware Filename**

Enter the name of the firmware filename exactly as it is represented.

**Radio Firmware Filename**

Enter the name of the radio firmware filename exactly as it is represented.

**Load Firmware via**

Select the method to load the firmware from the options in the drop-down menu.

**Load Cellular Gateway Firmware Options**

**FTP/SFTP/SCP Server**

Enter the server address from where to load the firmware.

**Path**

Enter the server directory pathway to the files.

**Login**

Enter the user login for the FTP/SFTP/SCP server to verify access rights to load new firmware.
3. To save your entries, click the **Apply** button. **Apply** makes the changes immediately and saves them so they will be there when the SLB branch office manager is rebooted.

### Ethernet Counters

The *Network > Network Settings (1 of 2)* page displays statistics for each of the SLB's Ethernet ports since boot-up. The system automatically updates them.

*Note:* *For Ethernet statistics for a smaller time period, use the* diag perfstat *command.*

### Network Commands

Go to *Network Commands (on page 320)* to view CLI commands which correspond to the web page entries described above.

### IP Filter

IP filters (also called a rule set) act as a firewall to allow or deny individual or a range of IP addresses, ports, and protocols. When a network connection is configured to use an IP filter, all network traffic through that connection is compared, in order, to the rules of that filter. Network traffic may be allowed to pass, it may be dropped (without notice), or it may be rejected (sends back an error packet) depending upon the rules of that filter rule set. A ruleset can contain a maximum of 256 rules.

The administrator uses the *Network > IP Filter* page to view, add, edit, delete, and map IP filters,

*Warning:* *IP filters configuration is a feature for advanced users. Adding and enabling IP filter sets incorrectly can disable your SLB.*

### Viewing IP Filters

You can view a list of filters and a table showing how each filter is mapped to an interface.

**To view a list of IP filters:**

1. Click the **Network** tab and select the **IP Filter** option. The following page displays:
Enabling IP Filters
On the Network > IP Filter page, you can enable all filters or disable all filters.

*Note:* There is no way to enable or disable individual filters.

**To enable IP filters:**

1. Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IP Filter</td>
<td>Select the Enable IP Filter checkbox to enable all filters, or clear the checkbox to disable all filters. Disabled by default.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>Displays the number of data packets that the filter ignored (did not respond to). View only.</td>
</tr>
<tr>
<td>Packets Rejected</td>
<td>Displays the number of data packets that the filter sent a “rejected” response to. View only.</td>
</tr>
<tr>
<td>Test Timer</td>
<td>Timer for testing IP Filter rulesets. Select No to disable the timer. Select Yes, minutes (1-120) to enable the timer and enter the number of minutes the timer should run. The timer automatically disables the IP Filters when the time expires.</td>
</tr>
<tr>
<td>Time Remaining</td>
<td>Indicates how many minutes are left on the timer before it expires and IP Filters disabled. View only.</td>
</tr>
</tbody>
</table>

Configuring IP Filters
The administrator can add, edit, delete, and map IP filters.

*Note:* A configured filter has no effect until it is mapped to a network interface. See Mapping a Ruleset on page 72.
To add an IP filter:

1. On the Network > IP Filter page, click the Add Ruleset button. The following page displays:

![Network > IP Filter Ruleset (Adding/Editing Rulesets)](image)

Rule sets can be added or updated on this page.

2. Enter the following:

<table>
<thead>
<tr>
<th>Rule Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Parameters</td>
<td>Name that identifies a filter; may be composed of letters, numbers, and hyphens only. (The name cannot start with a hyphen.) Example: FILTER-2</td>
</tr>
<tr>
<td>IP Address(es)</td>
<td>Specify a single IP address to act as a filter. Example: 172.19.220.64 – this specific IP address only</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify a subnet mask to act determine how much of the address should apply to the filter. Example: 255.255.255.255 to specify the whole address should apply.</td>
</tr>
<tr>
<td>Protocol</td>
<td>From the drop-down list, select the type of protocol through which the filter will operate. The default setting is All.</td>
</tr>
</tbody>
</table>
3. Click the right arrow button to add the new rule to the bottom of the Rules list box on the right. A ruleset can contain a maximum of 256 rules.

4. To remove a rule from the filter set, highlight that line and click the left arrow. The rule populates the rule definition fields, allowing you to make minor changes before reinserting the rule. To clear the definition fields, click the Clear button.

5. To change the order of priority of the rules in the list box, select the rule to move and use the up or down arrow buttons on the right side of the filter list box.

6. To save, click the Apply button. The new filter displays in the menu tree.

**Note:** To add another new filter rule set, click the Back to IP Filter link to return to the Network > IP Filter page.

### Port Range
Enter a range of destination TCP or UDP port numbers to be tested. An entry is required for TCP, TCP New, TCP Established, and UDP, and is not allowed for other protocols. Separate multiple ports with commas. Separate ranges of ports by colons.

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 – filter on port 22 only</td>
</tr>
<tr>
<td>23,64,80 – filter on ports 23, 64 and 80</td>
</tr>
<tr>
<td>23:64,80,143:150 – filter on ports 23 through 64, port 80 and ports 143 through 150</td>
</tr>
</tbody>
</table>

### Action
Select whether to Drop, Reject, or Accept communications for the specified IP address, subnet mask, protocol, and port range. Drop ignores the packet with no notification. Reject ignores the packet and sends back an error message. Allow permits the packet through the filter.

### Generate rule to allow service
You may wish to “punch holes” in your filter set for a particular protocol or service. For instance, if you have configured your NIS server and wish to create an opening in your filter set, select the NIS option and click the Add Rule button. This entry adds a new rule to your filter set using the NIS-configured IP address. Other services and protocols added automatically generate the necessary rule to allow their use.
Updating an IP Filter

To update an IP filter rule set:

1. From the Network > IP Filter page, the administrator selects the IP filter ruleset to be edited and clicks the Edit Ruleset button to return to the Network > IP Filter Ruleset (Adding/Editing Rulesets) page (see Figure 6-4).

2. Edit the information as desired and click the Apply button.

Deleting an IP Filter

To delete an IP filter rule set:

1. On the Network > IP Filter page, the administrator selects the IP filter ruleset to be deleted and clicks the Delete Ruleset button.

Mapping a Ruleset

The administrator can assign an IP Filter Ruleset to a network interface (Ethernet interface) and a modem connected to a Device Port.

To map a rule set to a network interface:

1. On the Network > IP Filter page, select the IP filter ruleset to be mapped.
2. From the Interface drop-down list, select the interface and click the Map Ruleset button. The Interface and rule set display in the IP Filter Mappings table.

To delete a mapping:

1) On the Network > IP Filter page, select the mapping from the list and click the Delete Mapping button. The mapping no longer displays.

2) Click the Apply button.

IP Filter Commands

Go to IP Filter Commands (on page 316) to view CLI commands which correspond to the web page entries described above

Routing

The SLB branch office manager allows you to define static routes and, for networks using Routing Information Protocol (RIP)-capable routes, to enable the RIP protocol to configure the routes dynamically.

To configure routing settings:

1. Click the Network tab and select the Routing option. The following page displays:
2. Enter the following:

**Dynamic Routing**

<table>
<thead>
<tr>
<th>Enable RIP</th>
<th>Select to enable Dynamic Routing Information Protocol (RIP) to assign routes automatically. Disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP Version</td>
<td>Select the RIP version. The default is 2.</td>
</tr>
</tbody>
</table>

**Static Routing**

| Enable Static Routing | Select to assign the routes manually. The system administrator usually provides the routes. Disabled by default. |

- To add a static route, enter the **IP Address**, **Subnet Mask**, and **Gateway** for the route and click the Add/Edit Route button. The route displays in the Static Routes table. You can add up to 64 static routes.
- To edit a static route, select the radio button to the right of the route, change the **IP Address**, **Subnet Mask**, and **Gateway** fields as desired, and click the Add/Edit Route button.
- To delete a static route, select the radio button to the right of the route and click the Delete Route button.

3. Click the **Apply** button.

**Note:** To display the routing table, status or specific report, see the section, Status/Reports on page 249.

**Routing Commands**

Go to Routing Commands (on page 332) to view CLI commands which correspond to the web page entries described above.
VPN

This page can be used to create a Virtual Private Network (VPN) tunnel to the SLB branch office manager for secure communication between the SLB unit and a remote host or gateway. The SLB unit supports IPsec tunnels using Encapsulated Security Payload (ESP). The SLB branch office manager supports host-to-host, net-to-net, host-to-net, and roaming user tunnels.

**Note:** To allow VPN tunnel access if the SLB firewall is enabled, traffic to UDP ports 500 and 4500 from the remote host should be allowed, as well as protocol ESP from the remote host.

**To complete the VPN page:**

1. Click the **Network** tab and select the **VPN** option. The following page displays:

   ![Network > VPN](image)

   - **Enable VPN Tunnel**
   - **Current VPN Tunnel Status:** Down
   - **Name:**
   - **Ethernet Port:**
   - **Remote Host:**
   - **Remote Id:**
   - **Remote Hop/Router:**
   - **Remote Subnet(s):**
   - **Local Id:**
   - **Local Hop/Router:**
   - **Local Subnet(s):**
   - **IKE Negotiation:** Main Mode, Aggressive Mode
   - **IKE Encryption:** Any, Authentication: Any, DH Group: Any
   - **ESP Encryption:** Any, Authentication: Any, DH Group: Any
   - **Authentication:** RSA Public Key, Pre-Shared Key
   - **RSA Public Key for Remote Host:**
   - **Pre-Shared Key:**
   - **Perfect Forward Secrecy:**
   - **Mode Configuration Client:**
   - **XAUTH Client:**
   - **XAUTH Login:**
   - **XAUTH Password:**
   - **Retype Password:**
   - **Apply**
2. Enter the following:

<table>
<thead>
<tr>
<th><strong>Enable VPN Tunnel</strong></th>
<th>Select to create a tunnel.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The name assigned to the tunnel. Required to create a tunnel.</td>
</tr>
<tr>
<td><strong>Only start VPN tunnel in network fail-over mode</strong></td>
<td>Select to start the VPN tunnel in network fail-over mode only. The VPN tunnel will not start if network fail-over parameters are configured and the network is not in fail-over mode. Once a network fail-over happens, the VPN tunnel will automatically be brought up; when network fail-back happens, the VPN tunnel will automatically be torn down. If this feature is enabled but the network fail-over parameters are not configured, this setting will be ignored and the VPN tunnel will be started normally and run continuously. Disabled by default.</td>
</tr>
<tr>
<td><strong>Ethernet Port</strong></td>
<td>Select ethernet port 1 or 2.</td>
</tr>
<tr>
<td><strong>Remote Host</strong></td>
<td>The IP address of the remote host’s public network interface. The special value of any can be entered if the remote host is a roaming user who may not have the same IP address each time a tunnel is created. In this case, it is recommended that the Remote Id also be configured.</td>
</tr>
<tr>
<td><strong>Remote Id</strong></td>
<td>How the remote host should be identified for authentication. The Id is used to select the proper credentials for communicating with the remote host.</td>
</tr>
<tr>
<td><strong>Remote Hop/Router</strong></td>
<td>If the remote host is behind a gateway, this specifies the IP address of the gateway’s public network interface.</td>
</tr>
<tr>
<td><strong>Remote Subnet(s)</strong></td>
<td>One or more subnets behind the remote host, expressed in CIDR notation (IP address/mask bits). If multiple subnets are specified, the subnets should be separated by a comma.</td>
</tr>
<tr>
<td><strong>Local Id</strong></td>
<td>How the SLB branch office manager should be identified for authentication. The Id is used by the remote host to select the proper credentials for communicating with the SLB.</td>
</tr>
<tr>
<td><strong>Local Hop/Router</strong></td>
<td>If the SLB unit is behind a gateway, this specifies the IP address of the gateway’s public network interface.</td>
</tr>
<tr>
<td><strong>Local Subnet(s)</strong></td>
<td>One or more subnets behind the SLB, expressed in CIDR notation (IP address/mask bits). If multiple subnets are specified, the subnets should be separated by a comma.</td>
</tr>
<tr>
<td><strong>IKE Negotiation</strong></td>
<td>The Internet Key Exchange (IKE) protocol is used to exchange security options between two hosts who want to communicate via IPsec. The first phase of the protocol authenticates the two hosts to each other and establishes the Internet Security Association Key Management Protocol Security Association (ISAKMP SA). The second phase of the protocol establishes the cryptographic parameters for protecting the data passed through the tunnel, which is the IPsec Security Association (IPsec SA). The IPsec SA can periodically be renegotiated to ensure security. The IKE protocol can use one of two modes: Main Mode, which provides identity protection and takes longer, or Aggressive Mode, which provides no identity protection but is quicker. With Aggressive Mode, there is no negotiation of which cryptographic parameters will be used; each side must give the correct cryptographic parameters in the initial package of the exchange, otherwise the exchange will fail. If Aggressive Mode is used, the IKE Encryption, IKE Authentication, and IKE DH Group must be specified.</td>
</tr>
<tr>
<td><strong>IKE Encryption</strong></td>
<td>The type of encryption, 3DES or AES, used for IKE negotiation. Any can be selected if the two sides can negotiate which type of encryption to use.</td>
</tr>
<tr>
<td><strong>Authentication (ike)</strong></td>
<td>The type of authentication, SHA1 or MD5, used for IKE negotiation. Any can be selected if the two sides can negotiate which type of authentication to use.</td>
</tr>
</tbody>
</table>
3. To save, click **Apply** button.

4. To see a details of the VPN tunnel connection, including the cryptographic algorithms used, select the **View Detailed Status** link.

5. To see the last 100 lines of the logs associated with the VPN tunnel, select the **View VPN Logs** link.

6. To see the RSA public key for the SLB branch office manager (required for configuring the remote host if RSA Public Keys are being used), select the **View SLB RSA Public Key** link.

<table>
<thead>
<tr>
<th><strong>DH Group</strong> (Ike)</th>
<th>The Diffie-Hellman Group, 2 or 5, used for IKE negotiation. <strong>Any</strong> can be selected if the two sides can negotiate which Diffie-Hellman Group to use.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESP Encryption</strong></td>
<td>The type of encryption, <strong>3DES</strong> or <strong>AES</strong>, used for encrypting the data sent through the tunnel. <strong>Any</strong> can be selected if the two sides can negotiate which type of encryption to use.</td>
</tr>
<tr>
<td><strong>Authentication</strong> (Ike)</td>
<td>The type of authentication, <strong>SHA1</strong> or <strong>MD5</strong>, used for authenticating data sent through the tunnel. <strong>Any</strong> can be selected if the two sides can negotiate which type of authentication to use.</td>
</tr>
<tr>
<td><strong>DH Group</strong> (Ike)</td>
<td>The Diffie-Hellman Group, 2 or 5, used for the key exchange for data sent through the tunnel. <strong>Any</strong> can be selected if the two sides can negotiate which Diffie-Hellman Group to use.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The type of authentication used by the host on each side of the VPN tunnel to verify the identity of the other host. For <strong>RSA Public Key</strong>, each host generates a RSA public-private key pair, and shares its public key with the remote host. The RSA Public Key for the SLB branch office manager (which has 2192 bits) can be viewed at either the web or CLI. For <strong>Pre-Shared Key</strong>, each host enters the same passphrase to be used for authentication.</td>
</tr>
<tr>
<td><strong>RSA Public Key for Remote Host</strong></td>
<td>If <strong>RSA Public Key</strong> is selected for authentication, enter the public key for the remote host.</td>
</tr>
<tr>
<td><strong>Pre-Shared Key</strong></td>
<td>If <strong>Pre-Shared Key</strong> is selected for authentication, enter the key.</td>
</tr>
<tr>
<td><strong>Retype Pre-Shared Key</strong></td>
<td>If <strong>Pre-Shared Key</strong> is selected for authentication, re-enter the key.</td>
</tr>
<tr>
<td><strong>Perfect Forward Secrecy</strong></td>
<td>When a new IPsec SA is negotiated after the IPsec SA lifetime expires, a new Diffie-Hellman key exchange can be performed to generate a new session key to be used to encrypt the data being sent through the tunnel. If this is enabled, it provides greater security, since the old session keys are destroyed.</td>
</tr>
<tr>
<td><strong>Mode Configuration Client</strong></td>
<td>If this is enabled, the SLB unit can receive network configuration from the remote host. This allows the remote host to assign an IP address/netmask to the SLB unit side of the VPN tunnel.</td>
</tr>
<tr>
<td><strong>XAUTH Client</strong></td>
<td>If this is enabled, the SLB branch office manager will send authentication credentials to the remote host if they are requested. XAUTH, or Extended Authentication, can be used as an additional security measure on top of the Pre-Shared Key or RSA Public Key.</td>
</tr>
<tr>
<td><strong>XAUTH Login</strong> (Client)</td>
<td>If <strong>XAUTH Client</strong> is enabled, this is the login used for authentication.</td>
</tr>
<tr>
<td><strong>XAUTH Password</strong></td>
<td>If <strong>XAUTH Client</strong> is enabled, this is the password used for authentication.</td>
</tr>
<tr>
<td><strong>Retype Password</strong></td>
<td>If <strong>XAUTH Client</strong> is enabled, this is the password used for authentication.</td>
</tr>
</tbody>
</table>
Performance Monitoring

The SLB supports Performance Monitoring probes for analyzing network performance. Probes for DNS Lookup, HTTP Get, ICMP Echo, TCP Connect, UDP Jitter and UDP Jitter VoIP are supported. Up to 15 different probes can be configured. Each probe will run a series of operations, each of which sends a series of packets to a destination host. The SLB will measure how long it took to receive a response, and record the results. For each operation, the user can view the results for each packet (round trip times), or the accumulated statistics for all packets - minimum, average and maximum latency, and for jitter probes, minimum, average, maximum and standard deviation of the jitter delay. Dropped packets and other error conditions are recorded for each operation. This capability allows an administrator to analyze network efficiency across the network.

An operation consists of sending a specified number of packets to a destination host and optional port, with a specified amount of time between each packet. All results for each operation are stored in one data file, and the results can be viewed later.

Repository and Operations Kept: The SLB can be configured to store probe results on the local SLB storage or an external USB thumb drive. The number of operations that can be stored per probe on the local SLB storage is 50 operations; for external USB thumb drive, 200 operations can be stored per probe.

Responders: The SLB can act as a responder for probes that require a responder to answer packets that are sent from the SLB (UDP jitter, UDP jitter VoIP, UDP Echo and TCP Connect). The SLB UDP jitter responder can support packet responses for up to 15 UDP jitter or UDP jitter VoIP probes. The UDP Echo and TCP Connect can support packets responses for one UDP Echo or TCP Connect probe.

Jitter Probes and Clock Skew: For jitter probes, it is important to have both the sender and responder synchronized to a reliable NTP server. Significant clock skew can greatly affect jitter results, as timestamps are recorded in the sender probe and the responder, and these timestamps are used to measure one-way latency for the packets. At the start of each jitter operation, the clock skew between the sender and the responder will be output to the system log.

Compatibility with Cisco Responders: The SLB Performance Monitor sender is compatible with Cisco IP SLA responders (IOS versions 12.2 and 15.0) for jitter probes. The SLB uses a simplified version of the IP SLA v2 (Engine II) protocol to communicate with the Cisco IP SLA responders. This compatibility gives the administrator a large number of devices with which to measure network performance.
To manage or view status for a Performance Monitoring probe:

1. Click the **Network** tab and select the **Perf Monitoring** option. The following page displays.

![Network > Perf Monitoring](image)

2. In the upper section of the page, modify the global Performance Monitoring settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of operations kept for each probe</td>
<td>Specifies the number of operation set files to keep for each probe. The limit for Local storage is 50 sets. The limit for external USB is 200 sets. While a probe is running, the operation set files will be automatically culled to remove the oldest operation set files.</td>
</tr>
<tr>
<td>Repository for operations</td>
<td>The repository where the operation set files will be kept - <strong>Local</strong> storage, or a USB thumb drive inserted in the upper <strong>USB Port U1</strong>. The data is stored in individual directories under a directory called &quot;perfmon&quot;. Once probes have been run and operation set files have been generated, changing the repository will cause all of the existing files to be moved from the old repository directory to the new repository directory. It is recommended that the repository only be changed when probes are not actively running. If external storage is used for the repository, it is recommended that the external storage device not be removed from the SLB while probes are actively running.</td>
</tr>
<tr>
<td>UDP Jitter Responder</td>
<td>Starts the UDP Jitter responder to reply to UDP jitter or UDP jitter VoIP packets. The responder will listen on UDP port 1967 for control messages requesting to start individual responders on a specific UDP port. The SLB UDP jitter responder can support up to 15 UDP jitter senders.</td>
</tr>
<tr>
<td>UDP Echo Responder</td>
<td>Starts the UDP Echo responder on the port configured in <strong>UDP Port</strong> to reply to UDP echo packets. The SLB UDP Echo responder supports one UDP echo sender. When the UDP Echo responder is enabled, the SLB will verify that the responder UDP port is not being used by any other SLB processes, including port 1967 which is reserved for the UDP Jitter responder.</td>
</tr>
</tbody>
</table>
3. Click the **Apply** button.

4. In the lower section of the page, select a probe by clicking the radio button to the far right in the probe’s row. The options that are available for that probe will be ungreyed. Select one of the following options:

| Refresh          | Refreshes the information on the Performance Monitoring page.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Probe</td>
<td>Displays the <em>Performance Monitoring - Add/Edit Probe</em> web page to add a new probe.</td>
</tr>
<tr>
<td>Operations</td>
<td>Displays a list of completed operations for the selected probe and allows the user to view either raw packet results or accumulated statistics for any operation.</td>
</tr>
<tr>
<td>Latest Results</td>
<td>Displays the latest raw packet results for the selected probe.</td>
</tr>
<tr>
<td>Latest Accumulated</td>
<td>Displays the latest accumulated statistics for the selected probe.</td>
</tr>
<tr>
<td>State: Restart</td>
<td>Allows the state of a probe to be controlled: the user can Restart a completed or running probe. When a probe is added, it will automatically start running, depending on how the probe start time is configured. Once a probe has run all of its configured operations, it will be in the &quot;Complete&quot; state. If the SLB is rebooted, all probes will automatically be restarted.</td>
</tr>
<tr>
<td>Edit Probe</td>
<td>Displays the <em>Performance Monitoring - Add/Edit Probe</em> web page to edit the currently selected probe.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected probe, after a confirmation.</td>
</tr>
</tbody>
</table>

The table at the bottom of the page lists information about completed and running probes.

<table>
<thead>
<tr>
<th>Id</th>
<th>Unique identifier for the probe.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name assigned to the probe.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the probe: Complete if all operations have been run, or Running if there are still operations that need to be run.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The date and time that the first operation started.</td>
</tr>
<tr>
<td>Finish Time</td>
<td>The date time that the most recently completed operation finished.</td>
</tr>
<tr>
<td>Error</td>
<td>Any errors reported by the probe:</td>
</tr>
<tr>
<td></td>
<td>◆ NMT: the current repository is an external source, but the USB thumb drive is not mounted</td>
</tr>
<tr>
<td></td>
<td>◆ NDR: the repository directory for the probe does not exist</td>
</tr>
<tr>
<td></td>
<td>◆ OPF: failed to open an operation data file</td>
</tr>
<tr>
<td></td>
<td>◆ SCT: error initializing a socket</td>
</tr>
<tr>
<td></td>
<td>◆ CFG: error retrieving probe configuration</td>
</tr>
<tr>
<td></td>
<td>◆ EXP: probe start time has expired</td>
</tr>
<tr>
<td>Operations Comp/Total</td>
<td>The number of operations that have been completed and the total number of operations that will be run.</td>
</tr>
</tbody>
</table>
Performance Monitoring - Add/Edit Probe

The Performance Monitoring - Add/Edit Probe web page allows a user to add a new Performance Monitoring probe or edit an existing Performance Monitoring probe.

To add a new probe or edit an existing probe:

1. Click the **Network** tab and select the Perf Monitoring option. The **Network > Perf Monitoring** page displays.

2. To add a new probe, in the lower section of the page, select the **Add Probe** link. To edit an existing probe, select a probe by clicking the radio button to the right in the probe’s row, then select the **Edit Probe** button. In both cases, the following page displays.

![Performance Monitoring - Add/Edit Probe](image-url)
3. Modify the probe settings:

<table>
<thead>
<tr>
<th>Probe Type</th>
<th>Select from one of the available probe types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DNS Lookup</td>
<td>Performs a DNS lookup on the hostname specified in the Destination Host using the Name Server. By default port 53 is always used as the Destination Port.</td>
</tr>
<tr>
<td>• HTTP Get</td>
<td>Performs an HTTP Get to the home (root) of the web server at the Destination Host and Destination Port.</td>
</tr>
<tr>
<td>• ICMP Echo</td>
<td>Sends ICMP Echo (ping) packets to the Destination Host.</td>
</tr>
<tr>
<td>• TCP Connect</td>
<td>Performs a TCP Connection to the Destination Host and Destination Port.</td>
</tr>
<tr>
<td>• UDP Echo</td>
<td>Sends UDP Echo packets to the Destination Host and Destination Port.</td>
</tr>
<tr>
<td>• UDP Jitter</td>
<td>Sends UDP jitter packets using a simplified version of the Cisco IP SLA v2 (Engine II) protocol to the Destination Host and Destination Port.</td>
</tr>
<tr>
<td>• UDP Jitter VoIP</td>
<td>Sends UDP jitter packets configured to simulate Voice over IP network traffic (VoIP) using a simplified version of the Cisco IP SLA v2 (Engine II) protocol to the Destination Host and Destination Port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Probe name, up to 40 characters long. Valid characters are letters, numbers, dashes (-), periods and underscores (_).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Operations</td>
<td>Number of operations to perform for the probe. Probes can for a specific number of operations. The valid range is 1 - 1000, and the default is 100.</td>
</tr>
<tr>
<td>Frequency between Operations</td>
<td>Time between probe operations, in seconds. The valid range is 5 - 3600 seconds, and the default is 60 seconds.</td>
</tr>
<tr>
<td>Number of Packets</td>
<td>Number of packets to send for each probe. For DNS Lookup probes, this is the number of lookups to perform. For HTTP Get probes, this is the number of HTTP Gets to perform. For TCP Connect probes, this is the number of TCP connections to perform. The valid range is 1 - 1000 for the Local repository and 1 - 2000 for a USB. The default is 10 packets.</td>
</tr>
<tr>
<td>Interval between Packets</td>
<td>Interval between packets in milliseconds. The valid range is 10 - 5000 milliseconds, and the default is 500 milliseconds. For HTTP Get, DNS Lookup and TCP Connect probes, the timeout must be less than the interval due to a new socket being created and destroyed for each packet.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Schedule a time to start the probe: Now starts the probe immediately; At date/time will start the probe at the specified date and time in the future; After waiting will start the probe after waiting a period of time that is less than 24 hours. When the SLB is rebooted, the probe will start according to the Start Time settings: (a) immediately if it set to Now, (b) at a date and time in the future if it is set to At date/time and the date and time is in the future, (c) after waiting a period of time if it is set to After waiting.</td>
</tr>
<tr>
<td>Destination Host</td>
<td>The hostname or IP address to send packets to. For DNS Lookup probes this is the hostname to lookup.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The TCP or UDP port to send packets to. For ICMP probes, the port setting is not used. For DNS Lookup probes, the destination port is always port 53. Port 1967 is reserved for the UDP jitter responder. The valid range is 1 - 65535.</td>
</tr>
<tr>
<td>Precision</td>
<td>The precision to view results in - milliseconds (the default) or microseconds. Jitter results are always displayed in milliseconds.</td>
</tr>
</tbody>
</table>
4. Click the **Apply** button.

**Performance Monitoring - Results**

The Performance Monitoring - Operations page displays all of the operations that have been saved for a selected probe. The probe ID and name are shown at the top of the web page. From this page, the user may select any operation to view its round trip time (RTT) results, or the accumulated statistics for all round trip times in an operation.

An operation consists of sending a specified number of packets to a destination host and optional port, with a specified amount of time between each packet. All results for each operation are stored in one data file.
### Round Trip Times

The results for each packet in an operation can be displayed with the **RTT Results** link. Each packet will be displayed with the packet start time and any error that resulted from sending the packet. For non-jitter probes, the total round trip time is displayed in either milliseconds or microseconds, depending on how the probe's precision setting:

**Probe 6/icmp-probe, operation icmp_170627_235709.dat:**

<table>
<thead>
<tr>
<th>Pkt</th>
<th>Time</th>
<th>RT Time</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17-06-27 23:57:09.171</td>
<td>0.419 ms</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>17-06-27 23:57:09.211</td>
<td>0.378 ms</td>
<td>OK</td>
</tr>
<tr>
<td>3</td>
<td>17-06-27 23:57:09.251</td>
<td>0.366 ms</td>
<td>OK</td>
</tr>
<tr>
<td>4</td>
<td>17-06-27 23:57:09.291</td>
<td>0.354 ms</td>
<td>OK</td>
</tr>
<tr>
<td>5</td>
<td>17-06-27 23:57:09.332</td>
<td>0.448 ms</td>
<td>OK</td>
</tr>
<tr>
<td>6</td>
<td>17-06-27 23:57:09.372</td>
<td>0.382 ms</td>
<td>OK</td>
</tr>
<tr>
<td>7</td>
<td>17-06-27 23:57:09.412</td>
<td>0.308 ms</td>
<td>OK</td>
</tr>
<tr>
<td>8</td>
<td>17-06-27 23:57:09.452</td>
<td>0.334 ms</td>
<td>OK</td>
</tr>
<tr>
<td>9</td>
<td>17-06-27 23:57:09.492</td>
<td>0.365 ms</td>
<td>OK</td>
</tr>
<tr>
<td>10</td>
<td>17-06-27 23:57:09.532</td>
<td>0.361 ms</td>
<td>OK</td>
</tr>
</tbody>
</table>

For jitter probes, the source to destination and destination times are displayed in the probe’s configured precision:

**Probe 7/udp-jitter-probe, operation udpjitter_170628_002049.dat:**

<table>
<thead>
<tr>
<th>Pkt</th>
<th>Time</th>
<th>Src To Dst Time</th>
<th>Dst To Src Time</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17-06-28 00:20:49.621</td>
<td>31029 usec</td>
<td>44191 usec</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>17-06-28 00:20:49.717</td>
<td>35409 usec</td>
<td>44170 usec</td>
<td>OK</td>
</tr>
<tr>
<td>3</td>
<td>17-06-28 00:20:49.808</td>
<td>35558 usec</td>
<td>34120 usec</td>
<td>OK</td>
</tr>
<tr>
<td>4</td>
<td>17-06-28 00:20:49.898</td>
<td>25500 usec</td>
<td>34175 usec</td>
<td>OK</td>
</tr>
<tr>
<td>5</td>
<td>17-06-28 00:20:49.988</td>
<td>35210 usec</td>
<td>34196 usec</td>
<td>OK</td>
</tr>
<tr>
<td>6</td>
<td>17-06-28 00:20:50.079</td>
<td>25517 usec</td>
<td>34177 usec</td>
<td>OK</td>
</tr>
<tr>
<td>7</td>
<td>17-06-28 00:20:50.169</td>
<td>35210 usec</td>
<td>54166 usec</td>
<td>Late Arrival</td>
</tr>
<tr>
<td>8</td>
<td>17-06-28 00:20:50.259</td>
<td>25549 usec</td>
<td>34170 usec</td>
<td>OK</td>
</tr>
<tr>
<td>9</td>
<td>17-06-28 00:20:50.350</td>
<td>25313 usec</td>
<td>34255 usec</td>
<td>OK</td>
</tr>
<tr>
<td>10</td>
<td>17-06-28 00:20:50.440</td>
<td>24848 usec</td>
<td>34351 usec</td>
<td>OK</td>
</tr>
</tbody>
</table>

### Accumulated Statistics

A summary of all round trip time and any error conditions is displayed. The display will vary for non-jitter and jitter results. For example, non-jitter accumulated results will show:

**Probe 6/icmp-probe, operation icmp_170627_235709.dat:**

- **Operation Type:**
  - ICMP Echo to 10.0.1.162, Ethernet Port: both
  - 30 packets sent 40 ms apart, timeout 1000 ms
- **Operation Start Time:** 17-06-27 23:57:09.171
- **Last Packet RTT:** 0.340 msec
- **Round Trip Time Results:**
  - Number of RTT: 30
  - RTT Min/Avg/Max: 0.306/0.362/0.448 msec
  - Number of Successes: 30
  - Number of Errors: 0
  - Lost Packet: 0 (0%)
  - Out of Sequence: 0
  - Late Arrival: 0
  - Miscellaneous Error: 0
For jitter probes, positive (increasing latency) and negative (decreasing latency) statistics are shown, as well as the number of positive or negative jitter samples in each direction, and the sum and (and sum squared) of the positive or negative jitter times. These numbers give a summary of how much variation there was in latency times and if the variation was small or large.

Probe 7/udp-jitter-probe, operation udpjitter_170628_002049.dat:

Operation Type:
  UDP Jitter to 10.0.1.93:50505
  50 packets sent 60 ms apart, timeout 1000 msec

Operation Start Time: 17-06-28 00:20:49.071
Last Packet RTT: 69.334 msec
Round Trip Time Results:
  Number of RTT: 50
  RTT Min/Avg/Max: 57.327/63.863/89.376 msec

One-way Latency Results:
  Number of samples: 50
  Source to Destination Min/Avg/Max: 23.174/27.467/45.206 msec
  Destination to Source Min/Avg/Max: 34.068/36.396/54.166 msec

Jitter, Source to Destination:
  Number of Samples: 49
  Positive and Negative Min/Avg/Max: 1/4/20 msec
  Positive Min/Avg/Max: 1/7/20 msec
  Positive Number Of/Sum of All/Sum of All Squared: 13/100/1090 msec
  Negative Min/Avg/Max: 1/5/20 msec
  Negative Number Of/Sum of All/Sum of All Squared: 17/96/1018 msec

Jitter, Destination to Source:
  Number of Samples: 49
  Positive and Negative Min/Avg/Max: 10/3/20 msec
  Positive Min/Avg/Max: 10/12/20 msec
  Positive Number Of/Sum of All/Sum of All Squared: 7/90/1300 msec
  Negative Min/Avg/Max: 10/12/20 msec
  Negative Number Of/Sum of All/Sum of All Squared: 8/100/1400 msec

Number of Successes: 49
Number of Errors: 1
  Lost Packet: 0 (0%)
  Out of Sequence: 0
  Late Arrival: 1
  Miscellaneous Error: 0

<table>
<thead>
<tr>
<th>Table 6-9 Error Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following error conditions are detected by the probes. Except where noted, the RTT results for a packet with errors will not be counted in the accumulated statistics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeout</strong></td>
<td>A response was never received for the packet. These packets are listed as Lost Packets under the accumulated statistics.</td>
</tr>
<tr>
<td><strong>Late Arrival</strong></td>
<td>A response was received for a packet, but the response was received after the timeout configured for the probe. The SLB will wait at most 2 times the probe's timeout for late arrival packets. The RTT results will be included in the accumulated statistics.</td>
</tr>
</tbody>
</table>
To view results for a Performance Monitoring probe:

1. Click the **Network** tab and select the **Perf Monitoring** option. The **Network > Perf Monitoring** page displays.

2. Select a probe from the table in the lower part of the page and select the **Operations** link. The **Performance Monitoring - Operations** page displays.

3. A table will list all available operations for the selected probe, with the most recent operation listed first. The table may be empty if no operations have been run for the probe or the operations for the probe have been deleted. Select an operation by clicking the radio button to...
the far right in the operation’s row. The options that are available for that operation will be ungreyed. Select one of the following options:

<table>
<thead>
<tr>
<th>Refresh</th>
<th>Refreshes the information on the Performance Monitoring - Operations page.</th>
</tr>
</thead>
</table>
| RTT Results | Displays the round trip time (RTT) results for the selected operation in a separate window. The results show:
  - The time that the packet was sent,
  - The total round trip time for non-jitter probes or the source to destination time and destination to source time for jitter probes, and
  - The status for the packet - OK/successful or an error condition.
  For more information, see *Round Trip Times* or *Error Conditions*). |
| Accumulated Results | Displays the accumulated statistics for the selected operation in a separate window. The results show parameters used for the selected operation, and the minimum, average and maximum round trip times for all probes. For jitter probes, the results show minimum, average and maximum one way latency times, as well as jitter results for source to destination and destination to source. For all probes, a summary of lost packets and error conditions is displayed. |

**Performance Monitoring Commands**

Go to *Performance Monitoring Commands (on page 326)* to view CLI commands which correspond to the web page entries described above.
7: Services

System Logging and Other Services

Use the Services > SSH/Telnet/Logging page to:

- Configure the amount of data sent to the logs.
- Enable or disable SSH and Telnet logins.
- Enable a Simple Network Management Protocol (SNMP) agent.

*Note:* The SLB branch office manager supports both MIB-II (as defined by RFC 1213) and a private enterprise MIB. The private enterprise MIB provides read-only access to all statistics and configurable items provided by the SLB unit. It provides read-write access to a select set of functions for controlling the SLB unit and device ports. See the MIB definition file for details.

- Identify a Simple Mail Transfer Protocol (SMTP) server.
- Enable or disable SSH and Telnet logins.
- Configure an audit log.
- View the status of and manage the SLB units on the secure Lantronix network.
- Set the date and time.
SSH/Telnet/Logging

To configure SSH, Telnet, and Logging settings:

1. Click the **Services** tab and select the **SSH/Telnet/Logging** option. The following page displays.

![Figure 7-1 Services > SSH/Telnet/Logging](image)

2. Enter the following settings:

**System Logging**

<table>
<thead>
<tr>
<th>Alert Levels</th>
<th>Select one of the following alert levels from the drop-down list for each message category:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Disables this type of logging.</td>
</tr>
<tr>
<td>Error</td>
<td>Saves messages that are output because of an error.</td>
</tr>
<tr>
<td>Warning</td>
<td>Saves message output from a condition that may be cause for concern, in addition to error messages. This is the default for all message types.</td>
</tr>
<tr>
<td>Info</td>
<td>Saves informative message, in addition to warning and error messages.</td>
</tr>
<tr>
<td>Debug</td>
<td>Saves extraneous detail that may be helpful in tracking down a problem, in addition to information, warning, and error messages.</td>
</tr>
</tbody>
</table>
### Network Level
Messages concerning the network activity, for example about Ethernet and routing.

### Services
Messages concerning services such as SNMP and SMTP.

### Authentication
Messages concerning user authentication.

### Device Ports
Messages concerning device ports and connections.

### Diagnostics
Messages concerning system status and problems.

### General
Any message not in the categories above.

### Remote Servers (#1 and #2)
IP address of the remote server(s) where system logs are stored.
The system log is always saved to local SLB storage. It is retained through SLB branch office manager reboots for files up to 200K. Saving the system log to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete system log history.

### Audit Log

<table>
<thead>
<tr>
<th>Enable Log</th>
<th>Select to save a history of all configuration changes in a circular log. Disabled by default. The audit log is saved through SLB reboots.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>The log has a default maximum size of 50 Kbytes (approximately 500 entries). You can set the maximum size of the log from 1 to 500 Kbytes.</td>
</tr>
<tr>
<td>Include CLI Commands</td>
<td>Select to cause the audit log to include the CLI commands that have been executed. Disabled by default.</td>
</tr>
<tr>
<td>Include In System Log</td>
<td>If enabled, the contents of the audit log are added to the system log (under the General/Info category/level). Disabled by default.</td>
</tr>
</tbody>
</table>

### SMTP

<table>
<thead>
<tr>
<th>Server</th>
<th>IP address of your network’s Simple Mail Transfer Protocol (SMTP) relay server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>The email address of the sender of outgoing emails. The strings &quot;$host&quot; and &quot;$domain&quot; can be part of the email address - they will be substituted with the actual hostname and domain. The default is donotreply@$host.$domain.</td>
</tr>
</tbody>
</table>

### SSH

<table>
<thead>
<tr>
<th>Enable Logins</th>
<th>Enables or disables SSH logins to the SLB branch office manager to allow users to access the CLI using SSH. Enabled by default. This setting does not control SSH access to individual device ports. (See Device Ports - Settings (on page 117) for information on enabling SSH access to individual ports.) Most system administrators enable SSH logins, which is the preferred method of accessing the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web SSH</td>
<td>Enables or disables the ability to access the SLB command line interface or device ports (connect direct) through the Web SSH window. Disabled by default.</td>
</tr>
<tr>
<td>Timeout</td>
<td>If you enable SSH logins, you can cause an idle connection to disconnect after a specified number of minutes. Select Yes and enter a value of from 1 to 30 minutes. Note: You must reboot the unit before a change will take effect.</td>
</tr>
<tr>
<td>SSH Port</td>
<td>Allows you to change the SSH login port to a different value in the range of 1 - 65535. The default is 22. Note: You must reboot the unit before a change will take effect.</td>
</tr>
</tbody>
</table>
### 7: Services

<table>
<thead>
<tr>
<th>DSA Keys</th>
<th>Enables or disables support for DSA keys for incoming and outgoing connections for the SLB unit. Any imported or exported DSA keys will be retained but will not be visible on the web or the CLI. Enabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use only SHA2 and Higher</td>
<td>Enables or disables support for only SHA2 and higher ciphers for incoming connections for the SLC unit. Disabled by default. Enabling this option will also disable MACs with tag sizes lower than 128 bits (e.g. <a href="mailto:umac-64-etm@openssh.com">umac-64-etm@openssh.com</a> and <a href="mailto:umac-64@openssh.com">umac-64@openssh.com</a>).</td>
</tr>
</tbody>
</table>

#### Telnet

<table>
<thead>
<tr>
<th>Enable Logins</th>
<th>Enables or disables Telnet logins to the SLB branch office manager to allow users to access the CLI using Telnet. Disabled by default. This setting does not control Telnet access to individual device ports. (See Device Ports - Settings (on page 117) for information on enabling Telnet access to individual ports.) You may want to keep this option disabled for security reasons.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Telnet</td>
<td>Enables or disables the ability to access the SLB command line interface or device ports (connect direct) through the Web Telnet window. Disabled by default.</td>
</tr>
<tr>
<td>Timeout</td>
<td>If you enable Telnet logins, you can cause an idle connection to disconnect after a specified number of minutes. Select Yes and enter a value of from 1 to 30 minutes. Note: You must reboot the unit before a change will take effect.</td>
</tr>
<tr>
<td>Escape Sequence</td>
<td>A single character or a two-character sequence that causes the SLB unit to terminate a Telnet client. Currently the Escape Sequence is only used for Web Telnet sessions. The default value is Esc+T (escape key, then uppercase “T” performed quickly but not simultaneously). You would specify this value as ‘\x1bT’, which is hexadecimal (\x) character 27 (1B) followed by a T. A control character can be specified with the hexadecimal number for the control character; for example, Control-E can be specified as ‘\x05’. Note that some browsers do not report key press events if Control is pressed for non-alphanumeric keys, so it is recommended to only use letters with Control character sequences.</td>
</tr>
<tr>
<td>Outgoing Telnet</td>
<td>Enables or disables the ability to create Telnet out connections.</td>
</tr>
</tbody>
</table>

#### Web SSH/Web Telnet Settings

| Terminal Buffer Size | Number of lines in the Web SSH or Web Telnet terminal window that are available for scrolling back through output. |

#### Phone Home

<table>
<thead>
<tr>
<th>Enable</th>
<th>If enabled, allows SLB branch office manager to directly contact a vSLM management appliance and request addition to the database</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the vSLM management appliance.</td>
</tr>
<tr>
<td>Last Attempt (view only)</td>
<td>Displays the date and time of last connection attempt.</td>
</tr>
<tr>
<td>Results (view only)</td>
<td>Indicates whether the attempt was successful.</td>
</tr>
</tbody>
</table>

3. To save, click the **Apply** button.
SNMP

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks.

1. Click the Services tab and select the SNMP option. The following page displays:

![Figure 7-2 Services > SNMP](image-url)
2. Enter the following:

<table>
<thead>
<tr>
<th>Enable Agent</th>
<th>Enables or disables SNMP agent, which allows read-only access to the system. Disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Traps</td>
<td>Traps are notifications of certain critical events. Disabled by default. This feature is applicable when SNMP is enabled. Traps that the SLB unit sends include:</td>
</tr>
<tr>
<td></td>
<td>- coldStart (generic trap 0, OID 1.3.6.1.6.3.1.1.5.1)</td>
</tr>
<tr>
<td></td>
<td>- linkDown (generic trap 2, OID 1.3.6.1.6.3.1.1.5.3)</td>
</tr>
<tr>
<td></td>
<td>- linkUp (generic trap 3, OID 1.3.6.1.6.3.1.1.5.4)</td>
</tr>
<tr>
<td></td>
<td>- authenticationFailure (generic trap 4, OID 1.3.6.1.6.3.1.1.5.5)</td>
</tr>
<tr>
<td></td>
<td>- slbEventPowerSupply (1.3.6.1.4.1.244.1.12.0.1)</td>
</tr>
<tr>
<td></td>
<td>- slbEventSysadminPassword (1.3.6.1.4.1.244.1.12.0.2)</td>
</tr>
<tr>
<td></td>
<td>- slbEventSLBShutdown (1.3.6.1.4.1.244.1.12.0.3)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortData (1.3.6.1.4.1.244.1.12.0.4)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortSLMData (1.3.6.1.4.1.244.1.12.0.5)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortSLMConfig (1.3.6.1.4.1.244.1.12.0.6)</td>
</tr>
<tr>
<td></td>
<td>- slbEventOverCurrentAlarm (1.3.6.1.4.1.244.1.12.0.7)</td>
</tr>
<tr>
<td></td>
<td>- slbEventPowerOutletStateChange (1.3.6.1.4.1.244.1.12.0.8)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortDeviceLowTemp (1.3.6.1.4.1.244.1.12.0.9)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortDeviceHighTemp (1.3.6.1.4.1.244.1.12.0.10)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortDeviceLowHumidity (1.3.6.1.4.1.244.1.12.0.11)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortDeviceHighHumidity (1.3.6.1.4.1.244.1.12.0.12)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortDeviceError (1.3.6.1.4.1.244.1.12.0.13)</td>
</tr>
<tr>
<td></td>
<td>- slbEventInternalTemp (1.3.6.1.4.1.244.1.12.0.15)</td>
</tr>
<tr>
<td></td>
<td>- slbEventUSBAction (1.3.6.1.4.1.244.1.12.0.16)</td>
</tr>
<tr>
<td></td>
<td>- slbEventDevicePortError (1.3.6.1.4.1.244.1.12.0.17)</td>
</tr>
<tr>
<td></td>
<td>- slbEventNoDialToneAlarm (1.3.6.1.4.1.244.1.12.0.18)</td>
</tr>
<tr>
<td></td>
<td>- slbEventNetworkFailover (1.3.6.1.4.1.244.1.12.0.23)</td>
</tr>
<tr>
<td></td>
<td>The SLB unit sends the traps to the host identified in the NMS #1 and NMS #2 field.</td>
</tr>
<tr>
<td>NMS #1 (or #2)</td>
<td>When SNMP is enabled, an NMS (Network Management System) acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP. The NMS can request information from the SLB unit and receive traps from the SLB unit. Enter the IP address of the NMS server. Required if you selected Enable Traps.</td>
</tr>
<tr>
<td>Location</td>
<td>Physical location of the SLB branch office manager (optional). Useful for managing the SLB unit using SNMP. Up to 20 characters.</td>
</tr>
<tr>
<td>Contact</td>
<td>Description of the person responsible for maintaining the SLB, for example, a name (optional). Up to 20 characters.</td>
</tr>
</tbody>
</table>

### Communities

<table>
<thead>
<tr>
<th>Read-Only</th>
<th>A string that acts like a password for an SNMP manager to access the read-only data the SLB unit the SNMP agent provides. The Read-Only Community is used for SNMP v1 and v2c. The default is public.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-Write</td>
<td>A string that acts like a password for an SNMP manager to access the read-only data the SLB SNMP agent provides and to modify data where permitted. The Read-Write Community is used for SNMP v1 and v2c. The default is private.</td>
</tr>
<tr>
<td>Trap</td>
<td>The trap used for outgoing generic and enterprise traps. Traps sent with the Event trigger mechanism still use the trap community specified with the Event Action. The default is public.</td>
</tr>
<tr>
<td>Enable v1</td>
<td>If checked, SNMP version 1 (which uses the Read-Only and Read-Write Communities) is enabled. The default is disabled.</td>
</tr>
</tbody>
</table>

---

**SLB™ Branch Office Manager User Guide**  
92
Enable v2c | If checked, SNMP version 2c (which uses the Read-Only and Read-Write Communities) is enabled. The default is enabled.

Alarm Delay | Number of seconds delay between outgoing SNMP traps.

### Version 3

**Security** | Levels of security available with SNMP v3.
- **No Auth/No Encrypt**: No authentication or encryption.
- **Auth/No Encrypt**: Authentication but no encryption. (default)
- **Auth/Encrypt**: Authentication and encryption.

**Auth with** | For **Auth/No Encrypt** or **Auth/Encrypt**, the authentication method:
- **MD5**: Message-Digest algorithm 5 (default)
- **SHA**: Secure Hash Algorithm

**Encrypt with** | Encryption standard to use:
- **DES**: Data Encryption Standard (default)
- **AES**: Advanced Encryption Standard

### V3 Read-Only User

**User Name** | SNMP v3 is secure and requires user-based authorization to access SLB MIB objects. Enter a user ID. The default is `snmpuser`. Up to 20 characters.

**Password/Retype**

**Password** | Password for a user with read-only authority to use to access SNMP v3. The default is `SNMPPASS`. Up to 20 characters.

**Passphrase/Retype**

**Passphrase** | Passphrase associated with the password for a user with read-only authority. Up to 20 characters. If this is not specified it will default to the V3 Password.

### V3 Read-Write User

**User Name** | SNMP v3 is secure and requires user-based authorization to access SLB MIB objects. Enter a user ID for users with read-write authority. The default is `snmprwuser`. Up to 20 characters.

**Password/Retype**

**Password** | Password for the user with read-write authority to use to access SNMP v3. The default is `SNMPRWPASS`. Up to 20 characters.

**Passphrase/Retype**

**Passphrase** | Passphrase associated with the password for a user with read-write authority. Up to 20 characters.

3. To save, click the **Apply** button.

### SNMP, SSH, Telnet, and Logging Commands

Go to *Services Commands (on page 335)* and *Logging Commands (on page 317)* to view CLI commands which correspond to the web page entries described above.
NFS and SMB/CIFS

Use the Services > NFS/CIFS page if you want to save configuration and logging data onto a remote NFS server, or export configuration by means of an exported CIFS share.

Mounting an NFS shared directory on a remote network server onto a local SLB directory enables the SLB branch office manager to store device port logging data on that network server. This configuration avoids possible limitations in the amount of disk space on the SLB unit available for the logging file(s). You may also save SLB configurations on the network server.

Similarly, use SMB/CIFS (Server Message Block/Common Internet File System), Microsoft’s file-sharing protocol, to export a directory on the SLB branch office manager as an SMB/CIFS share. The SLB exports a single read-write CIFS share called “public,” with the subdirectory The config directory, which contains saved configurations and is read-write.

The share allows users to access the contents of the directory or map the directory onto a Windows computer.

To configure NFS and SMB/CIFS:

1. Click the Services tab and select the NFS/CIFS option. The following page displays:

   Figure 7-3  Services > NFS/CIFS

   NFS & SMB/CIFS

   The SLB can be configured to share a directory containing the system logs to a Microsoft Windows network. This directory can also be used for saving SLB configurations via Firmware & Configurations.
2. Enter the following for up to three directories:

### NFS Mounts

<table>
<thead>
<tr>
<th>Remote Directory</th>
<th>The remote NFS share directory in the format: <code>nfs_server_hostname</code> or <code>ipaddr:/exported/path</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Directory</td>
<td>The local directory on the SLB unit on which to mount the remote directory. The SLB unit creates the local directory automatically.</td>
</tr>
<tr>
<td>Read-Write</td>
<td>If enabled, indicates that the SLB unit can write files to the remote directory. If you plan to log port data or save configurations to this directory, you must enable this option.</td>
</tr>
<tr>
<td>Mount</td>
<td>Select the checkbox to enable the SLB branch office manager to mount the file to the NFS server. Disabled by default.</td>
</tr>
</tbody>
</table>

3. Enter the following:

### SMB/CIFS Share

<table>
<thead>
<tr>
<th>Share SMB/CIFS directory</th>
<th>Select the checkbox to enable the SLB unit to export an SMB/CIFS share called “public.” Disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Interfaces</td>
<td>Select the network ports from which the share can be seen. The default is for the share to be visible on both network ports.</td>
</tr>
<tr>
<td>CIFS User Password/Retype Password</td>
<td>Only one user special username (cifsuser) can access the CIFS share. Enter the CIFS user password in both password fields. The default user password is <code>CIFSPASS</code>. More than one user can access the share with the <code>cifsuser</code> user name and password at the same time.</td>
</tr>
<tr>
<td>Workgroup</td>
<td>The Windows workgroup to which the SLB branch office manager belongs. Every PC exporting a CIFS share must belong to a workgroup. Can have up to 15 characters.</td>
</tr>
</tbody>
</table>

4. To save, click the **Apply** button.

### NFS and SMB/CIFS Commands

Go to [NFS and SMB/CIFS Commands on page 324](#) to view CLI commands which correspond to the web page entries described above.

## Secure Lantronix Network

Use the **Secure Lantronix Network** option to view and manage Lantronix console servers, branch office managers and Spider devices on the local subnet.

*Note:* Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, reload the web page by clicking the **Refresh** link.

### To access secure Lantronix managers and Spider devices on the local network:

1. Click the **Services** tab and select the **Secure Lantronix Network** option. The following page displays with an entry for each device discovered on the network. If Web SSH is enabled, device ports that have SSH In enabled are shown in a bright green. Settings that control the behavior of Web SSH and Web Telnet are on the **SSH/Telnet/Logging**
web page. For tips on troubleshooting browser issues, see *Troubleshooting Browser Issues*. For tips on Web SSH or Web Telnet copy and paste functionality, see *Web SSH/Telnet Copy and Paste*.

**Figure 7-4 Services > Secure Lantronix Network**

![Secure Lantronix Network](image)

2. Access your device or device port through any of the methods below.

**To directly access the web interface for a secure Lantronix device:**

1. Make sure Web Telnet and Web SSH is enabled for the specific device or device port.
2. Click the IP address of a specific secure Lantronix device to open a new browser page with the web interface for the selected secure Lantronix device.
3. Log in as usual.
To directly access the CLI interface for a device:

1. Make sure Web Telnet and/or Web SSH is enabled for the specific device or device port you wish to access.

2. Click the **SSH** or **Telnet** link in the SSH/Telnet to CLI column directly beside the port you would like to access.
   - If **Web SSH** and **SSH to the CLI** are enabled, an SSH link will display and be accessible beside the specific port(s). Clicking this link will open a new Web SSH session.
   - If **Web Telnet** and **Telnet to the CLI** are enabled, a Telnet link will display and be accessible beside the specific port(s). Clicking this link will open a new Web Telnet session.
   - If neither Web Telnet and/or Web SSH are enabled, "N/A" will display beside the ports.

The Web SSH or Web Telnet session appears. See *Figure 7-6* below.
To directly access a specific port on a particular device:

1. Click a port number in a green square beside the specific device.

   a. Enabled port numbers are in a bright green box and will allow you to select either a WebSSH or a WebTelnet session. If enabled, an SSH or Telnet popup window appears depending on what is clicked. See Figure 7-6.

   b. Disabled port numbers are in a dark green box and you will see a popup:

   ![Figure 7-7 Disabled Port Number Popup Window](image)

2. Click OK and login to the CLI interface which appears. See Figure 7-6.

To configure how secure Lantronix devices are searched for on the network:

1. Click the Search Options link on the top right of the Services > Secure Lantronix Network page. The following web page displays:
2. Enter the following:

<table>
<thead>
<tr>
<th>Secure Lantronix Network Search</th>
<th>Select the type of search you want to conduct.</th>
</tr>
</thead>
<tbody>
<tr>
<td>◆ Local Subnet</td>
<td>◆ Local Subnet performs a broadcast to detect secure Lantronix devices on the local subnet.</td>
</tr>
<tr>
<td>◆ Manually Entered IP Address List</td>
<td>◆ Manually Entered IP Address List provides a list of IP addresses that may not respond to a broadcast because of how the network is configured.</td>
</tr>
<tr>
<td>◆ Both</td>
<td>◆ Both is the default selection.</td>
</tr>
</tbody>
</table>

| IP Address | If you selected Manually Entered IP Address List or Both, enter the IP address of the secure Lantronix device you want to find and manage. |

3. If you entered an IP address, click the Add IP Address button. The IP address displays in the IP Address List.

4. Repeat steps 2 and 3 for each IP address you want to add.

5. To delete an IP address from the IP Address List, select the address and click the Delete IP Address button.

6. Click the Apply button. When the confirmation message displays, click Secure Lantronix Network on the main menu. The Services > Secure Lantronix Network page displays the secure Lantronix devices resulting from the search. You can now manage these devices.

**Troubleshooting Browser Issues**

Depending on which browser you are using and what type of SSL certificate the SLB web server is configured with, there may be errors connecting to a Web SSH or Web Telnet session. These errors may be the standard browser error displayed for self-signed or untrusted certificates (“There is a problem with this website’s security certificate,” or “Your connection is not private.”).

The SSL server that handles Web SSH and Web Telnet sessions is accessible on port 8000, instead of the standard port 443 for SSL connections. It is recommended that the SLB be configured to use a SSL certificate from a Certificate Authority to prevent issues accessing Web SSH and Web Telnet terminals. If your SLB web server is configured to use a self-signed or
untrusted SSL certificate, refer to the notes below for how to work around this for various browsers.

When an SLB is configured with a SSL certificate that is either a wildcard certificate or associated with a specific name, in order to establish a Web SSH or Web Telnet session to the SLB unit, the unit must be able to successfully perform a reverse lookup on any IP address to which Web SSH or Web Telnet requests are sent. For example, if a unit is configured with a SSL certificate for the name "slbXYZ.lantronix.com", and the unit website is being accessed in a browser with "https://slbXYZ.lantronix.com", the unit needs to be configured with a name server that will allow the unit to perform a reverse lookup on the IP address associated with slbXYZ.lantronix.com. Failure to perform a reverse lookup on a name may result in name mismatch errors in the browser when it attempts to open the Web SSH or Web Telnet window.

If you are unable to connect to a Web SSH or Web Telnet session for a reason other than a browser SSL certificate issue, restarting the SSL server on port 8000 may resolve the connection problem. This can be done by restarting the web server (with the CLI command "admin web restart") or by disabling both Web SSH and Web Telnet on the SSH/Telnet/Logging web page, and then re-enabling them.

- **Chrome** - For the greatest ease of use with Web SSH and Web Telnet, when the SLB web server is using a self-signed SSL certificate, use the Chrome browser. When the user accepts the self-signed SSL certificate in the browser for the primary SLB website, the self-signed SSL certificate is accepted for all ports - including port 8000 - for the SLB website.

- **Firefox** - When accessing the SLB website with Firefox, and when the SLB web server is using a self-signed SSL certificate, accepting the self-signed SSL certificate in the browser for the primary SLB website will only accept the certificate for port 443. It will not accept the certificate for port 8000. This may result in a popup being displayed in the Web SSH or Web Telnet window indicating that the browser needs to accept a certificate. To accept the self-signed certificate for port 8000, go to Firefox -> Options (or Preferences) -> Advanced -> Certificates -> View Certificates -> Servers, and add an exception for the SLB IP address or hostname, with port 8000.

- **Internet Explorer** - When accessing the SLB website with Internet Explorer, and when the SLB web server is using a self-signed SSL certificate, Explorer will grant access to the Web SSH and Web Telnet terminals if (a) the host name or common name in the self-signed certificate matches the name (or IP address) being used to access the SLB website, and (b) Explorer has imported and trusted the self-signed certificate. A custom self-signed certificate with the SLB name can be generated via the Services - SSL Certificate web page or the admin web certificate custom CLI command.

Once the SLB web server has been configured to use the custom self-signed certificate, follow these steps for Internet Explorer to trust the custom certificate:

- In Internet Explorer, browse to the SLB website whose certificate you want to trust.
- When the message "There is a problem with this website's security certificate.", choose Continue to this website (not recommended).
- In Internet Explorer, select Tools -> Internet Options.
- Select Security -> Trusted Sites -> Sites.
- Verify or fill in the SLB website URL in the Add this website field, click Add, and then Close.
- Close the Internet Options dialog with either OK or Cancel.
- Refresh the Internet Explorer web page with the SLB website.
- When the message "There is a problem with this website's security certificate", choose Continue to this website (not recommended).
- Click on the red **Certificate Error** at the right of the URL address bar and select **View certificates**.
- In the dialog that displays, click on **Install Certificate**, then in the **Certificate Import Wizard**, click **Next**.
- On the next page select **Place all certificates in the following store**.
- Click **Browse**, select **Trusted Root Certification Authorities**, and click **OK**.
- Back in the **Certificate Import Wizard**, click **Next**, then **Finish**.
- If you get a **Security Warning** message box, click **Yes**.
- Dismiss the **Import was successful** message box with **OK**.
- In Internet Explorer, select **Tools -> Internet Options**.
- Select **Security -> Trusted Sites -> Sites**.
- Select the SLB website URL you just added, click **Remove**, then **Close**.
- Now shut down all running instances of Internet Explorer, and start up Internet Explorer again.
- The SLB website's certificate should now be trusted.

**Web SSH/Telnet Copy and Paste**

There are security issues with letting a web page access the system clipboard, which is the main clipboard on a system that is shared between all applications. Because of this, browsers limit access to the system clipboard. The Web SSH and Web Telnet window provide copy and paste functionality via a right-click menu: the Copy option will copy what is highlighted in the Web SSH or Web Telnet window into an internal (non-system) clipboard, and the contents can be pasted into the Web SSH or Web Telnet window with the Paste.

Support for copying and pasting content between the system clipboard and the Web SSH or Web Telnet window will vary from browser to browser. With the exception of Internet Explorer, most browsers will not allow highlighted content from the Web SSH or Web Telnet window to be copied to the system clipboard (Internet Explorer will display a prompt confirming the copy). Likewise, most browsers will not allow content from the system clipboard to be directly pasted into the Web SSH or Web Telnet window with the standard Control-V paste key sequence. With some browsers, the user will be able to use the Paste from browser option in the right-click menu to paste content from the system clipboard into a text field in a popup, and after hitting Enter, the content will be sent to the Web SSH or Web Telnet window.

**Secure Lantronix Network Commands**

Go to *Secure Lantronix Network Commands (on page 338)* to view CLI commands which correspond to the web page entries described above.
Date and Time

You can specify the current date, time, and time zone at the SLB's location (default), or the SLB branch office manager can use NTP to synchronize with other NTP devices on your network.

To set the local date, time, and time zone:

1. Click the Services tab and select the Date & Time option. The following page displays:

   ![Figure 7-9 Services > Date & Time]

   - **Change Date/Time**: Select the checkbox to manually enter the date and time at the SLB’s location.
   - **Date**: From the drop-down lists, select the current month, day, and year.
   - **Time**: From the drop-down lists, select the current hour and minute.
   - **Time Zone**: From the drop-down list, select the appropriate time zone.

2. Enter the following:

<table>
<thead>
<tr>
<th>Change Date/Time</th>
<th>Select the checkbox to manually enter the date and time at the SLB’s location.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date</strong></td>
<td>From the drop-down lists, select the current month, day, and year.</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>From the drop-down lists, select the current hour and minute.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>From the drop-down list, select the appropriate time zone.</td>
</tr>
</tbody>
</table>

3. To save, click the Apply button.
To synchronize the SLB unit with a remote timeserver using NTP:

1. Enter the following:

<table>
<thead>
<tr>
<th>Enable NTP</th>
<th>Select the checkbox to enable NTP synchronization. NTP is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize via</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>★ Broadcast from NTP Server: Enables the SLB branch office manager to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP.</td>
</tr>
<tr>
<td></td>
<td>★ Poll NTP Server: Enables the SLB unit to query the NTP Server for the correct time. If you select this option, complete one of the following:</td>
</tr>
<tr>
<td></td>
<td>&gt; Local: Select this option if the NTP servers are on a local network, and enter the IP address of up to three NTP servers. This is the default, and it is highly recommended.</td>
</tr>
<tr>
<td></td>
<td>&gt; Public: Select this option if you want to use a public NTP server, and select the address of the NTP server from the drop-down list. This is not recommended because of the high load on many public NTP servers. All servers in the drop-down list are stratum-2 servers. (See <a href="http://www.ntp.org">www.ntp.org</a> for more information.) Each public NTP server has its own usage rules --please refer to the appropriate web site before using one. Our listing them here is to provide easy configuration but does not indicate any permission for use.</td>
</tr>
</tbody>
</table>

2. To save, click the Apply button.

Date and Time Commands

Go to Date and Time Commands (on page 303) to view CLI commands which correspond to the web page entries described above.

Web Server

The Web Server supports all versions of the TLS protocol, but due to security concerns, does not support any versions of the SSL protocol. The Web Server page allows the system administrator to:

★ Configure attributes of the web server.
★ View and terminate current web sessions.
★ Import a site-specific SSL certificate.
★ Enable an iGoogle gadget that displays the status of ports on multiple SLBs.

To configure the Web Server:

1. Click the Services tab and select the Web Server option. The following page appears:
2. Enter the following fields:

| **Timeout** | Select **No** to disable Timeout.  
Select **Yes** to enable timeout. Enter the number of minutes (must be between 5 and 120 minutes) after which the SLB web session times out. The default is 5.  
*Note:* If a session times out, refresh the browser page and login to a new web session. If you close the browser without logging off the SLB unit first, you will have to wait for the timeout time to expire. You can also end a web session by using the admin web terminate command at the CLI or by asking your system administrator to terminate your active web session.  
➢ To view or terminate current web sessions, click the **Web Sessions** link.  
➢ To view, import, or reset the SSL Certificate, click the **SSL Certificate** link. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable TLS v1.0 Protocol</strong></td>
<td>By default, the web supports the TLS v1.0 protocol. Uncheck this to disable the TLS v1.0 protocol. Changing this option requires a reboot or restarting the web server with the CLI command &quot;admin web restart&quot; for the change to take effect.</td>
</tr>
<tr>
<td><strong>Enable TLS v1.1 Protocol</strong></td>
<td>By default, the web supports the TLS v1.1 protocol. Uncheck this to disable the TLS v1.1 protocol. Changing this option requires a reboot or restarting the web server with the CLI command &quot;admin web restart&quot; for the change to take effect.</td>
</tr>
<tr>
<td><strong>Cipher</strong></td>
<td>Click one of the radio buttons to configure the web to support low security (less than 128 bits) or High/Medium security (128 bits or higher) for the cipher. By default, the web uses High/Medium. Changing this option requires a reboot for the change to take effect.</td>
</tr>
</tbody>
</table>
### Use only SHA2 and Higher Ciphers
By default, the web supports SHA1 as well as SHA2 and higher ciphers. Check this option to support only SHA2 and higher ciphers. Changing this option requires a reboot or restarting the web server with the CLI command "admin web restart" for the change to take effect.

### Group Access
If undefined, any group can access the web. If one or more groups are specified (groups are delimited by the characters ',' (comma) or ';' (semicolon)), then any user who logs into the web must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the SLB branch office manager. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ',' (comma), ';' (semicolon), or '=' (equals) - for example "group=group1,group2;" or "group1,group2,group3;".

### Banner
The text to display on the web manager home page after the user logs in. May contain up to 1024 characters (single quote and double quote characters are not supported). Blank by default.

**Note:** To create additional lines in the banner use the \n character sequence.

### Network Interfaces
The interfaces that the web server is available on. By default, Eth1, Eth2 and PPP interfaces on modems are enabled.

### Run Web Server
If enabled, the web server will run and listen on TCP ports 80 and 443 (all requests to port 80 are redirected to port 443). By default, the web server is enabled.

### Web Sessions
Click the Web Sessions link to view or terminate a web session. ([See Services - Web Sessions on page 105](#)).

### SSL Certificate
Click the SSL Certificate link to view, import or reset the SSL Certificate. ([See Services - SSL Certificate on page 106](#)).

3. Click the **Apply** button to save.

**Administrative Commands**

Go to Administrative Commands (on page 267) to view CLI commands which correspond to the web page entries described above.

**Services - Web Sessions**

The Services > Web Server page enables you to view and terminate current web sessions.

**To view or terminate current web sessions:**

1. On the Services tab, click the Web Server page and click the Web Sessions link to the right. The following page displays:
2. To terminate, select the check box for the session and click **Terminate**.

3. To return to the **Services > Web Server** page, click the **Back to Web Server** link.

### Services - SSL Certificate

The **Services > Web Server** page enables you to view and update SSL certificate information. The SSL certificate, consisting of a public/private key pair used to encrypt HTTP data, is associated with the web server. You can import a site-specific SSL certificate or generate a custom certificate, if desired.

**To view, reset, import, or change an SSL Certificate:**

1. On the **Services** tab, click the **Web Server** page and click the **SSL Certificate** link. The following page displays the current SSL certificate.
2. If desired, enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reset to Default Certificate</strong></td>
<td>To reset to the default certificate, select the checkbox to reset to the default certificate. Unselected by default.</td>
</tr>
<tr>
<td><strong>Import SSL Certificate</strong></td>
<td>To import your own SSL Certificate, select the checkbox. Unselected by default.</td>
</tr>
<tr>
<td><strong>Import via</strong></td>
<td>From the drop-down list, select the method of importing the certificate (SCP or SFTP). The default is SCP.</td>
</tr>
<tr>
<td><strong>Certificate Filename</strong></td>
<td>Filename of the certificate. If HTTPS is selected as the method for import, the Upload File link will be selectable to upload a certificate file.</td>
</tr>
<tr>
<td><strong>Key Filename</strong></td>
<td>Filename of the private key for the certificate. HTTPS is selected as the method for import, the Upload File link will be selectable to upload a key file.</td>
</tr>
</tbody>
</table>
3. Click the **Apply** button.

**Note:** You must reboot the SLB branch office manager for the update to take effect.

4. To return to the Services > Web Server page, click the **Back to Web Server** link.

### SSL Certificate Commands

Go to Administrative Commands (on page 267) to view CLI commands which correspond to the web page entries described above.
ConsoleFlow

ConsoleFlow is a cloud or on-premise portal for the centralized management of multiple Lantronix Out-of-band management devices, including and SLC 8000 and SLB devices. A browser based interface (including mobile phone app support) allows an administrator to view status, send commands, view logs and charts and update firmware for an SLC 8000 or SLB. Each device can communicate with the cloud server or on-premise server, sending status updates, responding to commands sent by the server.

An SLB device requires a unique Device ID to communicate with the ConsoleFlow portal. The ID is viewable in the ConsoleFlow settings. If a device is not already pre-configured with the ID, the ID must be provisioned using Lantronix Provisioning Manager (LPM).

Changing the console manager timezone or making significant changes to the current date and time may cause issues with the ConsoleFlow client's ability to connect to or send updates to the ConsoleFlow server; restarting the client will resolve these issues.

The ConsoleFlow client follows a sequence of steps to connect to the cloud or on-premise ConsoleFlow server, send status updates, check for firmware and configuration updates, and respond to commands from the server. This series of steps is the same each time the client starts - at SLB boot, or if the client is enabled. Any changes to the ConsoleFlow Device ID, Registration settings or Messaging settings require the ConsoleFlow client to be disabled and re-enabled for the changes to take effect.

1. **Registration**

   The client will attempt to register to the **Registration Host** using the Project Tag and Device ID. If registration fails, the client will wait 30 seconds to 16 minutes and retry. The client will retry until it is successful, or the client is disabled. Registration may fail if the Project Tag is invalid, the Device ID is invalid, the Registration Host name cannot be resolved, or the Registration Host is not reachable. Once registration is successful, **Status of Client** will display Registered with the date and time of registration.

   **Note:** The Registered date/time displayed in the SLB status may be different from the registered date/time shown in the ConsoleFlow web UI. The SLB registered date/time is the most recent date and time that the SLB registered with the ConsoleFlow server. The registered date and time shown in the ConsoleFlow web UI is the first time that the SLB ever registered with the ConsoleFlow server.

2. **Telemetry**

   After registration, the client will connect to the Telemetry Host (the hostname is provided during registration) and perform a telemetry handshake. This handshake may request that the client publish a set of statistics at regular intervals. If a telemetry handshake is successful, **Status of Client** will display Telemetry Handshake with the date and time of the handshake. Each time telemetry statistics are published, **Status of Client** will display Telemetry Statistics with the date and time the statistics were sent.

3. **Messages and Status Updates**

   After the telemetry handshake, the client will connect to the **Messaging Host** to receive messages and publish status updates. If the connection fails, the client will wait 5 seconds and retry. The connection may fail if the Messaging Host name cannot be resolved, or the Messaging Host is not reachable. Once the connection is successful, **Status of Client** will display Messaging connected with the date and time the connection was established.

   The client publishes status update messages (changes to device attributes) at the interval defined by **Interval between Status Updates**. Each time a status update is published, **Status of Client** will display Status with the date and time the status was sent. The client also
accepts command messages from the ConsoleFlow server to perform actions, such as reboot or shutdown. Each time a message is received, **Status of Client** will display **Message received** with the date and time the message was received.

### 4. Firmware and Configuration Updates

The client checks for firmware and configuration updates at the interval defined by **Interval between FW and Config Checks**. When the client checks for firmware or configuration updates, **Status of Client** will display **Checked for Content** with the date and time the check was performed. If a firmware update is found, it will be applied to the alternate (non-active) boot bank, and **Status of Client** will display **Firmware updated** with the date and time the firmware was updated. If a configuration update is found, it will be applied to the current boot bank, and **Status of Client** will display **Configuration restored** with the date and time the configuration was restored.

### 5. Web Terminal Connections

ConsoleFlow allows users to make secure, encrypted connections via SSL/TLS to the CLI and device ports. This connection opens a web terminal session in a new browser tab in the ConsoleFlow UI. The connection is terminated when the user closes the web terminal session. When a Web Terminal connection is initiated, **Status of Client** will display **Web Terminal Connection** with the date and time the connection was initiated. Web Terminal connections are also displayed in the Connections list in the SLB web UI and CLI. Currently paste in Web Terminal Sessions is limited to 500 lines. Some browsers may not support pasting more than 500 lines, as this may cause the Web Terminal session to be terminated.

### 6. Performance Monitoring Probes and Custom Scripts

ConsoleFlow allows users to create Performance Monitoring Probes and Custom Scripts to run on the SLB. When the client starts, it will request all probes and scripts that are defined to run on the SLB. The status of the probes and scripts is displayed in the **Status of Client**. When a script run completes (either for a single manual run or a recurring scheduled run), the status of the script will be retained on the SLB until a new script is initiated from ConsoleFlow and the SLB determines that the maximum number of ConsoleFlow scripts per SLB has been reached; at this time the oldest completed script will be deleted to accommodate the new script.

**Note:** If a script is initiated from ConsoleFlow to run on multiple ports on the SLB, each script/port combination is a separate script "instance", and is counted separately in the total number of scripts running on the SLB.

### 7. Device Port Connection Status Digital Probes

The primary method for determining the ConsoleFlow Device Port Connection Status is by reading the DSR status for the device port. For serial devices that do not set DSR, a digital probe can be enabled which will periodically send a newline (\n) character to the device, and the SLB will verify if a response is received from the device within approximately one second. If a response is received, the Device Port will be set to Connected; if no response is received, the Device Port status will be set to Disconnected. This feature is disabled by default for all device ports, and can be enabled for individual device ports via the CLI (the frequency that the newline character is sent can be configured). Digital probes that are enabled will only run while the ConsoleFlow client is running. If a digital probe is enabled for a device that has set DSR, the digital probe will still run, but the results from the digital probe will be ignored when determining the Device Port Connection Status.

**Note:**
- The digital probe is an intrusive feature and can affect actions on the Device Port, depending on what is happening on the Device Port or what users are connected to the
Device Port when the newline character is sent:

- Device Ports may not generate a response to the newline character within approximately one second, and this may result in the Device Port Connection Status being set to Disconnected.

8. CLI Commands

CLI commands can be issued to a set of console managers from ConsoleFlow. CLI commands which require user input for a confirmation or prompt, or require some other user interaction ('connect direct' or diag commands) are not supported. Abbreviated commands are also not supported (e.g., "show network all" is supported, but "sh ne all" is not supported).

To configure ConsoleFlow settings:

1. Click the Services tab and select the ConsoleFlow option. The following page displays.

Figure 7-13  Services > ConsoleFlow
2. Enter the following:

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ConsoleFlow Client</strong></td>
<td>Enables or disables the ConsoleFlow client. This option is enabled by default, unless an SLB is not configured with a Device ID. When the client is enabled, it will attempt to register with the Registration Host. If this is successful, the client will attempt to establish a connection with the Messaging Host. The General log (see SSH/Telnet/Logging on page 88) will contain messages about connections made to the Registration Host and Messaging Host. Status of Client displays the last time of actions performed by the client. Note that when the client is disabled, it may take as long as 30 seconds for the client to terminate, depending on what actions the client was performing at the time it was disabled.</td>
</tr>
<tr>
<td><strong>Interval between status updates</strong></td>
<td>Number of minutes between status updates sent from the client to the server. Valid values are 1 - 60 minutes. The default is 2 minutes.</td>
</tr>
<tr>
<td><strong>Interval between FW and Config Checks</strong></td>
<td>Number of hours between checks for firmware and configuration updates initiated by the server. Valid values are 1 - 72 hours. The default is 24 hours.</td>
</tr>
<tr>
<td><strong>Firmware Updates via ConsoleFlow</strong></td>
<td>If enabled, firmware updates can be initiated by ConsoleFlow for the SLB. The device will check for updates per the frequency defined by Interval between FW and Config Checks, and if a firmware update is found, the update will be downloaded to the device and applied to the alternate boot bank. Enabled by default.</td>
</tr>
<tr>
<td><strong>Configuration Updates via ConsoleFlow</strong></td>
<td>If enabled, configuration updates can be initiated by ConsoleFlow for the SLB. The device will check for updates per the frequency defined by Interval between FW and Config Checks, and if a configuration update is found, the update will be downloaded to the device and applied to the current boot bank, and the SLB will be immediately rebooted. Enabled by default.</td>
</tr>
<tr>
<td><strong>Reboot after Firmware Update</strong></td>
<td>If enabled, the SLB will automatically reboot after a successful firmware update via ConsoleFlow. Disabled by default.</td>
</tr>
<tr>
<td><strong>Audit Log Messages</strong></td>
<td>If enabled, audit log entries added to the Audit Log on the console manager are pushed to ConsoleFlow for viewing. Enabled by default.</td>
</tr>
<tr>
<td><strong>Connect to</strong></td>
<td>Allows you to choose Cloud or On-Premise server settings for the ConsoleFlow client. By default, Cloud is selected.</td>
</tr>
</tbody>
</table>

**Update Log**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear Update Log</strong></td>
<td>Clears the Firmware/Config updates log.</td>
</tr>
</tbody>
</table>

**Device Attributes**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Name</strong></td>
<td>The device name displayed in the ConsoleFlow server UI. Valid characters are alphanumeric characters, dash &quot;-&quot;, and underscore &quot;_&quot;. The default is the device type (SLB) with the last 4 characters of the Eth1 MAC address appended.</td>
</tr>
<tr>
<td><strong>Device Description</strong></td>
<td>Long description that is displayed in the ConsoleFlow server UI.</td>
</tr>
<tr>
<td><strong>Device ID</strong></td>
<td>The unique device identifier. The ID is 32 alphanumeric characters. The ID may be provisioned using Lantronix Provisioning Manager (LPM). Contact Lantronix Tech Support for more information on LPM.</td>
</tr>
<tr>
<td><strong>S/N</strong></td>
<td>Displays the serial number.</td>
</tr>
</tbody>
</table>
### Registration Host

<table>
<thead>
<tr>
<th><strong>Registration Host</strong></th>
<th>Hostname of the server the client registers with. The Host Name should start with api.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration Port</strong></td>
<td>The TCP port on the Registration Host. Defaults to 443.</td>
</tr>
<tr>
<td><strong>Use HTTPS for registration</strong></td>
<td>If enabled, HTTPS (instead of HTTP) is used for registration. Enabled by default.</td>
</tr>
<tr>
<td><strong>Validate certificates with HTTPS</strong></td>
<td>If enabled, use a certificate authority to validate the HTTPS certificate. A certificate authority file can be uploaded on the Web Server page. Disabled by default.</td>
</tr>
</tbody>
</table>

### Messaging Host

| **Messaging Services** | If enabled, messaging services are used for status updates and commands. Enabled by default. |

### Remote Access Idle Timeout

<table>
<thead>
<tr>
<th><strong>Remote Access CLI Timeout</strong></th>
<th>Remote Access CLI Connection will be idle timed out after a specified number of seconds as defined in the Seconds field to the right. Enter a value from 1 to 1800 seconds. The default is 600 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Access Device Port Timeout</strong></td>
<td>Remote Access Device Port Connection will be idle timed out after a specified number of seconds as defined in the Seconds field to the right. Enter a value from 1 to 1800 seconds. The default is 600 seconds.</td>
</tr>
</tbody>
</table>

3. To save, click **Apply**.

### ConsoleFlow Commands

Go to *ConsoleFlow Commands (on page 298)* to view CLI commands which correspond to the web page entries described above.
8: Device Ports

This chapter describes how to configure and use an SLB device port connected to an external device, such as a server or a modem. The next chapter, Chapter 10: Connections, describes how to use the Devices > Connections web page to connect external devices and outbound network connections (such as Telnet or SSH) in various configurations. The Devices > Console Port page allows you to configure the console port, if desired.

Connection Methods

A user can connect to a device port in one of the following ways:

1. Telnet or SSH to the Eth1 or Eth2 IP address, or connect to the console port, and log in to the command line interface. At the command line interface, issue the connect direct or connect listen commands.

2. If Telnet is enabled for a device port, Telnet to <Eth1 IP address>:<telnet port number> or <Eth2 IP address>:<telnet port number>, where telnet port number is uniquely assigned for each device port.

3. If SSH is enabled for a device port, SSH to <Eth1 IP address>:<ssh port number> or <Eth2 IP address>:<ssh port number>, where ssh port number is uniquely assigned for each device port.

4. If TCP is enabled for a device port, establish a raw TCP connection to <Eth1 IP address>:<tcp port number> or <Eth2 IP address>:<tcp port number>, where tcp port number is uniquely assigned for each device port.

5. If a device port has an IP address assigned to it, you can Telnet, SSH, or establish a raw TCP connection to <Eth1 IP address>:<tcp port number> or <Eth2 IP address>:<tcp port number>, where tcp port number is uniquely assigned for each device port.

6. Connect a terminal or a terminal emulation program directly to the device port. If logins are enabled, the user is prompted for a username and password and logs in to the command line interface.

   For #2, #3, #4, #5, and #6, if logins or authentication are not enabled, the user is directly connected to the device port with no authentication.

   For #1 and #6, if logins are enabled, the user is authenticated first, and then logged into the command line interface. The user login determines permissions for accessing device ports.

Permissions

There are three types of permissions:

1. Direct (or data) mode: The user can interact with and monitor the device port (connect direct command).

2. Listen mode: The user can only monitor the device port (connect listen command).

3. Clear mode: The user can clear the contents of the device port buffer (set locallog <port> clear buffer command).
The administrator and users with local user rights may assign individual port permissions to local users. The administrator and users with remote authentication rights assign port access to users authenticated by NIS, RADIUS, LDAP, Kerberos and TACACS+.

### Device Status

The **Devices > Device Status** page displays the status of the SLB’s ports, USB port and power outlets.

1. **Click the Devices tab and select the Device Status option. The following page displays:**

   ![Devices > Device Status](image)

   **Device Status**

   **Device Port Status and Counters**

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>DSR</th>
<th>Bytes Input/Output</th>
<th>Errors</th>
<th>Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Port-1</td>
<td>Yes</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>2</td>
<td>Port-2</td>
<td>Yes</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>3</td>
<td>Port-3</td>
<td>Yes</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>4</td>
<td>Port-4</td>
<td>Yes</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>5</td>
<td>Port-5</td>
<td>Yes</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>6</td>
<td>Port-6</td>
<td>Yes</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>7</td>
<td>Port-7</td>
<td>No</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>8</td>
<td>Port-8</td>
<td>No</td>
<td>0.0</td>
<td>0</td>
<td>Idle</td>
</tr>
</tbody>
</table>

**USB Ports**

- **Port U1**: Manufacturer = U.S. Robotics, Product = USB Modem, Serial Number = 00000003, State = Inserted
- **Port U2**: Manufacturer = Internal, State = N/A

**Power Outlets**

- **Outlet P1**: Name = PowerOutlet-1, State = Off
- **Outlet P2**: Name = PowerOutlet-2, State = Off
- **Outlet P3**: Name = PowerOutlet-3, State = Off
- **Outlet P4**: Name = PowerOutlet-4, State = Off
- **Outlet P5**: Name = PowerOutlet-5, State = Off
- **Outlet P6**: Name = PowerOutlet-6, State = Off
- **Outlet P7**: Name = PowerOutlet-7, State = Off
- **Outlet P8**: Name = PowerOutlet-8, State = Off

### Global Port Settings

On the **Devices > Device Ports** page, you can set up the numbering of Telnet, SSH, and TCP ports, view a summary of current port modes, establish the maximum number of direct connections for each device port, and select individual ports to configure.

1. **Click the Devices tab and select the Device Ports option. The following page displays:**

   ![Global Port Settings](image)
Current port numbering schemes for Telnet, SSH, and TCP ports display on the left. The list of ports 1-8 on the right includes the individual ports and their current mode.

**Note:** For units with more ports, click the buttons above the table to view additional ports.

Icons that represent some of the possible modes include:

- **Idle**
  - The port is not in use.

- **Data/Text**
  - The port is in data/text mode.
  - **Note:** You may set up ports to allow Telnet access using the IP Setting per Device Ports - Settings (on page 117).

- **Modem**
  - An external modem is connected to the port. The user may dial into or out of the port.

- **Telnet in or SSH in**
  - Telnet in or SSH in is enabled for the device port. The device port is either waiting for a Telnet or SSH login or has received a Telnet or SSH login (a user has logged in).

**To set up Telnet, SSH, and TCP port numbering:**

1. Enter the following:

**Telnet/SSH/TCP in Port Numbers**

<table>
<thead>
<tr>
<th>Starting Telnet Port</th>
<th>Each port is assigned a number for connecting via Telnet. Enter a number (1025-65528) that represents the first port. The default is 2000 plus the port number. For example, if you enter 2001, subsequent ports are automatically assigned numbers 2002, 2003, and so on.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting SSH Port</td>
<td>Each port is assigned a number for connecting via SSH. Enter a number (1025-65528) that represents the first port. The default is 3000 plus the port number. For example, if you enter 3001, subsequent ports are automatically assigned numbers 3002, 3003, and so on.</td>
</tr>
</tbody>
</table>
Caution: Ports 1-1024 are RFC-assigned and may conflict with services running on the SLB. Avoid this range.

2. Click the Apply button to save the settings.

To set limits on direct connections:

1. Enter the maximum number (1-10) of simultaneous direct connections for each device port.
   The default is 1.
2. Click the Apply button to save the settings.

To configure a specific port:

1. You have two options:
   - Select the port from the ports list and click the Configure button. The Device Ports > Settings page for the port displays.
   - Click the port number on the green bar at the top of each page.
2. Continue with directions in the section, Device Ports - Settings (on page 117).

Global Commands

Go to Global Commands (on page 313) to view CLI commands which correspond to the web page entries described above.

Device Ports - Settings

On the Device Ports > Settings page, configure IP and data (serial) settings for individual ports, and if the port connects to an external modem, modem settings as well.

To open the Device Ports - Settings page:

1. You have two options:
   - In the Devices > Device Ports page (described in the previous section), select the port from the ports list and click the Configure button.
   - Click the desired port number in the green bar (Figure 8-3) at the top of any page, and the following page appears:
Figure 8-4  Device Ports > Settings

Device Ports - Settings

Logins:
Connected to: undefined

IP Settings:
- Telnet In: Port 2022, Authentication: on, Timeout: 600 seconds
- SSH In: Port 3032, Authentication: on, Timeout: 600 seconds
- TCP In: Port 4002, Authentication: on, Timeout: 600 seconds

Data Settings:
- Baud: 9600
- Data Bits: 8
- Stop Bits: 1
- Parity: none
- Flow Control: none
- Use Sites: [ ]
- Max Direct Connects: 5
- Show Lines On Connecting: [ ]

Modem Settings:
- Mode: Text, PPP
- Use Sites: [ ]
- Initialization Script:
- Modern Timeout: No, Yes, seconds (1-9999)
- Caller ID Logging: [ ]
- Dial-back Number: Local User Number
- Dial-back Delay: 15 seconds
- Dial-back Retries: 3

Text Mode:
- Timeout Logins: No, Yes, minutes (1-30)
- Dial-in Host List: undefined

PPP Mode:
- Negotiate IP Address: Yes
- Local IP: [ ]
- Remote IP: [ ]
- Authentication: PAP, CHAP
- CHAP Handshake: Host/User Name:
- Secret/User Password:
- CHAP Auth Uses: CHAP Host, Local Users
- Same authentication:
- Dial-in & Dial-out Authentication:
- PPP Mode: [ ]
- PPP Debug: [ ]

Enable NAT: [ ]
- Note: Enabling NAT requires IP Forwarding to be enabled.
- Dial-out Number:
- Remote/Dial-out Login:
- Remote/Dial-out Password: Retype:
- Restart Delay: 300 seconds
- CBIC Server:
- Allow No Callback: [ ]
- CBIC Client Type: [ ]

Port Status and Counters:
- DSR/CD: No
- DSR: Yes
- RTS: Yes
- Bytes input: 0
- Bytes output: 0
- Framing errors: 0
- Parity errors: 0
- Overrun errors: 0
- Flow Control errors: 0
- Seconds since zeroed: 20715

< Back to Device Ports
2. Enter the following:

**Device Port Settings**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays number of port; displays automatically.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>The status of the port; displays automatically.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the port. Valid characters are letters, numbers, dashes (-), periods, and underscores (_).</td>
</tr>
<tr>
<td>Group Access</td>
<td>If undefined, any group can access the device port. If one or more groups are specified (groups are delimited by the characters ' ' (space), ',' (comma), or ';' (semicolon)), then any user who logs into the device port must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the SLB. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ' ' (space), ',' (comma), ',' (semicolon), or '=' (equals) - for example &quot;group=group1,group2,&quot; or &quot;group1,group2,group3&quot;.</td>
</tr>
<tr>
<td>Banner</td>
<td>Text to display when a user connects to a device port by means of Connect Direct (CLI), Telnet, SSH, or TCP. If authentication is enabled for the device port, the banner displays once the user successfully logs in. May contain up to 1024 characters (single quote and double quote characters are not supported). Blank by default.</td>
</tr>
<tr>
<td>Break Sequence</td>
<td>A series of one to ten characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase &quot;B&quot; performed quickly but not simultaneously). You would specify this value as \x1bB, which is hexadecimal (\x) character 27 (1B) followed by a B.</td>
</tr>
<tr>
<td>View Port Log Seq</td>
<td>The key sequence used to view the Port Log while in Connect Direct mode. Non-printing characters can be specified by giving their hexidecimal code (see Break Sequence above). The default is Esc+V (\x1bV).</td>
</tr>
<tr>
<td>View Port Log</td>
<td>Select to allow the user to enter the View Port Log Sequence to view the Port Log during Connect Direct mode. The default is disabled.</td>
</tr>
<tr>
<td>Zero Port Counters</td>
<td>Resets all of the numerical values in the Port Counters table at the bottom of the page to zero (0).</td>
</tr>
<tr>
<td>Logging</td>
<td>Click the Settings link to configure file logging, email logging, and local logging.</td>
</tr>
<tr>
<td>Connected to</td>
<td>The type of device connected to the device port. Presently, the SLB branch office manager supports Lantronix SLP power managers (SLP8 and SLP16 units) and Sensorsoft devices. If the type of device is not listed, select undefined. If you select anything other than undefined, click Device Commands. The appropriate web page displays.</td>
</tr>
</tbody>
</table>

**IP Settings**

| Telnet In | Enables access to this port through Telnet. Disabled by default. |
| SSH In | Enables access to this port through SSH. Disabled by default. |
8: Device Ports

<table>
<thead>
<tr>
<th>TCP in</th>
<th>Enables access to this port through a raw TCP connection. Disabled by default:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note:</td>
<td>When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, set the Break Sequence of the respective device port to null (clear it).</td>
</tr>
</tbody>
</table>

| Port | Automatically assigned Telnet, SSH, and TCP port numbers. You may override this value, if desired. |

| Authentication | If selected, the SLB branch office manager requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet in** and **SSH in**, but not for **TCP in**. |

| Timeout | To cause an idle Telnet, SSH or TCP connection to disconnect after a specified number of seconds, select the checkbox and enter a value from 1 to 1800 seconds. The default is no timeout. |

| Seconds | Number of seconds before a timeout. |

| IP Address/Netmask Bits | IP address used for this device port so a user can Telnet, SSH, or establish a raw TCP connection to this address and connect directly to the device port. The optional netmask bits specify the netmask to use for the IP address. For example, for a netmask of 255.255.255.0 specify 24 bits. If the netmask bits are not specified, a default netmask used for the class of network that the IP address falls in will be used. |

For Telnet and SSH, the default TCP port numbers (22 and 23, respectively) are used to connect to the device port. For raw TCP, the TCP port number defined for **TCP In** to the device port is used. |

| Note: | If Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported. Note that the IP address will be bound to Eth1 only, so if Eth2 is connected and configured, and Eth1 is not, this feature will not work. |

| Baud | The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate. |

| Data Bits | Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is **8** data bits. |

| Stop Bits | The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is **1**. |

| Parity | Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is **none**. |

| Flow Control | A method of preventing buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is **none**. |

| Enable Logins | For serial devices connected to the device port, displays a login prompt and authenticates users. Successfully authenticated users are logged into the command line interface. The default is disabled. This is the correct setting if the device port is the endpoint for a network connection. |

Data Settings

**Note:** Check the serial device’s equipment settings and documentation for the proper settings. The device port and the attached serial device must have the same settings.
8: Device Ports

**Max Direct Connects**
Enter the maximum number (1-10) of simultaneous connections for the device port. The default is 1.

**Show Lines on Connecting**
If enabled, when the user either does a connect direct from the CLI or connects directly to the port using Telnet or SSH, the SLB outputs up to 24 lines of buffered data as soon as the serial port is connected.

For example, an SLB user issues a `connect direct device 1` command to connect port 1 to a Linux server.

Then the SLB user `ls` command to display a directory on the Linux server, then exits the connection. When the SLB user issues another `direct connect device 1`, the last 24 lines of the `ls` command is displayed so the user can see what state the server was left in.

**Hardware Signal Triggers**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check DSR on Connect</td>
<td>If this setting is enabled, the device port only establishes a connection if DSR (Data Set Ready) is in an asserted state. DSR should already be in an asserted state, not transitioning to, when a connection attempt is made. Disabled by default unless dial-in, dial-out, or dial-back is enabled for the device port.</td>
</tr>
<tr>
<td>Disconnect on DSR</td>
<td>If a connection to a device port is currently in session, and the DSR signal transitions to a de-asserted state, the connection disconnects immediately. Disabled is the default unless dial-in, dial-out, or dial-back is enabled for the device port.</td>
</tr>
</tbody>
</table>

**Modem Settings**

*Note: Depending on the State and Mode you select, different fields are available.*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Indicates whether an external modem is attached to the device port. If enabling, set the modem to dial-out, dial-in, dial-back, dial-on-demand, dial-in/host list, or dial in &amp; dial-on-demand. Disabled by default. For more information on the different dialing types, see Modem Dialing States.</td>
</tr>
<tr>
<td>Mode</td>
<td>The format in which the data flows back and forth:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Text</strong>: In this mode, the SLB branch office manager assumes that the modem will be used for remotely logging into the command line. Text mode can only be used for dialing in or dialing back. Text is the default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PPP</strong>: This mode establishes an IP-based link over the modem. PPP connections can be used in dial-out mode (e.g., the SLB unit connects to an external network), dial-in mode (e.g., the external computer connects to the network that the SLB unit is part of), dial-back (dial-in followed by dial-out), dial-on-demand, CBCP server or CBCP client.</td>
</tr>
<tr>
<td>Use Sites</td>
<td>Enables the use of site-oriented modem parameters which can be activated by various modem-related events (authentication, outbound network traffic for dial-on-demand connections, etc.). Sites can be used with the following modem states: dial-in, dial-back, dial-on-demand, dial-in &amp; dial-on-demand, dial-back &amp; dial-on-demand, and CBCP server. For more information, see Sites (on page 169).</td>
</tr>
</tbody>
</table>
Initialization Script

Commands sent to configure the modem may have up to 100 characters. Consult your modem’s documentation for recommended initialization options. If you do not specify an initialization script, the SLB branch office manager uses a default initialization string of

\[ \text{AT S7=45 SO=0 L1 V1 X4 &D2 &c1 E1 Q0} \]

*Note: We recommend that the modem initialization script always be preceded with \text{AT} and include \text{E1 V1 X4} so that the SLB unit may properly control the modem. For information on AT commands, refer to the modem user guide, or do a web search for at command set.*

Modem Timeout

Timeout for all modem connections. Select \text{Yes} (default) for the SLB branch office manager to terminate the connection if no traffic is received during the configured idle time. Enter a value of from 1 to 9999 seconds. The default is 30 seconds.

Caller ID Logging

Select to enable the SLB branch office manager to log caller IDs on incoming calls. Disabled by default.

*Note: For the Caller ID AT command, refer to the modem user guide.*

Modem Command

Modem AT command used to initiate caller ID logging by the modem.

*Note: For the AT command, refer to the modem user guide.*

Dial-back Number

Users with dial-back access can dial into the SLB unit and enter their login and password. Once the SLB authenticates them, the modem hangs up and dials them back.

Select the phone number the modem dials back on - a fixed number or a number associated with their login. If you select \text{Fixed Number}, enter the number (in the format 2123456789).

The dial-back number is also used for CBCP client as the number for a user-defined number. See \text{Device Ports - Settings (on page 117)} for more information.

Dial-back Delay

For dial-back and CBCP Server, the number of seconds between the dial-in and dial-out portions of the dialing sequence.

Dial-back Retries

For dial-back and CBCP Server, the number of times the SLB unit will retry the dial-out portion of the dialing sequence if the first attempt to dial-out fails.

**Modem Settings: Text Mode**

Timeout Logins

If you selected \text{Text} mode, you can enable logins to time out after the connection is inactive for a specified number of minutes. The default is \text{No}. This setting is only applicable for text mode connections. \text{PPP} mode connections stay connected until either side drops the connection. Disabled by default.

Dial-in Host List

From the drop-down list, select the desired host list. The host list is a prioritized list of SSH, Telnet, and TCP hosts that are available for establishing outgoing modem connections or for \text{connect direct} at the CLI. The hosts in the list are cycled through until the SLB branch office manager successfully connects to one. To establish and configure host lists, click the Host Lists link.

**Modem Settings: PPP Mode**

Negotiate IP Address

If the SLB unit and/or the serial device have dynamic IP addresses (e.g., IP addresses assigned by a DHCP server), select \text{Yes}. \text{Yes} is the default.

If the SLB unit or the modem have fixed IP addresses, select \text{No}, and enter the Local IP (IP address of the port) and Remote IP (IP address of the modem).
3. To save settings for just this port, click the Apply button.

4. To save selected settings to ports other than the one you are configuring:
   - From the Apply Settings drop-down box, select none, a group of settings, or All.
   - In to Device Ports, type the device port numbers, separated by commas; indicate a range of port numbers with a hyphen (e.g., 2, 5, 7-10).
Note: It may take a few minutes for the system to apply the settings to multiple ports.

Port Status and Counters

Port Counters describe the status of signals and interfaces. SLB branch office manager updates and increments the port counters as signals change and data flows in and out of the system. These counters help troubleshoot connections or diagnose problems because they give the user an overview of the state of various parameters. By setting them to zero and then re-checking them later, the user can view changes in status.

The chart in the middle of the page displays the flow control lines and port statistics for the device port. The system automatically updates these values. To reset them to zeros, select the Zero port counters checkbox in the IP Settings section of the page.

Note: Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, you must reload the web page.

<table>
<thead>
<tr>
<th>Port Status and Counters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR/CD</td>
<td>No</td>
</tr>
<tr>
<td>DTR</td>
<td>Yes</td>
</tr>
<tr>
<td>CTS</td>
<td>No</td>
</tr>
<tr>
<td>RTS</td>
<td>Yes</td>
</tr>
<tr>
<td>Bytes input</td>
<td>0</td>
</tr>
<tr>
<td>Bytes output</td>
<td>0</td>
</tr>
<tr>
<td>Framing errors</td>
<td>0</td>
</tr>
<tr>
<td>Parity errors</td>
<td>0</td>
</tr>
<tr>
<td>Overrun errors</td>
<td>0</td>
</tr>
<tr>
<td>Flow Control errors</td>
<td>0</td>
</tr>
<tr>
<td>Seconds since zeroed</td>
<td>105734</td>
</tr>
</tbody>
</table>

Device Ports - SLP Units

On the Device Ports > SLP page, configure commands to send to an SLP power manager or SLP expansion chassis that expands the number of power ports.

To open the Device Ports - SLP page:

1. In the Connected to field above the IP Settings section of the Device Port Settings page, select an SLP or SLP EXP.
2. Click the Device Commands link. The following page displays:
To enter SLP commands:

1. Enter the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Outlets</td>
<td>Enter the number of outlets for a ServerTech CDU. This setting is not applicable for an SLP unit.</td>
</tr>
<tr>
<td>Number of Expansion Outlets</td>
<td>Enter the number of outlets for a ServerTech CDU expansion unit. This setting is not applicable for an SLP device.</td>
</tr>
<tr>
<td>Login</td>
<td>User ID for logging into the SLP power manager.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter password for logging into the SLP unit.</td>
</tr>
<tr>
<td>Retype Password</td>
<td>Re-enter password for logging into the SLP power manager.</td>
</tr>
<tr>
<td>Prompt</td>
<td>Enter the prompt displayed by the SLP unit or ServerTech CDU device. This will default to a typical prompt for an SLP power manager or ServerTech CDU device. If you are unable to control the SLP unit or ServerTech CDU device, verify that the prompt is set to the right value.</td>
</tr>
</tbody>
</table>

**Status/Info**

- **Outlet Status**
  
  *Note: If there is an SLP power manager and an SLP Expansion chassis, the SLP unit is Tower A and the Expansion chassis is Tower B.*

  For **Tower A** or **Tower B**, select **All Outlets** or **Single Outlet** to view the status of all outlets or a single outlet of the SLP power manager. If you select **Single Outlet**, enter a value of 1-8 for the SLP8 or 1-16 for the SLP16 device.

  Click the **Outlet Status** link to see the status of the selected outlet(s).

- **Environmental Status**

  Click the link to view the environmental status (e.g., temperature and humidity) of the SLP power manager.
8: Device Ports

Device Port - Sensorsoft Device

Devices made by Sensorsoft are used to monitor environmental conditions.

1. In the Connected to field above the IP Settings section of the Device Port Settings page, select Sensorsoft.

2. Click the Device Commands link. The following page displays:

![Figure 8-7 Devices > Device Ports > Sensorsoft](image)

3. Select a port and enter or view the following information:

<table>
<thead>
<tr>
<th>Device Port Name</th>
<th>Temp</th>
<th>Low Temp</th>
<th>High Temp</th>
<th>Use °F</th>
<th>Humidity (%)</th>
<th>Low Humidity</th>
<th>High Humidity</th>
<th>Traps</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Port-5</td>
<td>0.0°C</td>
<td>0</td>
<td>25</td>
<td></td>
<td>0</td>
<td>0</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

- **Infeed Status**: Click the link to view the status of the data the SLP unit is receiving.
- **System Info**: Click the link to see system information pertaining to the SLP power manager.

### Commands

**Restart SLP**

To restart the SLP power manager, select the checkbox.

**Control Outlet**

For Tower A or Tower B, select All Outlets or Single Outlet and the number of the outlet to be controlled (1-8 for the SLP8 or 1-16 for the SLP16 devices) and select the command for the outlet (No Action, Power On, Power Off, Cycle Power). **No Action** is the default.

2. Click the Apply button.
4. Click the **Apply** button.

5. To view the status detected by the Sensorsoft, click the **Sensorsoft Status** link to the right of the table.

### Device Port Commands

Go to *Device Port Commands (on page 305)* to view CLI commands which correspond to the web page entries described above.

### Interacting with a Device Port

Once a device port has been configured and connected to an external device such as the console port of an external server, the data received over the device port can be monitored at the command line interface with the `connect listen` command, as follows:

**To connect to a device port to monitor it:**

```bash
connect listen deviceport <Port # or Name>
```

In addition, you can send data out the device port (for example, commands issued to an external server) with the `connect direct` command, as follows:

**To connect to a device port to monitor and/or interact with it, or to establish an outbound network connection:**

```bash
connect direct <endpoint>
```

*endpoint* is one of:

- `deviceport <Port # or Name>`
- `ssh <IP Address> [port <TCP Port>] [<SSH flags>]`
  
  where:

  - `<SSH flags>` is one or more of:
    - `user <Login Name>`
    - `version <1|2>`
    - `command <Command to Execute>`
    - `tcp <IP Address> port <TCP Port>`
    - `telnet <IP Address> [port <TCP Port>]`
    - `udp <IP Address> port <UDP Port>`
    - `hostlist <Host List>`

**Note:** To escape from the `connect direct` command when the endpoint of the command is `deviceport`, `tcp`, or `udp` and return to the command line interface, type the escape sequence assigned to the currently logged in user. If the endpoint is `telnet` or `SSH`, logging out returns the user to the command line prompt.
Note: To escape from the connect listen command, press any key. Setting up a user with an escape sequence is optional. For any NIS, LDAP, RADIUS, Kerberos, or TACACS+ user, or any local user who does not have an escape sequence defined, the default escape sequence is Esc+A.

Device Ports - Logging

The SLB products support port buffering of the data on the system's device ports as well as notification of receiving data on a device port. Port logging is disabled by default. You can enable more than one type of logging (local, NFS file, email/SNMP, or USB port) at a time. The buffer containing device port data is cleared when any type of logging is enabled.

Local Logging

If local logging is enabled, each device port stores 256 Kbytes (approximately 400 screens) of I/O data in a true FIFO buffer. You may view this data (in ASCII format) at the CLI with the show locallog command or on the Devices > Device Ports - Logging page. Buffered data is normally stored in RAM and is lost in the event of a power failure if it is not logged using an NFS mount solution. If the buffer data overflows the buffer capacity, only the oldest data is lost, and only in the amount of overrun (not in large blocks of memory).

NFS File Logging

Data can be logged to a file on a remote NFS server. Data logged locally to the SLB branch office manager is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a file on an NFS server does not have these limitations. The system administrator can define the directory for saving logged data on a port-by-port basis and configure file size and number of files per port.

The directory path must be the local directory for one of the NFS mounts. For each logging file, once the file size reaches the maximum, a new file opens for logging. Once the number of files reaches the maximum, the oldest file is overwritten. The file naming convention is: <Device Port Number>_ <Device Port Name>_<File number>.log.

Examples:

02_Port-2_1.log
02_Port-2_2.log
02_Port-2_3.log
02_Port-2_4.log
02_Port-2_5.log

USB Flash Drive Logging

Data can be logged to a USB flash drive that is loaded into the USB port on the front of the SLB branch office manager (see USB Port on page 178). Data logged locally to the SLB unit is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a USB flash drive does not have these limitations. The system administrator can define the file size and number of files per port. For each logging file, once the file size reaches the maximum, a new file opens for logging. Once the number of files reaches the maximum, the oldest file is overwritten. The file naming convention is: <Device Port Number>_<Device Port Name>_<File number>.log.
Examples:
02_Port-2_1.log
02_Port-2_2.log
02_Port-2_3.log
02_Port-2_4.log
02_Port-2_5.log

Email/SNMP Notification
The system administrator can configure the SLB branch office manager to send an email alert message indicating a particular condition detected in the device port log to the appropriate parties or an SNMP trap to the designated NMS (see Chapter 7: Services on page 87). The email or trap is triggered when a user-defined number of characters in the log from your server or device is exceeded, or a specific sequence of characters is received.

Use the Device Ports - SLP Units (on page 124) to set logging parameters on individual ports.

Sylogs Logging
Data can be logged to the system log. If this feature is enabled, the data will appear in the Device Ports log, under the Info level. The log level for the Device Ports log must be set to Info for the data to be saved to the system log. (See Chapter 7: Services on page 87.)

To set logging parameters:

1. In the top section of the Device Port Settings page, click the Settings link in the Logging field. The following page displays:
### Local Logging

2. Enter the following:

#### Local Logging

<table>
<thead>
<tr>
<th><strong>Local Logging</strong></th>
<th><strong>Clear Local Log</strong></th>
<th><strong>View Local Log</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>If you enable local logging, each device port stores 256 Kbytes (approximately 400 screens) of I/O data in a true FIFO buffer. Disabled by default.</td>
<td>Select the checkbox to clear the local log.</td>
<td>Click this link to see the local log in text format.</td>
</tr>
</tbody>
</table>

#### Email/SNMP Traps

<table>
<thead>
<tr>
<th><strong>Email/Traps</strong></th>
<th><strong>Email/SNMP Traps</strong></th>
<th><strong>Email/SNMP Traps</strong></th>
<th><strong>Email/SNMP Traps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the checkbox to enable email and SNMP logging. Email logging sends an email message to pre-defined email addresses or an SNMP trap to the designated NMS (see Chapter 7: Services on page 87) when alert criteria are met. Disabled by default.</td>
<td>For NFS File Logging, the directory to log to must reside on an external NFS server. Specify the local directory for the <strong>NFS mount</strong>.</td>
<td>Select the checkbox to enable email and SNMP logging. Email logging sends an email message to pre-defined email addresses or an SNMP trap to the designated NMS (see Chapter 7: Services on page 87) when alert criteria are met. Disabled by default.</td>
<td>Select the checkbox to enable email and SNMP logging. Email logging sends an email message to pre-defined email addresses or an SNMP trap to the designated NMS (see Chapter 7: Services on page 87) when alert criteria are met. Disabled by default.</td>
</tr>
</tbody>
</table>

### Diagram

**Figure 8-8 Devices > Device Ports - Logging**

- **Device Ports - Logging**

  - **Port 5**
  - **Name:** Port 6

  - **Local Logging:**
    - Clear Local Log: [ ]
    - View Local Log: [ ]

  - **Email/Traps:**
    - Send:
      - Email
      - SNMP Trap
      - Both
    - Trigger on:
      - Byte Count
      - Text String Recognition
    - Byte Threshold: 100
    - Test String: [ ]
    - Email Delay: 60 seconds
    - Restart Delay: 60 seconds
    - Email To: [ ]
    - Email Subject: Port 64d Logging

  - **Log Viewing Attributes**
    - Display: [ ] Tail [ ] Head
    - Number of Lines: 40

  - **NFS File Logging:**
    - NFS Log to View: [ ] Most Recent
    - Directory to Log to: [ ] select one
    - Max Number of Files: 10
    - Max Size of Files: 2048 bytes

  - **USB Logging:**
    - USB Log to View: [ ] Most Recent
    - Log to: [ ] Port U1
    - Max Number of Files: 10
    - Max Size of Files: 2048 bytes

  - **Syslog Logging:**
    - [ ]

  - **Note:** The logging level for the Device Ports log must be set to 'Info' to view Syslog entries for Device Port logging.

**Apply settings to Device Ports:** [ ]

**Note:** In addition to applying settings to the currently selected Device Port, the settings can also be applied to other Device Ports.
Device Ports

Send
If you enabled email and SNMP logging, select what type of notification log to send:
- Email (default)
- SNMP Trap
- Both

Trigger on
Select the method of triggering a notification:
- **Byte Count**: A specific number of bytes of data. This is the default.
- **Text String Recognition**: A specific pattern of characters, which you can define by a regular expression.

*Note: Text string recognition may negatively impact the SLB unit’s performance, particularly when regular expressions are used.*

Byte Threshold
The number of bytes of data the port receives before the SLB unit captures log data and sends a notification regarding this port. The default is 100 bytes.

In most cases, the console port of your device does not send any data unless there is an alarm condition. After the SLB branch office manager receives a small number of bytes, it perceives that your device needs some attention. The SLB unit notifies your technician when that point has been passed, and the notification includes the logged data.

For example, a threshold preset at 30 characters means that as soon as the SLB branch office manager receives 30 bytes of data, it captures log data and sends an email regarding this port.

Text String
The specific pattern of characters the SLB unit must recognize before sending a notification to the technician about this port. The maximum is 100 characters. You may use a regular expression to define the pattern. For example, the regular expression “abc[def]g” recognizes the strings abcdg, abceg, abcfg.

The SLB unit supports GNU regular expressions; for more information, see: [http://www.delorie.com/gnu/docs/regex/regex.html](http://www.delorie.com/gnu/docs/regex/regex.html)

Email Delay
A time limit of how long (in seconds), after the SLB branch office manager detects the trigger, that the device port captures data before closing the log file (with a fixed internal buffer maximum capacity of 1500 bytes) and sending a notification. The default is **60** seconds.

Restart Delay
The number of seconds for the period after the notification has been sent during which the device port ignores additional characters received. The data is simply ignored and does not trigger additional alarms until this time elapses. The default is **60** seconds.

Email to
The complete email address of the message recipient(s) for each device port(s). Each device port has its own recipient list. To enter more than one email address, separate the addresses with a **single space**. You can enter up to 128 characters.

Email Subject
A subject text appropriate for your site. May have up to 128 characters.

The email subject line is pre-defined for each port with its port number. You can use the email subject to inform the desired recipients of the problem on a certain server or location (e.g., server location or other classification of your equipment). This is helpful if the email message goes to the system administrator’s or service technician’s mobile or wireless device (e.g., text messaging by means of email).

*Note: The character sequence %d anywhere in the email subject is replaced with the device port number automatically.*

Log Viewing Attributes

<table>
<thead>
<tr>
<th>Display</th>
<th>Select to view either the beginning (head) or end (tail) of the log.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Lines</td>
<td>Number of lines from the head or tail of the log to display.</td>
</tr>
</tbody>
</table>
NFS File Logging

<table>
<thead>
<tr>
<th>NFS Log to View</th>
<th>Select the checkbox to log all data sent to the device port to one or more files on an external NFS server. Disabled by default.</th>
</tr>
</thead>
</table>
| Directory to Log to | The path of the directory where the log files will be stored.  
  *Note:* This directory must be a directory exported from an NFS server mounted on the SLB. Specify the local directory path for the NFS mount. |
| Max Number of Files | The maximum number of files to create to contain log data to the port. These files keep a history of the data received from the port. Once this limit is exceeded, the oldest file is overwritten. The default is 10. |
| Max Size of Files | The maximum allowable file size in bytes. The default is 2048 bytes. Once the maximum size of a file is reached, the SLB unit begins generating a new file. |

USB Logging

| USB Log to View | Available log files in the selected USB port to view. |
| Log To | Select the USB port to use for logging. |
| Max Number of Files | The maximum number of files to create to contain log data to the port. These files keep a history of the data received from the port. Once this limit is exceeded, the oldest file is overwritten. The default is 10. |
| Max Size of Files | The maximum allowable file size in bytes. The default is 2048 bytes. Once the maximum size of a file is reached, the SLB branch office manager begins generating a new file. The default is 2048 bytes. |

Syslog Logging

| Syslog Logging | Select to enable system logging.  
  *Note:* The logging level for the device ports log must be set to Info to view Syslog entries for Device Port logging on the Services > SSH/Telnet/Logging page. |

Note: To apply the settings to additional device ports, in the Apply settings to Device Ports field, enter the additional ports, (e.g., 1-3, 5, 6)

3. To apply settings to other device ports in addition to the currently selected port, select the **Apply settings to Device Ports** and enter port numbers separated by commas. Indicate a range of port numbers with a hyphen (e.g., 2, 5, 7-10), and separate ranges with commas.

4. To save, click the **Apply** button.

Logging Commands

Go to **Logging Commands (on page 317)** to view CLI commands which correspond to the web page entries described above.
8: Device Ports

Console Port

The console port initially has the same defaults as the device ports. Use the Devices > Console Port page to change the settings, if desired.

To set console port parameters:

1. Click the Devices tab and select Console Port. The following page displays:

   ![Console Port Page](image)

2. Change the following as desired:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud</td>
<td>The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the console port defaults to this value.</td>
</tr>
<tr>
<td>Data Bits</td>
<td>Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is 8 data bits.</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>The number of stop bits that indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is 1.</td>
</tr>
<tr>
<td>Parity</td>
<td>Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>A method of preventing buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is none.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The number of minutes (1-30) after which an idle session on the console is automatically logged out. Disabled by default.</td>
</tr>
<tr>
<td>Show Lines on Connecting</td>
<td>If selected, when you connect to the console port with a terminal emulator, you will see the last lines output to the console, for example, the SLB boot messages or the last lines output during a CLI session on the console.</td>
</tr>
</tbody>
</table>
3. Click the **Apply** button to save the changes.

### Console Port Commands

Go to [Console Port Commands (on page 300)] to view CLI commands which correspond to the web page entries described above.

### Power Outlets

The SLB branch office manager has eight outlets that can provide power to other units in an IT environment. Each outlet can be configured and controlled through the SLB unit. The SLB unit can issue an SNMP trap if the total current for all eight outlets exceeds a specified threshold.

**To configure a power outlet:**

1. Click the **Devices** tab and select the **Power Outlets** option. The following page displays:

   **Note:** Clicking any of the red P1 through P8 buttons, located at the top of each page displayed, allows controlled configuration of the power outlets.
Figure 8-10  Devices > Power Outlets

Switching Delay: **2000** msec

Over Current Alarm:  Off  On, Threshold (1-180): **10** Tents of Amps

Current Level for all Outlets: **0.0** Amps

<table>
<thead>
<tr>
<th>Outlet</th>
<th>Status</th>
<th>Name</th>
<th>Description</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Off</td>
<td>PowerOutlet-1</td>
<td>Power Outlet 1</td>
<td>0.0 Amps</td>
</tr>
<tr>
<td>P2</td>
<td>Off</td>
<td>PowerOutlet-2</td>
<td>Power Outlet 2</td>
<td>0.0 Amps</td>
</tr>
<tr>
<td>P3</td>
<td>Off</td>
<td>PowerOutlet-3</td>
<td>Power Outlet 3</td>
<td>0.0 Amps</td>
</tr>
<tr>
<td>P4</td>
<td>Off</td>
<td>PowerOutlet-4</td>
<td>Power Outlet 4</td>
<td>0.0 Amps</td>
</tr>
<tr>
<td>P5</td>
<td>Off</td>
<td>PowerOutlet-5</td>
<td>Power Outlet 5</td>
<td>0.0 Amps</td>
</tr>
<tr>
<td>P6</td>
<td>Off</td>
<td>PowerOutlet-6</td>
<td>Power Outlet 6</td>
<td>0.0 Amps</td>
</tr>
<tr>
<td>P7</td>
<td>Off</td>
<td>PowerOutlet-7</td>
<td>Power Outlet 7</td>
<td>0.0 Amps</td>
</tr>
<tr>
<td>P8</td>
<td>Off</td>
<td>PowerOutlet-8</td>
<td>Power Outlet 8</td>
<td>0.0 Amps</td>
</tr>
</tbody>
</table>

Power State:  Off  On  Last State
Wake Up Mode:  Off  On  Last State
Reboot:       

Power State:  Off  On  Last State
Wake Up Mode:  Off  On  Last State
Reboot:       

Power State:  Off  On  Last State
Wake Up Mode:  Off  On  Last State
Reboot:       

Power State:  Off  On  Last State
Wake Up Mode:  Off  On  Last State
Reboot:       

Power State:  Off  On  Last State
Wake Up Mode:  Off  On  Last State
Reboot:       

Power State:  Off  On  Last State
Wake Up Mode:  Off  On  Last State
Reboot:       

Power State:  Off  On  Last State
Wake Up Mode:  Off  On  Last State
Reboot:       

Apply
2. Enter the following:

<table>
<thead>
<tr>
<th><strong>Switching Delay</strong></th>
<th>Number of milliseconds the SLB branch office manager between subsequent switching. The range is 1000-2500 msec. The default is 2000 msec (2 sec).</th>
</tr>
</thead>
</table>
| **Over Current Alarm** | If SNMP traps are enabled (see Chapter 7: Services on page 87), a trap (alarm) is sent if the total current for all outlets exceeds a threshold. Enter the number of amps (measured in tenths of an amp) above which the SLB unit sends a trap. The maximum is 180.  
*Note: If the alarm goes off, a warning message displays on the CLI.* |
| **Current Level for all Outlets** | Displays the total load carried by the outlets. |

3. View or enter the following information for each outlet:

| **Outlet** | Displays the number of the outlet being configured. |
| **Status** | Displays the current state of the outlet. |
| **Name** | User-configurable name identifying the outlet. |
| **Description (optional)** | User-configurable text describing the outlet. |
| **Current** | Displays the load, in Amps, for the outlet. |
| **Power State** | Select whether the power should be on or off. Default is Off. |
| **Wakeup Mode** | Select whether, after a reboot, the power state for the outlet should be on, off, or returned to the state it was in before the reboot. Default is Off. |
| **Last State** | Select whether to return the outlet to the state it was in before the reboot. |
| **Reboot** | To power cycle the outlet, select the checkbox. Default is unchecked.  
*Note: You can reboot the SLB unit on the Maintenance > Firmware & Configurations page, but after the reboot, the power outlet has the same power state as it did before the reboot.* |

4. To save, click **Apply**.

**Power Commands**

Go to Power Commands (on page 330) to view CLI commands which correspond to the web page entries described above.

**Host Lists**

A host list is a prioritized list of SSH, Telnet, and TCP hosts available for establishing incoming modem connections or for the connect direct command on the CLI. The SLB branch office manager cycles through the list until it successfully connects to one.

**To view, update or delete a host list:**

1. Click the Devices tab and select the Host Lists option. The following page displays:
2. Select a host list and click the View Host List button. The list of hosts display in the Hosts box along with the settings for the selected host list (Figure 8-11).

3. You have the following options with a selected, existing host list:
   - To delete the selected host list, click the Delete Host List button.
   - To edit the selected host list, follow the steps below beginning with step 5.
   - To add a new host list, follow the steps below beginning with proceed to step 4.

4. To add a new host list, first deselect any selected host list by clicking the Clear Host List button, then proceed to step 5.

5. Enter or modify host list settings:

   **Host List Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host List Id</td>
<td>Displays after a host list is saved.</td>
</tr>
<tr>
<td>Host List Name</td>
<td>Enter a name for the host list.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times the SLB unit should attempt to retry connecting to the host list.</td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Escape Sequence</td>
<td></td>
</tr>
</tbody>
</table>

   **Host Parameters**

   - **Host**: The IP address of the host.
   - **Protocol**: The type of protocol used for communication.
   - **Port**: The port number used for communication.
   - **Escape Sequence**: The sequence used for escape sequences.

   **Hosts (in order of precedence)**

   - `172.19.37.2:ssh/22`
   - `172.19.37.3:ssh/22`
   - `0.0.0.123:tcp/123`
6. Click the right arrow. The host displays in the Hosts box.

7. Utilize the following options for managing the hosts in each host list:
   - To remove a host from the host list, select the host in the Hosts box and click the left arrow.
   - To give the host a higher precedence, select the host in the Hosts box and click the up arrow.
   - To give the host a lower precedence, select the host in the Hosts box and click the down arrow.

8. Repeat steps above as necessary, to modify or add host lists.

9. Save your changes:
   - Click the Add Host List button if adding new host lists.
   - Click the Clear Host List button if editing existing host lists.

After the process completes, a link back to the Device Ports > Settings page displays.

### Host List Commands

Go to Host List Commands (on page 315) to view CLI commands which correspond to the web page entries described above.

### Scripts

The SLB branch office manager supports three types of scripts:

- **Interface Scripts** which use a subset of the Expect/Tcl scripting language to perform pattern detection and action generation on Device Port output.

- **Batch Scripts** which are a series of CLI commands.
Custom Scripts are Expect scripts that use most of the Expect scripting language, can be run against the CLI or a Device Port, and can be scheduled to run at periodic intervals, with the results from each run saved to a file in a repository. Up to 10 Custom Scripts can be created. Each Custom Script run is an operation, and the results from each operation can be viewed. Up to 50 script result files will be saved locally in the SLB storage. Once this maximum is reached and new result files are generated, the oldest result files will automatically be deleted to accommodate the new result files.

A user can create scripts at the web, view scripts at the web and the CLI, and use (run) scripts at the CLI. For a description of the syntax allowed in the various types of scripts, see Batch Script Syntax, Interface Script Syntax, and Custom Script Syntax. Example Custom Scripts for Expect, Tcl and Python are provided.

The following versions are supported: Expect 5.45.4, Tcl 8.6.8, and Python 3.6.7. For Python scripts, the Pexpect module is supported.

All scripts have permissions associated with them; a user who runs a script must have the permissions associated with the script in order to run the script.

To add a script:

1. Click the Devices tab and select the Scripts option. This page displays.

Figure 8-12 Devices > Scripts
2. Click the **Add Script** button. The page for editing script attributes displays.

![Figure 8-13 Adding or Editing New Scripts](image)

3. Enter the following:

**Scripts**

<table>
<thead>
<tr>
<th>Script Name</th>
<th>A unique identifier for the script.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>◆ Select <strong>Interface</strong> for a script that utilizes Expect/Tcl to perform pattern detection and action generation on Device Port output.</td>
</tr>
<tr>
<td></td>
<td>◆ Select <strong>Batch</strong> for a script of CLI commands.</td>
</tr>
<tr>
<td></td>
<td>◆ Select <strong>Custom</strong> for an Expect, Tcl, or Python script that can be run against a CLI session or a Device Port, either manually or scheduled to run at periodic intervals.</td>
</tr>
</tbody>
</table>
4. In the **User Rights** section, select the user **Group** to which the script will belong:

### User Rights

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Users</td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td>Power Users</td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td>Administrators</td>
<td>This group has all possible rights. For more information on how the group and rights are used with scripts, see <em>To use a script at the CLI:</em> below.</td>
</tr>
</tbody>
</table>

5. Assign or unassign **User Rights** for the specific user by checking or unchecking the following boxes:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Administrative</td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td>Networking</td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage secure Lantronix units (e.g., SLP, Spider, SLC and SLB units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create a custom user menu for the CLI for NIS users.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to use the CLI or shut down the SLB unit and then reboot it.</td>
</tr>
<tr>
<td>Firmware &amp; Configuration</td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot &amp; Shutdown.</td>
</tr>
<tr>
<td>Device Port Operations</td>
<td>Right to enter device port settings for operations.</td>
</tr>
<tr>
<td>Device Port Configurations</td>
<td>Right to enter device port configurations.</td>
</tr>
<tr>
<td>USB</td>
<td>Right to enter modem settings for USB.</td>
</tr>
<tr>
<td>Power Outlets</td>
<td>Right to configure power outlets.</td>
</tr>
</tbody>
</table>

6. To save, click the **Apply** button. If the type of script is Interface, the script will be validated before it is saved. Once the script is saved, the main **Scripts** page is displayed.
To view or update a script:
1. In the Scripts table, select the script and click the Edit Script button. The page for editing script attributes displays (see Figure 8-13).
2. Update the script attributes (see To add a script: above).
3. To save, click the Apply button.

To rename a script:
1. In the Scripts table, select the script and enter a new script name in the New Name field.
2. Click the Rename Script button. The script will be renamed and the Devices > Scripts page redisplays.

To delete a script:
1. In the Scripts table, select the script to delete.
2. Click the Delete Script button. After a confirmation, the script will be deleted and the Devices > Scripts page redisplays.

To schedule a custom script:
1. Click the Devices tab and select the Scripts option. The Scripts page displays.
2. In the Scripts table, select the script and click the Schedule button. The Custom Scripts - Schedule page displays.

Figure 8-14  Devices > Scripts - Scheduler
3. Enter the following (each Custom Script can be run against one device - CLI or Device Port - with one schedule):

<table>
<thead>
<tr>
<th>Device Type</th>
<th>The device - either the CLI or a Device Port - that the script is connected to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The state of the script's schedule. A script must be enabled in order to allow the script scheduler to run the schedule. After a script has been scheduled and enabled, it can be disabled. In the disabled state the script manager will continue to update the scheduled run time for a script, but the script will not run or produce any results. At any point a schedule for a script can be deleted.</td>
</tr>
<tr>
<td>Command Line Arguments</td>
<td>Optional command line arguments to pass to the script each time it is run.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The date and time when the script should start running, either Now or at a specific date and time.</td>
</tr>
<tr>
<td>Frequency</td>
<td>How often the script will run, given in hours or days. The web UI and CLI will always display the frequency in hours.</td>
</tr>
<tr>
<td>Stop Time</td>
<td>The date and time when the script should stop running, either at a specified date and time, or Forever if it should never stop running.</td>
</tr>
</tbody>
</table>

4. To save, click the Apply button. The schedule will be validated, and the script manager will either immediately start running the script or schedule the next run of the script. The main Scripts page is displayed, showing the schedule status of the script (this may take a few seconds to be updated while the script manager processes the script - click Refresh to view the latest information).

Notes on scheduling:

- Scripts that are scheduled to start immediately and run forever will be restarted when the SLB is rebooted.
- Scripts that are scheduled to start at a specific time will be restarted when the SLB is rebooted if the script is scheduled to run forever or if the stop time has not expired.
- After the SLB has booted, there will be a short delay after launching each script before starting the next script in order to minimize the impact on system resources. Shortly after boot, if the script status shows that a script is not scheduled when the script is configured with a schedule, refreshing the status will eventually show that all scheduled scripts will be running and/or scheduled.
- If the date, time or timezone is changed on the SLC or SLB while a script is scheduled, the CLI and web UI will still show the same scheduled date and time for the script, until the next time the script is run. It is recommended that the date, time and timezone not be changed while scripts are scheduled to run.

To change the Enable/Disable state of a custom script schedule:

1. In the Scripts table, select the script to enable or disable.
2. Click the Enable button (this will resume running of a script at its next scheduled time if it was previously disabled) or the Disable button (this will suspend running of a script but continue to update the schedule). The script's state will be updated and the Scripts page redispays.

To view the list of completed operations (runs) for a custom script:

1. In the Scripts table, select the script to view operations for, and click Script Operations.
2. The Custom Scripts - Operations page displays, with a list of any results that have been
generated for a script, in reverse date/time order.

3. Any of the results can be viewed by selecting the operation and clicking **Script Results**.
To view the latest results from a completed operation (run) of a custom script:

1. Click the Devices tab and select the Scripts option. The Scripts page displays.
2. In the Scripts table, select the script to view results for, and click Latest Results. The results are displayed in a popup window.

![Figure 8-16 View Custom Script Results](image)

**SLB882 - Script Results**

The results are displayed in a popup window.

To use a script at the CLI:

1. To run an Interface Script or a Custom Script on a device port for pattern recognition and action generation, use the `connect script <Script Name> deviceport <Device Port # or Name>` command. This action requires that a SLB user running the connect script command have Device Port Operations (do) rights and port permissions for the selected device port.
2. To run a Batch Script at the CLI with a series of CLI commands, or a Custom Script for pattern recognition and action generation, use the `set script runcli <Script Name>` command.
command. This action requires that a SLB user running the \texttt{runcli} command belong to a group that is the same or greater than the group assigned to the script (e.g., if the script is assigned to the Power group, the user running the \texttt{runcli} command must belong to the Power or Admin group). For Batch Scripts, if this minimum group requirement is met, the SLB user will temporarily be granted all of the individual rights assigned to the script while the Batch Script is running. It is recommended that scripts that spawn \texttt{clisession} only be used with the \texttt{set script runcli} command (and not the \texttt{connect script} command), and that scripts that spawn \texttt{portsession} only be used with the \texttt{connect script} command (and not the \texttt{set script runcli} command).

\textbf{Note:} Custom Scripts have a \texttt{debug enable} option that supports printing Expect debug information to aid in creating an Expect script. The \texttt{debug} option is not supported for \texttt{Tcl} and \texttt{Python} scripts.

\section*{Batch Script Syntax}

The syntax for Batch Scripts is exactly the same as the commands that can be typed at the CLI, with the additions described in this section.

The \texttt{sleep} command suspends execution of the script (puts it to 'sleep') for the specified number of seconds. Syntax:

\begin{verbatim}
sleep <value>
\end{verbatim}

The \texttt{while} command allows a loop containing CLI commands to be executed. Syntax:

\begin{verbatim}
while {<Boolean expression>} { \\
  CLI command 1 \\
  CLI command 2 \\
  ... \\
  CLI command n
}
\end{verbatim}

\textbf{Note:} The closing left brace '{' must be on a line without any other characters. To support a \texttt{while} command, the \texttt{set} command, variables, and secondary commands are also supported.

\section*{Interface Script Syntax}

This section describes the abbreviated scripting syntax for Interface Scripts. This limited syntax was created to prevent the creation of scripts containing potentially harmful commands. Script commands are divided into three groups: Primary, Secondary and Control Flow. Primary commands provide the basic functionality of a script and are generally the first element on a line of a script, as in:

\begin{verbatim}
send_user "Password:"
\end{verbatim}

Secondary commands provide support for the primary commands and are generally not useful by themselves. For example, the \texttt{expr} command can be used to generate a value for a set command.

\begin{verbatim}
set <my_var> [expr 1 + 1]
\end{verbatim}

Control Flow commands allow conditional execution of other commands based on the results of the evaluation of a Boolean expression.
### Table 8-17 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word</td>
<td>A contiguous group of characters delimited on either side by spaces. Not enclosed by double quotes.</td>
</tr>
<tr>
<td>Primary Command</td>
<td>One of the primary commands listed in this section.</td>
</tr>
<tr>
<td>Secondary Command</td>
<td>One of the secondary commands defined in this section.</td>
</tr>
<tr>
<td>Quoted String</td>
<td>A group of characters enclosed by double quote (&quot; &quot;) characters. A quoted string may include any characters, including space characters. If a double quote character is to be included in a quoted string it must be preceded (escaped) by a backslash character ('').</td>
</tr>
<tr>
<td>Variable Reference</td>
<td>A word (as defined above) preceded by a dollar sign character ('$').</td>
</tr>
<tr>
<td>CLI Command</td>
<td>A quoted string containing a valid CLI <code>show</code> command.</td>
</tr>
<tr>
<td>Arithmetic Operator</td>
<td>A single character representing a simple arithmetic operation. The character may be one of the following:</td>
</tr>
<tr>
<td></td>
<td>✦ A plus sign (+) representing addition</td>
</tr>
<tr>
<td></td>
<td>✦ A minus sign (-) representing subtraction</td>
</tr>
<tr>
<td></td>
<td>✦ An asterisk sign (*) representing multiplication</td>
</tr>
<tr>
<td></td>
<td>✦ A forward slash (/) representing division</td>
</tr>
<tr>
<td></td>
<td>✦ A percent sign (%) representing a modulus</td>
</tr>
<tr>
<td>Boolean Expression</td>
<td>An expression which evaluates to TRUE or FALSE. A Boolean expression has the following syntax:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;value&gt; &lt;Boolean operator&gt; &lt;value&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Each can be either a word or a variable reference.</td>
</tr>
<tr>
<td>Boolean Operator</td>
<td>A binary operator which expresses a comparison between two operands and evaluates to TRUE or FALSE. The following Boolean operators are valid:</td>
</tr>
<tr>
<td></td>
<td>✦ '&lt;' less than</td>
</tr>
<tr>
<td></td>
<td>✦ '&gt;' greater than</td>
</tr>
<tr>
<td></td>
<td>✦ '&lt;=' less than or equal to</td>
</tr>
<tr>
<td></td>
<td>✦ '&gt;=' greater than or equal to</td>
</tr>
<tr>
<td></td>
<td>✦ '==' equal to</td>
</tr>
<tr>
<td></td>
<td>✦ '!=' not equal to</td>
</tr>
</tbody>
</table>

### Primary Commands

These are stand-alone commands which provide the primary functionality in a script. These commands may rely on one or more of the Secondary Commands to provide values for some parameters. The preprocessor will require that these commands appear only as the first element of a command line. The start of a command line is delimited by any of the following:

- The start of a new line of text in the script
- A semicolon (";")
- A left brace ('{')
### Table 8-18 Primary Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>set</strong></td>
<td>The <code>set</code> command assigns a value to a variable. Syntax: &lt;br&gt;<code>&lt;variable&gt; &lt;value&gt;</code> &lt;br&gt;where <code>&lt;variable&gt;</code> is a word, and <code>&lt;value&gt;</code> can be defined in one of the following ways:  &lt;br&gt;♦ A quoted string  &lt;br&gt;♦ A word  &lt;br&gt;♦ A variable reference  &lt;br&gt;♦ A value generated via one of the string secondary commands (compare, match, first, etc.)  &lt;br&gt;♦ A value generated via the <code>expr</code> secondary command  &lt;br&gt;♦ A value generated via the <code>format</code> secondary command  &lt;br&gt;♦ A value generated via the <code>expr timestamp</code> command</td>
</tr>
<tr>
<td><strong>unset</strong></td>
<td>This command removes the definition of a variable within a script. Syntax: &lt;br&gt;<code>unset &lt;variable&gt;</code> &lt;br&gt;where <code>&lt;variable&gt;</code> is a word.</td>
</tr>
<tr>
<td><strong>scan</strong></td>
<td>The <code>scan</code> command is analogous to the C language <code>scanf()</code>. Syntax: &lt;br&gt;<code>scan &lt;variable&gt; &lt;format string&gt; &lt;value 1&gt; &lt;value 2&gt; ... &lt;value n&gt;</code> &lt;br&gt;where <code>&lt;variable&gt;</code> a variable reference, and <code>&lt;format string&gt;</code> is a quoted string. Each of the <code>&lt;value x&gt;</code> elements will be a word.</td>
</tr>
<tr>
<td><strong>sleep</strong></td>
<td>The <code>sleep</code> command suspends execution of the script (puts it to 'sleep') for the specified number of seconds. Syntax: &lt;br&gt;<code>sleep &lt;value&gt;</code> &lt;br&gt;where <code>&lt;value&gt;</code> can be a word, a quoted string or a variable reference.</td>
</tr>
<tr>
<td><strong>exec</strong></td>
<td>The <code>exec</code> command executes a single CLI command. Currently only CLI 'show' commands may be executed via <code>exec</code>. Syntax: &lt;br&gt;<code>exec &lt;CLI command&gt;</code></td>
</tr>
<tr>
<td><strong>send, send_user</strong></td>
<td>The <code>send</code> command sends output to a sub-process. The <code>send_user</code> command sends output to the standard output. Both commands have the same syntax: &lt;br&gt;<code>send &lt;string&gt;</code> &lt;br&gt;<code>send_user &lt;string&gt;</code> &lt;br&gt;where <code>&lt;string&gt;</code> can be either a quoted string or a variable reference.</td>
</tr>
<tr>
<td><strong>expect, expect_user, expect_before, expect_after, expect_background</strong></td>
<td>The <code>expect</code> command waits for input and attempts to match it against one or more patterns. If one of the patterns matches the input the corresponding (optional) command is executed. All <code>expect</code> commands have the same syntax: &lt;br&gt;<code>expect {&lt;string 1&gt; {command 1} &lt;string 2&gt; {command 2} ... &lt;string n&gt; {command n}}</code> &lt;br&gt;where <code>&lt;string x&gt;</code> will either be a quoted string, a variable reference or the reserved word 'timeout.' The command <code>x</code> is optional, but the curly braces <code>{' and '}</code>). are required. If present it must be a primary command.</td>
</tr>
<tr>
<td><strong>return</strong></td>
<td>The <code>return</code> command terminates execution of the script and returns an optional value to the calling environment. Syntax: &lt;br&gt;<code>return &lt;value&gt;</code> &lt;br&gt;where <code>&lt;value&gt;</code> can be a word or a variable reference.</td>
</tr>
</tbody>
</table>
Secondary Commands

These are commands which provide data or other support to the Primary commands. These commands are never used by themselves in a script. The preprocessor will require that these commands always follow a left square bracket ('[') character and be followed on a single line by a right bracket (']').

Table 8-19  Secondary Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| string    | The string command provides a series of string manipulation operations. The string command will only be used with the set command to generate a value for a variable. There are nine operations provided by the string command. Syntax (varies by operation):
  string compare <str 1> <str 2>
    Compare two strings
  string match <str 1> <str 2>
    Determine if two strings are equal
  string first <str needle> <str haystack>
    Find and return the index of the first occurrence of 'str_needle' in 'str_haystack'
  string last <str needle> <str haystack>
    Find and return the index of the last occurrence of 'str_needle' in 'str_haystack'
  string length <str>
    Return the length of 'str'
  string index <str> <int>
    Return the character located at position 'int' in 'str'
  string range <str> <int start> <int end>
    Return a string consisting of the characters in 'str' between 'int start' and 'int end'
  string tolower <str>
    Convert <str> to lowercase
  string toupper <str>
    Convert <str> to uppercase
  string trim <str 1> <str 2>
    Trim 'str 2' from 'str 1'
  string trimleft <str 1> <str 2>
    Trim 'str 2' from the beginning of 'str 1'
  string trimright <str 1> <str 2>
    Trim 'str 2' from the end of 'str 1'
In each of the above operations, each <str *> element can either be a quoted string or a variable reference. The <int *> elements will be either words or variable references.
Control Flow Commands

The control flow commands allow conditional execution of blocks of other commands. The preprocessor treats these as Primary commands, allowing them to appear anywhere in a script that a Primary command is appropriate.

Table 8-20 Control Flow Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| expr | This command evaluates an arithmetic expression and returns the result. The expr command will only be used in combination with the set command to generate a value for a variable. Syntax: 
  expr <value> <operation> <value>
  Each <value> will be either a word or a variable reference, and <operation> an arithmetic operation. |
| timestamp | This command returns the current time of day as determined by the SLB unit. The timestamp command will only be used in combination with the set command to produce the value for a variable. Syntax: 
  timestamp <format> 
  where <format> is a quoted string. |
| format | The format command is analogous to the C language sprintf(). The format command will only be used in combination with the set command to produce the value for a variable. Syntax: 
  format <format string> <value 1> <value 2> ... <value n> 
  where <format string> will be a quoted string. Each of the <value x> elements will be a word, a quoted string or a variable reference. |
| while | The while command executes an associated block of commands as long as its Boolean expression evaluates to TRUE. After each iteration the Boolean expression is re-evaluated; when the Boolean expression evaluates to FALSE execution passes to the first command following the associated block. Each command within the block must be a Primary command. Syntax: 
  while {<Boolean expression>} { 
    command 1 
    command 2 
    ... 
    command n 
  } |
Custom Script Syntax

This section describes the scripting syntax for Custom Scripts. The syntax is more flexible than Interactive Script syntax, but still has restrictions to prevent the creation of scripts containing potentially harmful commands. In addition, Custom Scripts can be configured to use command line parameters. Custom Scripts have the following guidelines:

1. The size of the script file cannot exceed 6 Kbytes.
2. The size of the results generated by the script cannot exceed 1 Kbyte (any results over 1Kbyte will be truncated).
3. The first line of the script must contain a Linux script style interpreter directive so that the SLB will know which interpreter to use to run the script. The format of the first line is `#!/ expect`, `#!/ tcl`, or `#!/ python`. When a custom script is imported, the interpreter line must match the selected script or file type (Expect, Tcl or Python), otherwise the script will be invalid.
4. The script should include a spawn command to connect the script to either a SLB CLI session or a SLB Device Port session. Refer to the following spawn command syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| if, elseif and else | The `if` command executes an associated block of commands if its Boolean expression evaluates to TRUE. Each command within the block must be a Primary command. Syntax: 

```bash
if {<Boolean expression>} {
    command 1
    command 2
    ...
    command n
}
```

The `elseif` command is used in association with an `if` command - it must immediately follow an `if` or `elseif` command. It executes an associated block of commands if its Boolean expression evaluates to TRUE. Each command within the block must be a Primary command. Syntax: 

```bash
elseif {<Boolean expression>} {
    command 1
    command 2
    ...
    command n
}
```

The `else` command is used in combination with an `if` or `elseif` command to provide a default path of execution. If the Boolean expressions for all preceding `if` and `elseif` commands evaluate to FALSE the associated block of commands is executed. Each command within the block must be a primary command. Syntax: 

```bash
else {
    command 1
    command 2
    ...
    command n
}
```
Note:

- For CLI sessions, a local user name should be given
- For Device Port sessions, the $devicePort variable will be used by the SLB to connect the script to the appropriate Device Port. The -noecho flag may be passed to spawn command.

- Expect script - CLI session
  
  spawn clisession -U <username>

- Expect script - Device Port session
  
  spawn portsession -p $devicePort

- Tcl script - CLI session
  
  set io [open "| clisession -U <username>" r+]

- Tcl script - Device Port session
  
  set io [open "| portsession -p $devicePort" r+]

- Python script - CLI session
  
  subprocess.Popen(['clisession', '-U', '<username>'],
                   stdin=subprocess.PIPE,
                   stdout=subprocess.PIPE,
                   stderr=subprocess.PIPE)

- Python script - Device Port session
  
  subprocess.Popen(['portsession', '-p', devicePort],
                   stdin=subprocess.PIPE,
                   stdout=subprocess.PIPE,
                   stderr=subprocess.PIPE)

It is recommended that scripts that spawn clisession only be used with the set script runcli command (and not the connect script command), and that scripts that spawn portsession only be used with the connect script command (and not the set script runcli command).

5. The script cannot contain commands which spawn or fork other commands, read or write files on the SLB filesystem, or interrogate the SLB environment. The list of commands that are not allowed for Expect scripts includes "fork", "open", "exp_open", "exec", "system", "log_file", "pwd".

6. For scripts that return an exit code, the SLB will interpret an exit code of zero as a successful exit code, and any non-zero exit code as an error. Non-zero exit codes are displayed (at the CLI) or logged (for scripts that are run by the script scheduler).
Example Scripts

*Interface Script—Monitor Port*

The Monitor Port (Monport) script connects directly to a device port by logging into the SLB port, gets the device hostname, loops a couple of times to get port interface statistics, and logs out. The following is the script:

```bash
set monPort 7
set monTime 5
set sleepTime 2
set prompt ">
set login "sysadmin"
set pwd "PASS"
#Send CR to echo prompt
send ";r"
sleep $sleepTime
#Log in or check for Command Prompt
expect {
    #Did not capture "login" or Command Prompt
    timeout { send_user "Time out login.......\n"; return }
    #Got login prompt
    "login" {
        send_user "Logging in....\n"
        send "$login\r"
        expect {
            timeout { send_user "Time out waiting for pwd
            prompt.......\n"; return }
            #Got password prompt
            "password" {
                #Send Password
                send "$pwd\r"
                expect {
                    timeout { send_user "Time out waiting for prompt.......\n";
                    return }
                    $prompt {}
                }
            }
        }
    }
    #Already Logged in got Command Prompt
    $prompt {
        send_user "Already Logged....\n"
    }
}
#Get hostname info
send "show network port 1 host\r"
expect {
    timeout { send_user "Time out Getting Hostname 1\r\n"; return }
    "Domain" {
        #Get Hostname from SLB
        set hostname "[string range $expect_out(buffer) [string first
                      Hostname:
```
$expect_out(buffer)
$expect_out(buffer)-2
}
}$expect_out(buffer)

send_user "$r\n$r\n$r\n$r\n"
send_user "Device [string toupper $hostname]\r\n"

send_user "Monitored Port: Port $monPort \r\n"

send_user "Monitor Interval Time: $monTime Seconds \r\n"

set loopCtr 0
set loopMax 2
while { $loopCtr < $loopMax } {
    #Get current time

    The following is the screen output:

    show network port 1 host

    Hostname: slb251glenn
    Domain: support.int.lantronix.com
    Device HOSTNAME: SLB 251GLENN

    Monitored Port: Port 7
    Monitor Interval Time: 5 Seconds
    [Current Time:21:16:43]
    show portcounter deviceport 7

    Device Port: 7 Seconds since zeroed: 1453619
    Bytes input: 0 Bytes output: 0
    Framing errors: 0 Flow control errors: 0
    Overrun errors: 0 Parity errors: 0

    [slb251glenn]> show portcounter deviceport 7

    Device Port: 7 Seconds since zeroed: 1453634
    Bytes input: 0 Bytes output: 0
    Framing errors: 0 Flow control errors: 0
    Overrun errors: 0 Parity errors: 0

    Port Counter Monitor Script Ending.....

    Login Out........
    logout
    Returning to command line
Batch Script—SLB CLI

This script runs the following SLB CLI commands, then runs the Monport Interface script:

- show network port 1 host
- show deviceport names
- show script
- connect script monport deviceport 7

The following is the screen output of the script:

```
[slb247glenn]> se script runcli cli
[slb247glenn]> show network port 1 host
Current Hostname Settings
Hostname: slb247glenn
Domain: <none>

[slb247glenn]> show deviceport names
Current Device Port Names
01 - SCS_ALIAS_Test 05 - Port-5
02 - Port-2 06 - Port-6
03 - Port-3 07 - SLB -251
04 - Port-4 08 - Port-8

[slb247glenn]> show script
Interface Scripts
getslb Adm/ad,nt,sv,dt,lu,ra,um,dp,fc,dr,sn,wb,sk,po,do
Test Adm/ad,nt,sv,dt,lu,ra,um,dp,fc,dr,sn,wb,sk,po,do
monport Adm/<none>

[slb247glenn]> connect script monport deviceport 7
login: Logging in....
sysadmin
Password: PASS
Welcome to the Secure Lantronix Branch Office Manager
Model Number: slb 48
For a list of commands, type 'help'.

[slb251glenn]> show network port 1 host
show network port 1 host
Current Hostname Settings
Hostname: slb251glenn
Domain: support.int.
Device HOSTNAME: SLB 251GLENN

Monitored Port: Port 7
Monitor Interval Time: 5 Seconds
[Current Time: 21:25:04]
show portcounter deviceport 7
lantronix.com
```
[slb251glenn]> show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1454120
Bytes input: 0 Bytes output: 0
Framing errors: 0 Flow control errors: 0
Overrun errors: 0 Parity errors: 0
[slb251glenn]> [Current Time:21:25:20]
show portcounter deviceport 7
show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1454136
Bytes input: 0 Bytes output: 0
Framing errors: 0 Flow control errors: 0
Overrun errors: 0 Parity errors: 0
[slb251glenn]> Port Counter Monitor Script Ending......
________________________________________________________________________
Login Out....... logout
Returning to command line
[slbvz249_glenn]> show script
___Interface Scripts______Group/Permissions_____________________________
test3_________________Def/do
___Batch Scripts__________Group/Permissions_____________________________
test1_________________adm/
AD,nt,sv,dt,lu,ra,um,dp,ub,rs,fc,dr,sn,wb,sk,po,do
[slbvz249_glenn]>

Expect Custom Script - SLB CLI Session

An example of an Expect Custom Script that interacts with a SLB CLI session:

```bash
#!/ expect
# script to get the current internal temperature of the SLB
# accepts one optional command line parameter for location

set slbPrompt ">
set slbTemp "unknown"
set location 

proc myprint {str} {
  send_user -- "$str
"
}

proc abortSession {err} {
  send_user "Error $err. Terminating session.\n"
  exit $err
}

# Are there any command line parameters?
if {$argc > 0} {
  set location [lindex $argv 0]
}

set now [clock seconds]
```
set date [clock format $now -format {%D %R}]
if {$argc > 0} {
    myprint "Internal temperature of the $location SLB at $date"
} else {
    myprint "Internal temperature of the SLB at $date"
}

# spawn the CLI session
if {[catch {spawn -noecho clisession -U sysadmin} result]} {
    abortSession 1
} set sessionId $spawn_id

# Handle eof
expect_after {
    -i $sessionId eof {
        myprint "Session unexpectedly terminated."
        abortSession 2
    }
}

set timeout 10
log_user 0

# Wait for the first prompt
set loggedIn false
while {! $loggedIn} {
    expect {
        timeout {myprint "Timeout waiting to login"; abortSession 3} "Need to specify username" {myprint "Need to specify -U "; abortSession 4} "*> " {set loggedIn true} ;
    }
}

exp_send "$\n"
expect {
    timeout {myprint "Timeout waiting for CLI prompt"; abortSession 3} -re "$\n(\[^r]*\)>" 
} set slbPrompt $expect_out(1,string)

# Run the temperature command
exp_send "show temperature\n"
expect {
    timeout {myprint "Timeout waiting for temperature"; abortSession 3} -re "Current Internal Temperature: (.*)\n"
} set slbTemp $expect_out(1,string)
myprint "Temperature: $slbTemp"

exp_send "logout\n"
sleep .5
close
exit 0

This script can be run manually at the CLI:

```
[slb431d] set script runcli cliExample parameters "East Data Center"
Internal temperature of the East Data Center SLB at 01/27/2019 02:07
Temperature: 48C (118F)
```

**Expect Custom Script - SLB Device Port Session**

An example of an Expect Custom Script that interacts with a SLB Device Port (in this example a ServerTech PDU is connected to a Device Port):

```
#!/ expect
#
# Script to get the load of a ServerTech PDU outlet
#
set pduPrompt "\"\""
set pduLoad "unknown"

proc myprint {str} {
    send_user -- "$str\n"
}

proc abortSession {err} {
    send_user "Error $err. Terminating session.\n"
    exit $err
}

set now [clock seconds]
set date [clock format $now -format {%D %R}]
myprint "Load of ServerTech PDU outlet B1 at $date"

# spawn the port session on a device port
if {[catch {spawn -noecho portsession -p $devicePort} result]} {
    abortSession 1
}
set sessionId $spawn_id

# Handle eof
expect_after {
    -i $sessionId eof {
        myprint "Session unexpectedly terminated."
        abortSession 2
    }
}

set timeout 10
log_user 0

# Login to the PDU
# The "Error:*" pattern matches all error messages output by portsession
```
# send "\n"
expect {
    "Username:" {send "admn\n" }
    "Error:*\r\n" {send_user $expect_out(0,string); abortSession 2 }
}
expect "Password:"
send "admn\n"

# Wait for the first prompt
set loggedIn false
while {! $loggedIn} {
    expect {
        timeout {myprint "Timeout waiting to login"; abortSession 3}
        "*CDU: " {set loggedIn true}
    };
}

# Detect the prompt
exp_send "\n"
expect "are:\r\n"
expect "LOGIN:\r\n"
expect "REMOVE:\r\n"
expect "RESTART:\r\n"
expect {
    timeout {myprint "Timeout waiting for prompt"; abortSession 3}
    -re "\r\n([^\r]*)"
}
set pduPrompt $expect_out(1,string)

# Run the ostat command
exp_send "ostat .b1\n"
expect "Outlet*Power:\r\n"
expect "ID*Watts*:\r\n"
expect {
    timeout {myprint "Timeout waiting for load"; abortSession 3}
    -re "\.B1\s+\S+\s+\S+\s+(\S+))"
}
set pduLoad $expect_out(1,string)
myprint "Outlet B1 Load: $pduLoad Amps"

expect $pduPrompt
exp_send "logout\n"
sleep .5
close
exit 0
**Expect Custom Script - SLB Device Port Session**

An example of an Expect Custom Script that interacts with a SLC or SLB Device Port (in this example a Cisco server is connected to a Device Port):

```bash
#! expect
#
# Save a copy of the running config of a Cisco server to a TFTP server
# The Cisco server is connected to a SLC/B device port
#
proc myprint {str} {
    send_user -- "$str\n"
}

proc abortSession {err} {
    send_user "Error $err. Terminating session.\n"
    exit $err
}

if {$argc < 2} {
    myprint "Usage: script_md_cisco.exp <TFTP Server> <Backup File Name>"
    abortSession 1
}

set tftp [lindex $argv 0]
set configFile [lindex $argv 1]
set enablePassword "secret"
set timeout 10

set now [clock seconds]
set date [clock format $now -format {%D %R}]
myprint "Backing up Cisco Server to $tftp:$configFile at $date"

# spawn the port session on a device port
if {{[catch {spawn -noecho portsession -p $devicePort} result]}} {
    abortSession 2
}
set sessionId $spawn_id

# Handle eof
expect_after {
    -i $sessionId eof {
        myprint "Session unexpectedly terminated."
        abortSession 3
    }
}

log_user 0

# Send carriage return, see if we are connected
set loggedIn false
set execMode false
set passwordPrompt false
set cnt 1
while {! $loggedIn || ! $execMode} {
    if {$cnt == 5} {
        myprint "Timeout waiting for > or # prompt"
        abortSession 4
    }
    if {! $passwordPrompt} {
        send "\r"
    }
    expect {
        "Password: " { send "$enablePassword\r" }
        ">" { set loggedIn true; set passwordPrompt true; send "enable\r"
        }
        "#" { set loggedIn true; set execMode true }
        "Error:*\r\n" { send_user $expect_out(0,string); abortSession 5 }
        timeout {set cnt [expr {$cnt + 1}]} }
    }
    myprint "Logged in."
    send "copy running-config tftp://$tftp/$configFile\r"
    expect "$tftp"
    send "\r"
    expect "$configFile"
    send "\r"
    myprint "Backup initiated."
    expect {
        "!!" { myprint "Successfully backed up." }
        timeout { myprint "Timeout waiting for backup to complete.";
        abortSession 6 }
    }
    send "exit\r"
    sleep .5
    close
    exit 0
**Python Custom Script - SLB CLI Session**

An example of a Python Custom Script that interacts with a CLI session:

```python
#!/ python
# Script to set the RADIUS authentication settings of the SLB
# Sets the first RADIUS server and secret, and enables RADIUS
# Note: passing secret as a command line parameter is a security vulnerability
# Usage:
#   script_cli_radius.py <RADIUS server> <RADIUS secret>
#

import subprocess
import datetime
import sys

num_args = len(sys.argv) - 1
if num_args < 2:
    print("Usage: script_cli_radius.py <RADIUS server> <RADIUS secret>")
    sys.exit(1)

print("Settings RADIUS server on SLC at ", end="")
now = datetime.datetime.now()
print(now.strftime("%Y-%m-%d %H:%M"), end="")

server = sys.argv[1]
secret = sys.argv[2]

proc = subprocess.Popen(['clisession', '-U', 'sysadmin'],
                        stdin=subprocess.PIPE,
                        stdout=subprocess.PIPE,
                        stderr=subprocess.PIPE)

# wait for prompt
while True:
    output_str = proc.stdout.readline()
    if b'list of commands' in output_str:
        proc.stdin.write(b'\n')
        proc.stdin.flush()
    if b'>' in output_str:
        break
    if b'Invalid local user' in output_str:
        print("Invalid local user passed to clisession.")
        proc.stdin.close()
        proc.terminate()
        proc.wait()
        sys.exit(1)

# Run the RADIUS command
s = "set radius server 1 host " + server + " secret " + secret + "\n"
b = bytearray(s.encode())
proc.stdin.write(b)
proc.stdin.flush()```
while True:
    output_str = proc.stdout.readline()
    if b'RADIUS settings successfully updated' in output_str:
        break
    elif b'set radius' not in output_str:
        # RADIUS command returned an error
        s1 = str(output_str)
        s2 = s1.split("\r")[1]
        print("RADIUS command returned: " + s2.split("\n")[0])
        proc.stdin.close()
        proc.terminate()
        proc.wait()
        sys.exit(1)

    proc.stdin.write(b'set radius state enable
')
    proc.stdin.flush()
    while True:
        output_str = proc.stdout.readline()
        if b'RADIUS settings successfully updated' in output_str:
            break
        elif b'set radius' not in output_str:
            # RADIUS command returned an error
            s1 = str(output_str)
            s2 = s1.split("\r")[1]
            print("RADIUS command returned: " + s2.split("\n")[0])
            proc.stdin.close()
            proc.terminate()
            proc.wait()
            sys.exit(1)

    print("RADIUS settings updated and enabled.")
    proc.stdin.close()
    proc.terminate()
    proc.wait()
    sys.exit(0)

**Python Custom Script - SLB CLI Session**

An example of a Python Custom Script that uses the Pexpect module to interact with the CLI session and the device ports to detect the prompt on any devices connected to the SLB, and set the device port name to be the same as the device prompt:

```python
#!/ python
# Script to detect the prompt on a device connected to a SLC or SLB device port,
# and set the device port name to the prompt. Punctuation characters are
# removed and the device port number is appended to the name. Prompts ending
# in '>' are detected. For example, for a Cisco device attached to device
# port 3 and displays this prompt:
#   engcisco_cat3560>
# the name for device port 3 will be set to "engcisco_cat3560-3"
```
import pexpect
import datetime
import time
import sys
import re

now = datetime.datetime.now()
print("Detecting devices on SLC at ", end="")
print(now.strftime("%Y-%m-%d %H:%M"))

# start the CLI session to get number of device ports
p=pexpect.spawn('clisession -U sysadmin')

slcPrompt = ""
numPorts = 0
loggedIn = False

while not loggedIn:
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
        'Model Number: SLC80(\d*)\r\n', 'Model Number: SLB882\r\n', '(\[.*>)', timeout=10)

    if i == 0:   # Timeout
        print("Timeout waiting to login.")
        p.terminate(True)
        sys.exit(1)
    elif i == 1: # EOF
        print("Session unexpectedly terminated.")
        p.terminate(True)
        sys.exit(1)
    elif i == 2: # SLC8000 model number
        model = p.match.group(1)
        numPorts = int(model)
    elif i == 3: # SLB882 model number
        numPorts = 8
    elif i == 4: # prompt
        loggedIn = True
        slcPrompt = p.match.group(1).decode('utf-8')

if numPorts == 0:
    print("Cannot determine number of device ports.")
    p.terminate(True)
    sys.exit(1)

print("Number of device ports:", numPorts)

# Terminate the CLI session
p.sendline("logout")
time.sleep(.500)
p.wait()

skipPorts = False
devicePort = 1
pList = []

if numPorts == 24 or numPorts == 40:
    # Adjust port numbering for SLC8024 and SLC8040
    skipPorts = True
    numPorts = numPorts + 8

# Loop through device ports, connect and try to detect the prompt
while devicePort <= numPorts:
    if skipPorts and devicePort >= 9 and devicePort <= 16:
        devicePort = devicePort + 1
        continue
    print("Scanning device port", devicePort, ",", sep=''")
    port = str(devicePort)
    p = pexpect.spawn('portsession', ['-p', port])

    # Login (if required), and wait for the first prompt
    p.sendline(""")
    gotPrompt = False
    slcDevice = False
    cnt = 1
    while not gotPrompt:
        i = p.expect([pexpect.TIMEOUT, pexpect.EOF, 'login:', 'Error: (.*)\r\n', '>', ], timeout=10)
        if i == 0:     # Timeout
            cnt = cnt + 1
            print("Timeout waiting to connect to DP", devicePort, ".")
            p.terminate(True)
            break
            # may need to send a CR to get prompt
            p.send("\r")
        elif i == 1:   # EOF
            print("portsession on DP ", devicePort, "unexpectedly terminated.")
            break
        elif i == 2:   # login prompt
            p.sendline("sysadmin")
            p.expect("Password:")
            p.sendline("PASS")
            slcDevice = True
            gotPrompt = True
        elif i == 3:   # error from portsession
            print(p.match.group(1).decode('utf-8'))
            p.terminate(True)
            p.wait()
            break
        elif i == 4:   # prompt
            gotPrompt = True
            break
    # end if while not gotPrompt:
if not gotPrompt:
    devicePort = devicePort + 1
    pList.append('')
    continue

# Detect the prompt
devPrompt = ""
p.send("\n")
i = p.expect([pexpect.TIMEOUT, pexpect.EOF, '\r\n(.*)>'], timeout=10)
if i == 0 or i == 1:   # Timeout or EOF
    print("Timeout waiting for the prompt on DP", devicePort, ".")
p.terminate(True)
p.wait()
devicePort = devicePort + 1
pList.append('')
continue
if i == 2:             # prompt
    devPrompt = p.match.group(1).decode('utf-8')
if devPrompt == "":
    print("Timeout waiting for the prompt on DP", devicePort, ".")
    devicePort = devicePort + 1
    pList.append('')
    continue

print("Detected prompt", devPrompt, ".")
# Strip characters not allowed in DP names
devPromptStrip = re.sub("[^0-9A-Za-z\._\-]", ",", devPrompt)
devPromptComplete = devPromptStrip + "-" + str(devicePort)
pList.append(devPromptComplete)

p.terminate(True)
p.wait()
devicePort = devicePort + 1
# end of while devicePort <= numPorts:

# Connect to the SLC CLI and set the device port names
p=pexpect.spawn('clisession -U sysadmin')

loggedIn = False
while not loggedIn:
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
                  'Model Number: SLC80(\d*)\r\n', 'Model Number:
SLB882\r\n', '('\[.*\])', timeout=10)
    if i == 0:   # Timeout
        print("Timeout waiting to login.")
p.terminate(True)
sys.exit(1)
elif i == 1: # EOF
    print("Session unexpectedly terminated.")
p.terminate(True)
sys.exit(1)
elif i == 4: # prompt
    loggedIn = True

devicePort = 1
while devicePort <= numPorts:
    if skipPorts and devicePort >= 9 and devicePort <= 16:
        devicePort = devicePort + 1
        continue
    if len(pList[devicePort - 1]) > 0:
        # Detected a prompt; set it
        print("Setting name on DP", devicePort, "to", pList[devicePort -
1], ", ".")
        s = "set deviceport port " + str(devicePort) + " name " +
pList[devicePort - 1]
        p.sendline(s)
        i = p.expect([pexpect.TIMEOUT,
            'Device Port settings successfully updated.\r\n'],
            timeout=10)
        if i == 0:   # Timeout
            print("Timeout waiting for response.")
        devicePort = devicePort + 1

    # Terminate the CLI session
    p.sendline("logout")
    time.sleep(.500)
    p.wait()
    print("Script completed.")
    sys.exit(0)

Tcl Custom Script - SLB CLI Session

An example of a Tcl Custom Script that interacts with a CLI session:

#! tcl
# Script to get the current internal temperature of the SLB
# Accepts one optional command line parameter for location

set slcTemp "unknown"
set location ""

# Are there any command line parameters?
if {$argc > 0} {
    set location [lindex $argv 0]
}

set now [clock seconds]
set date [clock format $now -format {%D %R}]
if {$argc > 0} {
    puts "Internal temperature of the $location SLC at $date"
} else {
    puts "Internal temperature of the SLC at $date"
}
set io [open "| clisession -U sysadmin" r+]

set loggedIn false
while {! $loggedIn} {
    set len [gets $io line]
    if {[string first "Invalid local user" $line] != -1} {
        puts "Invalid local user passed to clisession"
        break
    }
    if {[string first "For a list of commands" $line] != -1} {
        puts $io "\n"
        flush $io
    }
    if {[string first ">" $line] != -1} {
        set loggedIn true
    }
}
if {! $loggedIn} {
    exit 1
}

puts $io "show temp"
flush $io
set gotTemp false
while {! $gotTemp} {
    set len [gets $io line]
    if {[string first "Current Internal Temperature" $line] != -1} {
        set slcTemp [string range $line [expr {[string first ":" $line] + 1}]]
        set gotTemp true
    }
}

puts "Temperature: $slcTemp"
puts $io "logout"
flush $io
exit 0
Sites

A site is a group of site-oriented modem parameters that can be activated by various modem-related events (authentication on dial-in, outbound network traffic for a dial-on-demand connection, etc.). The site parameters will override parameters that are configured for a modem.

To use sites with a modem, create one or more sites (described below), then enable Use Sites for the modem. Sites can be used with the following modem states: dial-in, dial-back, CBCP Server, dial-on-demand, dial-in & dial-on-demand, and dial-back & dial-on-demand. For more information on how sites are used with each modem state, see Modem Dialing States on page 173.

To add a site:

1. Click the Devices tab and select the Sites option. The Sites page displays:
2. In the lower section of the page, enter the following:

   Note: To clear fields in the lower part of the page, click the Reset Site button.

<table>
<thead>
<tr>
<th>Site Id (view only)</th>
<th>Displays after a site is created.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Enter a name for the site.</td>
</tr>
<tr>
<td>Port</td>
<td>Select the Device Port or the USB Port the site is assigned to. For dial-on-demand sites, a port must be selected. For any other sites, the port selection can be set to None. See Modem Dialing States on page 173.</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Login/CHAP Host</td>
<td>The login name (for PAP authentication) or CHAP host (for CHAP authentication) associated with this site. If a modem has sites enabled and the authentication is successful at dial-in (for modem states dial-in, dial-back, CBCP server, dial-in &amp; dial-on-demand, or dial-back &amp; dial-on-demand), and the name that was authenticated matches the Login/CHAP Host, the site parameters will be used for the remainder of the modem connection.</td>
</tr>
<tr>
<td>CHAP Secret</td>
<td>The CHAP secret associated with this site. If a modem has sites enabled and CHAP authentication enabled, then at dial-in, if the remote server sends a name in the CHAP challenge response that matches the CHAP host of a site, the CHAP secret for the site will be used to authenticate the CHAP challenge response sent by the remote server.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The type of authentication, PAP or CHAP, for which this site is applicable. On dial-in authentication, only sites with the authentication type that matches the authentication type configured for the modem will be used to try to find a matching site.</td>
</tr>
<tr>
<td>Timeout Logins</td>
<td>For text dial-in connections, the connection can time out after the connection is inactive for a specified number of minutes.</td>
</tr>
<tr>
<td>Negotiate IP Address</td>
<td>If the SLB branch office manager and the remote server should negotiate the IP addresses for each side of the PPP connection, select Yes. Select No if the address of the SLB unit (Local IP) and remote server (Remote IP) need to be specified.</td>
</tr>
</tbody>
</table>
| Static Route IP Address | The Static Route IP Address, Subnet Mask and Gateway must be configured for dial-on-demand sites. The SLB device will automatically dial-out and establish a PPP connection when IP traffic destined for the network specified by the static route needs to be sent.  
**Note:** Static Routing must be enabled on the Network - Routing page for dial-on-demand connections. |
| Static Route Subnet Mask | The subnet mask for a dial-on-demand connection. |
| Static Route Gateway | The gateway for a dial-on-demand connection. |
| Dial-out Number | The dial-out number must be specified for dial-on-demand sites. This indicates the phone number to dial when the SLB branch office manager needs to send IP traffic for a dial-on-demand connection. |
| Dial-out Login | User ID for authentication when dialing out to a remote system. May have up to 32 characters. This ID is used for authenticating the SLB unit during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand. |
| Dial-out Password | Enter the password for authentication when dialing out to a remote system. May have up to 64 characters. This password is used for authenticating the SLB unit during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand. |
| Retype Password | Re-enter the password for authentication when dialing out to a remote system. May have up to 64 characters. This password is used for authenticating the SLB branch office manager during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand. |
| Dial-back Number | The phone number to dial on callback for text or PPP dial-back connections. A site must successfully authenticate, have Allow Dial-back enabled and have a Dial-back Number defined in order for the site to be used for callback. |
| Allow Dial-back | If enabled, the site is allowed to be used for dial-back connections. |
| Dial-back Delay | For dial-back and CBCP Server, the number of seconds between the dial-in and dial-out portions of the dialing sequence. |
To view or update a site:

1. In the Sites table, select the site and click the View Site button. The site attributes are displayed in the bottom half of the page.

2. Update any of the site attributes.

3. Click the Edit Site button.

To delete a site:

1. Select the site in the Sites table.

2. Click the Delete Site button.

Configures a set of site-oriented modem parameters that can be activated by various modem-related events (authentication, outbound network traffic for DOD connections, etc.).

The site parameters will override any parameters configured for the modem.

Uses sites with a modem, enable 'usesites'. Sites can be used with the following modem states: dialin, dialback, cbcpserver, dialondemand, dialin+ondemand, and dialback+ondemand.

Site Commands

Go to Site Commands (on page 337) to view CLI commands which correspond to the web page entries described above.

Access Lists

An access list, also known as a white list, is a list of phone numbers that will be granted access during the modem dial-in process. An access list can contain up to 100 phone numbers. This feature requires the Caller ID service be enabled for the phone line by the TelCo provider, and modem Caller ID Logging is enabled with a directive to enable caller ID for the modem in the Caller ID Logging Modem Command. This directive is usually AT+VCID=1 (refer to the AT command set for your modem).

The access list can be configured with two options for responding to a phone number that is not in the access list: hang up the call or ignore the call. If the access list is configured for ignore, the console manager dialing process will wait until the other side of the call hangs up (if the other side
never hangs up, this can result in dial-in access to the console manager being blocked until the administrator resolves this issue).

A maximum of 20 access lists can be created.

To use an access list with a modem, create one or more access lists (described below), then assign the access list to the console manager internal modem or an external USB modem.

**To add an access list:**

1. Click the Devices tab and select the Access Lists option. The Access Lists page displays

   ![Figure 8-22 Devices > Access Lists.](image)

   **Access List Id (view only)** Displays after an access list is created.

   **Access List Name** Enter a name for the access list. Valid characters are letters, numbers, hyphen and underscore. The maximum length is 40 characters.

   **Response** The response to phone numbers that dial-in and are not on the access list: Hang Up or Ignore. If the access list is configured for ignore, the console manager dialing process will wait until the other side of the call hangs up (if the other side never hangs up, this can result in dial-in access to the console manager being blocked until the administrator resolves this issue).

2. In the lower section of the page, enter the following:
   
   **Note:** To clear fields in the lower part of the page, click the Clear Access List button.
To view or update an access list:

1. In the Access Lists table, select the access list and click the View Access List button. The access list attributes are displayed in the bottom half of the page.
2. Update any of the access list attributes.
3. Click the Edit Access List button.

To delete an access list:

1. Select the access list in the Access Lists table.
2. Click the Delete Access List button.

Access List Commands

Go to Access List Commands (on page 266) to view CLI commands which correspond to the web page entries described above.

Modem Dialing States

This section describes the modem states and the options that are used for each modem state. For a description of modem states that can be used with sites, see Sites.

Dial-In

The SLB unit waits for a peer to call the SLB to establish a text (command line) or PPP connection.

- For text connections, the user will be prompted for a login and password, and will be authenticated via the currently enabled authentication methods (Local Users, NIS, LDAP, etc). Once authenticated, a CLI session will be initiated, and the user will remain connected to the SLB unit until they either logout of the CLI session, or (if Timeout Logins is enabled) the CLI session is terminated if it has been idle.

- For PPP connections, the user will be authenticated via PAP or CHAP (configured with the Authentication setting). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the CHAP Handshake Host/User Name and Secret/User Password will be used to authenticate the CHAP Challenge response sent by the PPP peer. If the remote peer requests PAP or CHAP authentication from the SLB unit, the Remote/Dial-out Login and Remote/Dial-out Password will be provided as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the Negotiate IP Address setting). The PPP connection will stay active until no IP traffic is sent for Modern Timeout seconds.
Dial-Out
The SLB unit dials a remote peer to establish a PPP connection. The SLB unit dials the Dial-out Number, and if the remote peer requests PAP or CHAP authentication, provides the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the Negotiate IP Address setting).

Dial-Back
The SLB unit waits for a peer to call the device, establishes a text (command line) or PPP connection, authenticates the user, and if the SLB unit is able to determine a dial-back number to use, hangs up and calls the dial-back number to establish either a text or PPP connection.

- For text connections, the user will be prompted for a login and password, and will be authenticated via the currently enabled authentication methods (Local Users, NIS, LDAP, etc). Once authenticated, the SLB unit will use the Dial-back Number configured for the modem - either a fixed number assigned to the modem, or a number associated with the user that was authenticated (the user must have Allow Dial-back enabled and a Dial-back Number defined). If the SLB unit can determine a dial-back number to use, it will hang up and wait Dial-back Delay seconds before initiating the dial-back. The SLB unit will dial, prompt the user again for a login and password, and a CLI session will be initiated (if the dial-back fails, the SLB unit will try Dial-back Retries times to dial-back). The user will remain connected to the SLB unit until they either logout of the CLI session, or (if Timeout Logins is enabled) the CLI session is terminated if it has been idle.

- Special SLM (Secure Lantronix Management Appliance) Text Dial-back support. When the SLM unit is configured for SLB unit callback support, the SLM dials the SLB. The SLM will provide the callback number in a text string (DIALBACK #) to the modem that the SLM it is currently using. The SLB will hang up and wait Dial-back Delay seconds before initiating the dial-back to the SLM unit using the phone number provided above.

- For PPP connections, the user will be authenticated via PAP or CHAP (configured with the Authentication setting). For PAP, the Local/Remote list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the CHAP Handshake Host/User Name and Secret/User Password will be used to authenticate the CHAP Challenge response sent by the PPP peer. If the remote peer requests PAP or CHAP authentication from the SLB unit, the Remote/Dial-out Login and Remote/Dial-out Password will be provided as authentication tokens. Once authenticated, the SLB unit will use the Dial-back Number configured for the modem - either a fixed number assigned to the modem, or a number associated with the user that was authenticated (the user must have Allow Dial-back enabled and a Dial-back Number defined). If the SLB unit can determine a dial-back number to use, it will hang up and wait Dial-back Delay seconds before initiating the dial-back. The SLB unit will dial, and if the remote peer requests PAP or CHAP authentication, provide the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the Negotiate IP Address setting).

Dial-On-Demand
The SLB unit automatically dials out and establishes a PPP connection when IP traffic destined for a remote network needs to be sent. It will remain connected until no data packets have been sent to the peer for a specified amount of time. The modem cannot be configured for Negotiate IP Address - it must be configured with a Local IP and a Remote IP as the PPP connection will be...
established when it sees IP traffic destined for the Remote IP. When this occurs, the SLB unit dials the Dial-out Number, and if the remote peer requests PAP or CHAP authentication, provides the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, a PPP session will be established using the Local IP and the Remote IP. The PPP connection will stay active until no IP traffic for the Remote IP is sent for Modem Timeout seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least Restart Delay seconds.

Dial-In & Dial-On-Demand

A modem is configured to be in two modes: answering incoming calls to establish a PPP connection, and automatically dialing out to establish a PPP connection when IP traffic destined for a remote network needs to be sent. When either event occurs (an incoming call or IP traffic destined for the remote network), the other mode will be disabled. The modem cannot be configured for Negotiate IP Address - it must be configured with a Local IP and a Remote IP as the PPP connection will be established when it sees IP traffic destined for the Remote IP.

♦ For Dial-in, the user will be authenticated via PAP or CHAP (configured with the Authentication setting). For PAP, the Local/Remote list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the CHAP Handshake Host/User Name and Secret/User Password will be used to authenticate the login and password sent by the PPP peer. If the remote peer requests PAP or CHAP authentication from the SLB unit, the Remote/Dial-out Login and Remote/Dial-out Password will be provided as authentication tokens. Once authenticated, a PPP session will be established using the Local IP and the Remote IP. The PPP connection will stay active until no IP traffic is sent for Modem Timeout seconds.

♦ For Dial-on-Demand, the PPP connection will be established when it sees IP traffic destined for the Remote IP. When this occurs, the SLB unit dials the Dial-out Number, and if the remote peer requests PAP or CHAP authentication, provides the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, a PPP session will be established using the Local IP and the Remote IP. The PPP connection will stay active until no IP traffic for the Remote IP is sent for Modem Timeout seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least Restart Delay seconds.

Dial-Back & Dial-On-Demand

A modem is configured to be in two modes: answering incoming calls to initiate a dial-back, and automatically dialing out to establish a PPP connection when IP traffic destined for a remote network needs to be sent. When either event occurs (an incoming call or IP traffic destined for the remote network), the other mode will be disabled. The modem cannot be configured for Negotiate IP Address - it must be configured with a Local IP and a Remote IP as the PPP connection will be established when it sees IP traffic destined for the Remote IP.

♦ For Dial-back, the user will be authenticated via PAP or CHAP (configured with the Authentication setting). For PAP, the Local/Remote list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the CHAP Handshake Host/User Name and Secret/User Password will be used to authenticate the CHAP Challenge response sent by the PPP peer. If the remote peer requests PAP or CHAP authentication from the SLB unit, the Remote/Dial-out Login and Remote/Dial-out Password will be provided as authentication tokens. Once authenticated, the SLB unit will use the Dial-back Number configured for the modem - either a fixed number assigned to the modem, or a number associated with the user that was authenticated (the user must have Allow Dial-back enabled and a Dial-back Number defined). If the SLB unit can determine a dial-back number to use, it will hang up and wait Dial-back Delay seconds before initiating the dial-back (if the dial-back fails, the SLB unit will try Dial-back Retries times to dial-back). The SLB unit will dial, and if the remote peer requests
PAP or CHAP authentication, provide the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, a PPP session will be established using the Local IP and the Remote IP.

- For Dial-on-Demand, the PPP connection will be established when it sees IP traffic destined for the Remote IP. When this occurs, the SLB dials the Dial-out Number, and if the remote peer requests PAP or CHAP authentication, provides the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, a PPP session will be established using the Local IP and the Remote IP. The PPP connection will stay active until no IP traffic for the Remote IP is sent for Modem Timeout seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least Restart Delay seconds.

Dial-In/Host List

The SLB waits for a peer to call and establishes a text (command line) connection to the first host in a Host List that connects. A host list of a prioritized list of SSH, Telnet or raw TCP hosts to connect to. If Authentication is enabled for the Host List, the user will be prompted for a login and password, and will be authenticated via the currently enabled authentication methods (Local Users, NIS, LDAP, etc). Once authenticated, the SLB will try to connect to each host in the host list until a successful connection is established.

CBCP Server and CBCP Client

Callback Control Protocol (CBCP) is a PPP option that negotiates the use of callback where the server, after authenticating the client, terminates the connection and calls the client back at a phone number that is determined by the CBCP handshake. For more information on CBCP, see http://technet.microsoft.com/en-us/library/cc957979.aspx. CBCP is used primarily by Microsoft PPP peers. CBCP supports two options for determining the number to dial on callback: the client can specify a user-defined number for the server to dial on callback, or the client can request the server use an administrator-defined number to dial on callback. Optionally, some servers may also allow "no callback" as an option.

CBCP Server

The SLB unit waits for a client to call the it, establish a PPP connection, authenticate the user, and negotiate a dial-back number with the client using CBCP. If the SLB unit is able to determine a dial-back number to use, it hangs up and calls the dial-back number.

When a call is received, a PPP connection is established, and the user will be authenticated via PAP or CHAP (configured with the Authentication setting). For PAP, the Local/Remote list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the CHAP Handshake Host/User Name and Secret/User Password will be used to authenticate CHAP Challenge response sent by the PPP peer. If the remote peer requests PAP or CHAP authentication from the SLB unit, the Remote/Dial-out Login and Remote/Dial-out Password will be provided as authentication tokens. Once authenticated, the CBCP handshake with the client determines the number to use for dial-back. The SLB unit will present the client with the available options: if the authenticated user is a Local/Remote User with Allow Dial-back enabled and a Dial-back Number defined, the administrator-defined option is allowed; if this is not the case, the user-defined number is allowed. Additionally, if CBCP Server Allow No Callback is enabled, the client can also select no callback (the PPP connection established at dial-in will remain up). The client will select from the available callback options. If the SLB unit can determine a dial-back number to use, it will hang up and wait Dial-back Delay seconds before initiating the dial-back (if the dial-back fails, the SLB will try Dial-back Retries times to dial-back). The SLB unit will call back the previously authenticated remote peer, and if the remote peer requests PAP or CHAP
authentication, provide the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the Negotiate IP Address setting).

**CBCP Client**

The SLB unit will dial out to a CBCP server, establish a PPP connection, negotiate a callback number with the server using CBCP, terminate the connection, and wait for the server to call back. The SLB unit dials the Dial-out Number, and if the remote peer requests PAP or CHAP authentication, provides the Remote/Dial-out Login and Remote/Dial-out Password as authentication tokens. Once authenticated, the CBCP handshake with the server determines the number to use for dial-back. The SLB unit will request the type of number defined by CBCP Client Type - either an Admin-defined Number (the CBCP server determines the number to call) or a User-defined Number (the SLB unit will provide the Fixed Dial-back Number as the number to call). If the CBCP handshake is successful, the SLB unit will terminate the PPP connection, hang up, and wait for the server to dial back. When the remote server calls back the SLB unit and the PPP connection is established, the user will be authenticated via PAP or CHAP (configured with the Authentication setting). For PAP, the Local/Remote list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the CHAP Handshake Host/User Name and Secret/User Password will be used to authenticate CHAP Challenge response sent by the PPP peer. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the Negotiate IP Address setting).

**Notes:**

- In a state where the modem will be answering a call, the modem should always be configured for manual answer, not auto answer.
- When answering a call, the SLB unit answers after the 2nd ring.
- Any text or PPP connection can be terminated by setting the modem state to disabled.
9: **USB Port**

This chapter describes how to configure storage (thumb drive), USB modems and USB serial devices by using the Devices > USB Ports page and CLI. The thumb drive is useful for saving and restoring configurations and for device port logging. See Device Port Settings (on page 119).

This chapter describes the Web Manager pages and available CLI commands that configure the USB port. This chapter contains the following sections:

- **USB Storage**
- **USB Modem Settings**
- **USB Serial Settings**

**USB Storage**

The Devices > USB Ports page has an USB Access checkbox. USB Access is a security feature ensures that access to any USB device is disabled if the box is unchecked. The SLB unit ignores any USB device plugged into the port.

**To set up USB storage in the SLB branch office manager:**

1. Insert any of the supported thumb drives into the USB port on the front of the SLB branch office manager. You can do this before or after powering up the SLB. If the first partition on the thumb drive is formatted with a file system supported by the SLB unit (ext2, FAT16, or FAT32), the card mounts automatically.

2. Log into the SLB branch office manager and click **Devices**.

3. Click **USB**. Figure 9-1 shows the page that displays. Your USB device should display in Port U1 if you have inserted it. If it does not display and you have inserted it, refresh the web page.

4. View the USB card information and options available on the page:

<table>
<thead>
<tr>
<th><strong>Port (view only)</strong></th>
<th>Port on the SLB unit where the USB device is inserted.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device (view only)</strong></td>
<td>Type of USB device (modem, serial, or storage).</td>
</tr>
<tr>
<td><strong>Type (view only)</strong></td>
<td>Information read from USB device.</td>
</tr>
<tr>
<td><strong>State (view only)</strong></td>
<td>Indicates if the device is mounted, and if mounted, how much space is available.</td>
</tr>
<tr>
<td><strong>USB Access (check box)</strong></td>
<td>Check to enable USB Access. Uncheck to disable USB access.</td>
</tr>
</tbody>
</table>
To configure the USB storage port, from the USB Ports table:

1. Click the radio button (on the far right) for a USB port.
2. Click Configure. Figure 9-2 shows the page that displays if a USB storage device is inserted in the selected port.

Figure 9-2  Devices > USB > USB - Storage

Port: U1
Device: Storage
Type: Manufacturer=USB 2.0 Product=Flash Disk
SerialNumber=05222000D668B202
State: fat16, mounted, Size/Used/Avail 32M/10M/22N

Mount: □
Unmount: □
Format: □
Ext2  □  FAT16  □  FAT32

Filesystem Check: □
Manage Files on Thumb Drive

Apply
3. Enter the following fields.

<table>
<thead>
<tr>
<th>Mount</th>
<th>Enables the first partition of the USB device (if not currently mounted). Once mounted, a device is used for device port logging and saving/restoring configurations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmount</td>
<td>Enables ejecting the USB device.</td>
</tr>
<tr>
<td><strong>Warning:</strong></td>
<td><em>If you eject a USB device from the SLB branch office manager without unmounting it, subsequent mounts may fail, and you will need to reboot the SLB unit to restore the functionality.</em></td>
</tr>
<tr>
<td>Format</td>
<td>Select to:</td>
</tr>
<tr>
<td></td>
<td>♦ Unmount the USB device (if it is mounted)</td>
</tr>
<tr>
<td></td>
<td>♦ Remove all existing partitions</td>
</tr>
<tr>
<td></td>
<td>♦ Create one partition</td>
</tr>
<tr>
<td></td>
<td>♦ Format it with the selected file system (ext2 or FAT)</td>
</tr>
<tr>
<td></td>
<td>♦ Mount the USB device</td>
</tr>
<tr>
<td>Filesystem</td>
<td>Select <strong>Ext2</strong> or a <strong>FAT</strong> file system the SLB branch office manager supports.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.

**Manage Firmware and Configuration Files**

To manage any firmware and configuration files stored on a USB thumb drive, perform the following steps.

1. Click the **Manage Files on the Thumb Drive** link on the *Devices > USB > USB - Storage* page.
2. To delete a file, click the check box next to the filename and click **Delete File**. A confirmation message displays.

3. To download a file, click the **Download File** button. Select the file from the list.

4. To rename a file, click the check box next to the filename and enter a new name in the **New File Name** field.

5. Click **Rename File**.

**USB Modem Settings**

*To enter modem settings for a USB:*

1. Insert any of the supported USB modem devices into the USB port on the front of the SLB unit. You can do this before or after powering up the console manager.

2. Log into the SLB unit and click **Devices**.

3. Click **USB**.

4. Select the USB device you want to configure from the USB Ports table and click **Configure**. *Figure 9-4* shows the page that displays if a USB modem is inserted in Port U1, or if Port U2 is selected.
Figure 9-4 Devices > USB > USB - Modem

USB - Modem

- Port: U2
- Device: Modem
- Type: Internal
- State: N/A

Note: Dial-out GPRS connections may replace the default route and DNS entries. Static Routes may be required to maintain access to subnets that are not directly attached to the SLB.

Data Settings
- Baud: 115200
- Data Bits: 8
- Parity: none
- Stop Bits: 1
- Flow Control: RTS/CTS

GSM/GPRS Settings
- Dial-out Mode: GPRS
- PIN: [field]
- Retype PIN: [field]
- PPP Compression: [field]
- Auto-configure DNS: [field]
- Negotiated IP: N/A
- GPRS Context: AT+CGDCONT=1,"IP","[Access]
- GSM Bearer Svc: AT+CBST=7,0

Modem Statistics
- Tx bytes: N/A
- Rx bytes: N/A

Ask questions or need further assistance? Please reach out to our support team at support@sample.com.
5. Enter the following fields.

**Data Settings**

*Note: Check the modem’s equipment settings and documentation for the proper settings. The attached modem must have the same settings.*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud</td>
<td>The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate.</td>
</tr>
<tr>
<td>Data Bits</td>
<td>Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is 8 data bits.</td>
</tr>
<tr>
<td>Parity</td>
<td>Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none.</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is 1.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>A method of preventing buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is none.</td>
</tr>
</tbody>
</table>

**GSM/GPRS Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial-out Mode</td>
<td>Select either GPRS or GSM (Global System for Mobile communication) as the type of dial-out connection.</td>
</tr>
<tr>
<td>PIN</td>
<td>Enter PIN (personal identification number) for accessing the GSM/GPRS card.</td>
</tr>
<tr>
<td>Retype PIN</td>
<td>Re-enter PIN (personal identification number) for accessing the GSM/GPRS card.</td>
</tr>
<tr>
<td>PPP Compression</td>
<td>Select to enable negotiation of data compression over PPP links. Disabled by default.</td>
</tr>
<tr>
<td>Auto-acquire DNS</td>
<td>Select to enable the SLB branch office manager to acquire up to three DNS servers by means of GPRS (General Packet Radio Service). Enabled by default.</td>
</tr>
<tr>
<td>Negotiated IP</td>
<td>IP address associated with the GPRS connection.</td>
</tr>
<tr>
<td>GPRS Context</td>
<td>Command to specify the protocol data packet (PDP) context parameter values.</td>
</tr>
<tr>
<td>GSM Bearer Svc</td>
<td>Command to select the bearer service, data rate, and connection element to use when data call originate.</td>
</tr>
</tbody>
</table>

**Modem Settings**

*Note: Depending on the State and Mode you select, different fields are available.*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Indicates whether an external modem is attached to the device port. If enabling, set the modem to dial-out, dial-in, dial-back, dial-on-demand, dial-in/host list, or dial in &amp; dial-on-demand. Disabled by default.</td>
</tr>
</tbody>
</table>
### Mode

The format in which the data flows back and forth:
- **Text**: In this mode, the SLB unit assumes that the modem will be used for remotely logging into the command line. Text mode can only be used for dialing in or dialing back. **Text** is the default.
- **PPP**: This mode establishes an IP-based link over the modem. PPP connections can be used in dial-out mode (e.g., the SLB unit connects to an external network), dial-in mode (e.g., the external computer connects to the network that the SLB branch office manager is part of), dial-back (dial-in followed by dial-out), CBCP server and CBCP client.

### Use Sites

Enables the use of site-oriented modem parameters which can be activated by various modem-related events (authentication, outbound network traffic for dial-on-demand connections, etc.). Sites can be used with the following modem states: dial-in, dial-back, dial-on-demand, dial-in & dial-on-demand, dial-back & dial-on-demand, and CBCP server.

For more information, see [Sites on page 169](#).

### Group Access

If undefined, any group can access the modem (text login only). If one or more groups are specified (groups are delimited by the characters ‘ ’ (space), ‘,’ (comma), or ‘;’ (semicolon)), then any user who logs into the modem must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the SLB. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ‘ ’ (space), ‘,’ (comma), ‘;’ (semicolon), or ‘=’ (equals) - for example "group=group1,group2;" or "group1,group2,group3".

### Initialization Script

Commands sent to configure the modem may have up to 100 characters. Consult your modem’s documentation for recommended initialization options. If you do not specify an initialization script, the SLB unit uses a default initialization string of `AT S7=45  SO=0  L1  V1  X4  &D2  &c1  E1  Q0`.

**Note:** We recommend that the modem initialization script always be preceded with `AT` and include `E1  V1  X4  Q0` so that the SLB unit may properly control the modem.

### Modem Timeout

Timeout for all modem connections. Select **Yes** (default) for the SLB branch office manager to terminate the connection if no traffic is received during the configured idle time. Enter a value of from 1 to 9999 seconds. The default is 30 seconds.

### Check Dial Tone

If enabled, the SLB branch office manager will periodically check the modem for a dial tone while waiting for a dial in (i.e., if the Modem State is set to Dial-in, or if the Modem State is set to Dial-back and the SLB unit is in the Dial-in portion of the sequence). The SLB unit can issue a trap or an event can be setup to notify the user if no dial tone is detected. Enabled by default (every 15 minutes).

### Caller ID Logging

Select to enable the SLB unit to log caller IDs on incoming calls. Disabled by default.

**Note:** For the Caller ID `AT` command, refer to the modem user guide.

### Modem Command

Modem `AT` command used to initiate caller ID logging by the modem.

**Note:** For the `AT` command, refer to the modem user guide.
Dial-back Number: Users with dial-back access can dial into the SLB unit and enter their login and password. Once the SLB branch office manager authenticates them, the modem hangs up and dials them back. Select the phone number the modem dials back on—a fixed number or a number associated with their login. If you select Fixed Number, enter the number (in the format 2123456789). The dial-back number is also used for CBCP client as the number for a user-defined number. See Device Ports - Settings (on page 117) for more information.

Dial-back Delay: For dial-back and CBCP Server, the number of seconds between the dial-in and dial-out portions of the dialing sequence.

Dial-back Retries: Specify the number of times to retry dialing back.

Access List: For the dial-in state, a modem access list (or white list) that defines which phone numbers will be granted access to the console manager. See Access Lists for more information.

Text Mode

Timeout Logins: If you selected Text mode, you can enable logins to time out after the connection is inactive for a specified number of minutes. The default is No. This setting is only applicable for text mode connections. PPP mode connections stay connected until either side drops the connection. Disabled by default.

Dial-in Host List: From the drop-down list, select the desired host list. The host list is a prioritized list of SSH, Telnet, and TCP hosts that are available for establishing outgoing modem connections or for connect direct at the CLI. The hosts in the list are cycled through until the SLB branch office manager successfully connects to one. To establish and configure host lists, click the Host Lists link. See Host Lists on page 136.

PPP Mode

Negotiate IP Address: If the SLB unit and/or the serial device have dynamic IP addresses (e.g., IP addresses assigned by a DHCP server), select Yes. Yes is the default. If the SLB unit or the modem have fixed IP addresses, select No, and enter the Local IP (IP address of the port) and Remote IP (IP address of the modem).

Authentication: Enables PAP or CHAP authentication for modem logins. PAP is the default. With PAP, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With CHAP, the CHAP Handshake fields authenticate the user.

CHAP Handshake: The Host/User Name (for UNIX systems) or Secret/User Password (for Windows systems) used for CHAP authentication. May have up to 128 characters.

CHAP Auth Uses: For CHAP authentication, determines what is used to validate the CHAP host/user sent by the remote peer: either the CHAP Host defined for the modem, or any of the users in the Local Users list.

Same authentication for Dial-in & Dial-on-Demand (DOD): Select this option to let incoming connections (dial-in) use the same authentication settings as outgoing connections (dial-on-demand). If this option is not selected, then the dial-on-demand connections take their authentication settings from the DOD parameter settings. If DOD Authentication is PAP, then the DOD CHAP Handshake field is not used.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOD Authentication</strong></td>
<td>Enables <strong>PAP</strong> or <strong>CHAP</strong> authentication for dial-in &amp; dial-on-demand. <strong>PAP</strong> is the default. With <strong>PAP</strong>, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With <strong>CHAP</strong>, the DOD CHAP Handshake fields authenticate the user.</td>
</tr>
<tr>
<td><strong>DOD CHAP Handshake</strong></td>
<td>For <strong>DOD Authentication</strong>, enter the <strong>Host/User Name</strong> for UNIX systems) or <strong>Secret/User Password</strong> (for Windows systems) used for CHAP authentication. May have up to 128 characters.</td>
</tr>
<tr>
<td><strong>Enable NAT</strong></td>
<td>Select to enable Network Address Translation (NAT) for dial-in and dial-out PPP connections on a per modem (device port or USB port) basis. Users dialing into the SLB unit access the network connected to Eth1 and/or Eth2.</td>
</tr>
<tr>
<td><strong>Dial-out Number</strong></td>
<td>Phone number for dialing out to a remote system or serial device. May have up to 20 characters. Any format is acceptable.</td>
</tr>
<tr>
<td><strong>Remote/Dial-out Login</strong></td>
<td>User ID for dialing out to a remote system. May have up to 32 characters.</td>
</tr>
<tr>
<td><strong>Remote/Dial-out Pwd</strong></td>
<td>Enter password for dialing out to a remote system. May have up to 64 characters.</td>
</tr>
<tr>
<td><strong>Retype</strong></td>
<td>Re-enter password for dialing out to a remote system. May have up to 64 characters.</td>
</tr>
<tr>
<td><strong>Restart Delay</strong></td>
<td>The number of seconds after the timeout and before the SLB branch office manager attempts another connection. The default is 30 seconds.</td>
</tr>
<tr>
<td><strong>CBCP Server Allow No Callback</strong></td>
<td>For CBCP Server state, allows &quot;No Callback&quot; as an option in the CBCP handshake in addition to User-defined Number and Admin-defined Number.</td>
</tr>
<tr>
<td><strong>CBCP Client Type</strong></td>
<td>For CBCP Client, this selects the number that the client would like to use for callback - either a user-defined number passed to the server (specified by the Fixed Dial-back Number) or an administrator-defined number determined by the server based on the login that is PAP or CHAP authenticated.</td>
</tr>
</tbody>
</table>

**IP Settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service</strong></td>
<td>The available connection services for this modem port (Telnet, SSH, or TCP). Only one can be active at a time. The default is None.</td>
</tr>
</tbody>
</table>
| **Telnet Port**          | Telnet Port Telnet session port number to use if you selected Telnet.  Defaults:  
  - USB Port U1: 2049  
  - USB Port U2: 2050  
  - Range: 1025-65535 |
| **SSH Port**             | The SSH session port number to use if you selected SSH.  Defaults:  
  - USB Port U1: 3049  
  - USB Port U2: 3050  
  - Range: 1025-65535 |
| **TCP Port**             | The TCP (raw) session port number to use if you selected TCP.  Defaults:  
  - USB Port U1: 4049  
  - USB Port U2: 4050  
  - Range: 1025-65535 |
| **Authenticate (checkbox)** | If selected, the SLB unit requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet Port** and **SSH Port**, but not for **TCP Port**. |
6. Click **Apply**.

**USB Serial Settings**

The SLB supports connecting USB serial devices to the front USB ports. A user can interact with the device by logging into the CLI and performing a **connect direct** to the USB port, or by establishing a SSH, Telnet or TCP connection to the USB port. A maximum of 3 concurrent sessions to the port are allowed.

**To enter serial settings for a USB:**

1. Insert any of the supported USB serial devices into the USB port on the front of the SLB unit. You can do this before or after powering up the console manager.

2. Log into the SLB unit and click **Devices**.

3. Click **USB / SD Card**. *Figure 9-5* shows the page that displays. Your USB device should display in the appropriate row of the USB ports / SD card table if you have inserted it. If it does not display and you have inserted it, refresh the web page.

**Figure 9-5 Devices > USB Ports**

4. Select the USB device you want to configure from the USB Ports table and click the **Configure** button. *Figure 9-6* shows the page that displays if a USB serial device is inserted in Port U1.
5. Complete or view the following sections:

**Data Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Baud</strong></td>
<td>The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so this is the default. Check the equipment settings and documentation for the proper baud rate.</td>
</tr>
<tr>
<td><strong>Parity</strong></td>
<td>Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none.</td>
</tr>
<tr>
<td><strong>Flow Control</strong></td>
<td>A method of preventing buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is none.</td>
</tr>
<tr>
<td><strong>Data Bits</strong></td>
<td>Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is 8 data bits.</td>
</tr>
<tr>
<td><strong>Stop Bits</strong></td>
<td>The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is 1.</td>
</tr>
</tbody>
</table>
**IP Settings**

<table>
<thead>
<tr>
<th>Service</th>
<th>The available connection services for this USB Port (Telnet, SSH, or TCP). Only one can be active at a time. The default is None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet Port</td>
<td>Telnet Port Telnet session port number to use if you selected Telnet. Defaults: USB Port U1: <strong>2049</strong> • Range: <strong>1025-65535</strong></td>
</tr>
<tr>
<td>SSH Port</td>
<td>The SSH session port number to use if you selected SSH. Defaults: USB Port U1: <strong>3049</strong> • Range: <strong>1025-65535</strong></td>
</tr>
<tr>
<td>TCP Port</td>
<td>The TCP (raw) session port number to use if you selected TCP. Defaults: USB Port U1: <strong>4049</strong> • Range: <strong>1025-65535</strong></td>
</tr>
<tr>
<td>Authenticate</td>
<td>If selected, the console manager requires user authentication before granting access to the port. Authenticate is selected by default for Telnet Port and SSH Port, but not for TCP Port.</td>
</tr>
</tbody>
</table>

6. To save settings for just this port, click **Apply**.

**USB Commands**

Go to [USB Access Commands](#), [USB Storage Commands](#), [USB Modem Commands](#), and [USB Serial Commands](#), to view CLI commands which correspond to the web page entries described above.
10: Connections

Chapter 8: Device Ports described how to configure and interact with an SLB device port connected to an external device. This chapter describes how to use the Devices > Connections page to connect external devices and outbound network connections (such as Telnet or SSH) in various configurations.

An SLB device port attached to an external device can be connected to one of the following endpoints:

- Another device port attached to an external device
- Another device port with a modem attached
- An outgoing Telnet or SSH session
- An outgoing TCP or UDP network connection

This enables the user to set up connections such as those described in the next section. You can establish a connection at various times:

- Immediately. These connections are always re-established after reboot.
- At a specified date and time. These connections connect if the date and time have already passed.
- After a specified amount of data or a specified sequence of data passes through the connection. Following reboot, the connection is not re-established until the specified data passes through the connection.

Typical Setup Scenarios for the SLB

Following are typical configurations in which SLB connections can be used, with references to settings on the Devices > Connections and Device Ports > Settings web pages.

Terminal Server

In this setup, the SLB branch office manager acts as a multiplexer of serial data to a single server computer. Terminal devices are connected to the serial ports of the SLB and configured as a Device Port to Telnet out type connection on the Devices > Connections page. The users of the terminals can access the server as if they were connected directly to it by local serial ports or a console.
Remote Access Server

In this setup, the SLB unit is connected to one or more modems by its device ports. Configure the device ports on the Device Ports > Settings web page by selecting the Dial-in option in the Modem Settings section. Most customers use the modems in PPP mode to establish an IP connection to the SLB branch office manager and either Telnet or SSH into the SLB unit. They could also select text mode where, using a terminal emulation program, a user could dial into the SLB unit and connect to the command line interface.

Reverse Terminal Server

In this scenario, the SLB branch office manager has one or more device ports connected to one or more serial ports of a mainframe server. Users can access a terminal session by establishing a Telnet or SSH session to the SLB unit. To configure the SLB unit, select the Enable Telnet In or Enable SSH In option on the Device Ports > Settings page.
Multiport Device Server
A PC can use the device ports on the SLB branch office manager as virtual serial ports, enabling the ports to act as if they are local ports to the PC. To use the SLB unit in this setup, the PC requires special software, for example, Com Port Redirector (available on www.lantronix.com) or similar software.

Console Server
For this situation, the SLB unit is configured so that the user can manage a number of servers or pieces of network equipment using their console ports. The device ports on the SLB branch office manager are connected to the console ports of the equipment that the user would like to manage. To manage a specific piece of equipment, the user can Telnet or SSH to a specific port or IP address on the SLB unit and be connected directly to the console port of the end server or device. To configure this setup, set the Enable Telnet In or Enable SSH In option on the Device Ports > Settings page for the device port in question. The user can implement an extra remote management capability by adding a modem to one of the device ports and setting the Dial-in option in the Modem Settings section of the Device Ports > Settings page. A user could then dial into the SLB unit using another modem and terminal emulation program at a remote location.
Connection Configuration

To create a connection:

1. Click the **Devices** tab and select the **Connections** option. The following page displays:

![Figure 10-5 Devices > Connections](image)

- **Outgoing Connection Timeout**: Select to turn on or turn off the connection timeout:
  - No for no timeout
  - Yes for a timeout. Specify the number of seconds in the seconds field.

- **Port**: The number of the device port you are connecting.
  - This device port must be connected to an external serial device and must not have command line interface logins enabled, be connected to a modem, or be running a loopback test.
  - To see the current settings for this device port, click the **Settings** link.

- **Data Flow**: Select the arrow showing the direction (bidirectional or unidirectional) the data will flow in relationship to the device port you are connecting.

2. For a device port, enter the following:

   - **Outgoing Connection Timeout**: Select to turn on or turn off the connection timeout:
     - No for no timeout
     - Yes for a timeout. Specify the number of seconds in the seconds field.

   - **Port**: The number of the device port you are connecting.
     - This device port must be connected to an external serial device and must not have command line interface logins enabled, be connected to a modem, or be running a loopback test.
     - **Note**: To see the current settings for this device port, click the **Settings** link.

   - **Data Flow**: Select the arrow showing the direction (bidirectional or unidirectional) the data will flow in relationship to the device port you are connecting.
To view, update, or disconnect a current connection:

The bottom of the Current Connections page displays current connections.

**Figure 10-6 Current Connections**

<table>
<thead>
<tr>
<th>Current Connections</th>
<th>Configure</th>
<th>Terminate</th>
<th>Keep Connection:</th>
<th>Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port/Service</td>
<td>Flow</td>
<td>Port/Service</td>
<td>User</td>
<td>Time</td>
</tr>
<tr>
<td>Console Port</td>
<td>Command Line</td>
<td>N/A</td>
<td>69:48:45</td>
<td></td>
</tr>
</tbody>
</table>

1. To view details about a connection, hold the mouse over the arrow icon in the Flow column.
2. To disconnect (delete) a connection, select the connection in the check box column and click the Terminate button.
3. To update (reconfigure) a connection, select the connection in the check box column, modify the attributes and click the Configure button.
4. To re-establish the connection, create the connection again in the top part of the page.
5. To re-establish a connection that has been suspended, select the connection and click the Restart button.

6. To view information about Web connections, click the here link in the text above the table. The Maintenance > Firmware & Configurations page displays.

**Connection Commands**

Go to [Connection Commands (on page 294)](#) to view CLI commands which correspond to the web page entries described above.
11: User Authentication

Users who attempt to log in to the SLB branch office manager by means of Telnet, SSH, the console port, or one of the device ports are granted access by one or more authentication methods.

The User Authentication page provides a submenu of methods (Local Users, NIS, LDAP, RADIUS, Kerberos, and TACACS+) for authenticating users attempting to log in. Use this page to assign the order in which the SLB unit will use the methods. By default, local user authentication is enabled and is the first method the SLB unit uses to authenticate users. If desired, you can disable local user authentication or assign it a lower precedence.

**Note:** Regardless of whether local user authentication is enabled, the local user sysadmin account is always available for login. For security purposes, full administrative access to the SLB via the default sysadmin local user account can be limited to only the front console port of the SLB unit. See Limiting Sysadmin User Access (on page 45).

Authentication can occur using all methods, in the order of precedence, until a successful authentication is obtained, or using only the first authentication method that responds (in the event that a server is down).

If you have the same user name defined in multiple authentication methods, the result is unknown.

**Example:**
There is an LDAP user "joe" and an NIS user "joe" and the order of authentication methods is:

1. Local Users
2. LDAP
3. NIS

User "joe" tries to log in. Because there is an LDAP user "joe," the SLB branch office manager tries to authenticate him against his LDAP password first. If he fails to log in, then the SLB unit may (or may not) try to authenticate him against his NIS "joe" user password.
To enable, disable, and set the precedence of authentication methods:

1. From the main menu, select **User Authentication**. The following page displays:

   ![User Authentication > Authentication Methods](image)

   **Figure 11-1 User Authentication > Authentication Methods**

2. To enable a method currently in the **Disabled methods** list, select the method and press the left arrow to the left of the list. The methods include:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NIS</strong> (Network Information System)</td>
<td>A network naming and administration system developed by Sun Microsystems for smaller networks. Each host client or server computer in the system has knowledge about the entire system. A user at any host can access files or applications on any host in the network with a single user identification and password. NIS uses the client/server model and the Remote Procedure Call (RPC) interface for communication between hosts. NIS consists of a server, a library of client programs, and some administrative tools. NIS is often used with the Network File System (NFS).</td>
</tr>
<tr>
<td><strong>LDAP</strong> (Lightweight Directory Access Protocol)</td>
<td>A set of protocols for accessing information directories, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services.</td>
</tr>
<tr>
<td><strong>RADIUS</strong> (Remote Authentication Dial-In User Service)</td>
<td>An authentication and accounting system used by many Internet Service Providers (ISPs). A client/server protocol, it enables remote access servers to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It increases security, allowing a company to set up a policy that can be applied at a single administered network point.</td>
</tr>
</tbody>
</table>
3. To disable a method currently in the **Enabled methods** list, select the method and click the right ➡️ arrow between the lists.

4. To set the order in which the SLB branch office manager will authenticate users, use the up ⬆️ and down ⬇️ arrows to the left of the **Enabled methods** list.

5. For **Attempt next method on authentication rejection**, you have the following options:
   - To enable the SLB unit to use all methods, in order of precedence, until it obtains a successful authentication, select the check box. This is the default.
   - To enable the SLB unit to use only the first authentication method that responds (in case a server is down or unavailable), clear the check box.

6. Click **Apply**.

Now that you have enabled one or more authentication methods, you must configure them.

### Authentication Commands

Go to *Authentication Commands (on page 278)* to view CLI commands which correspond to the web page entries described above.
Local and Remote User Settings

The system administrator can configure the SLB branch office manager to use local accounts and remote accounts to authenticate users.

1. Click the **User Authentication** tab and select the **Local/Remote Users** option. The following page displays.

![Figure 11-2 User Authentication > Local/Remote Users](image)

The top of the page has entry fields for enabling local and remote users and for setting password requirements. The bottom of the page displays a table listing and describing all local and remote users.

**To enable local and/or remote users:**

2. Enter the following:

<table>
<thead>
<tr>
<th>Enable Local Users</th>
<th>Select to enable all local users except sysadmin. The sysadmin is always available regardless of how you set the check box. Enabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Sysadmin Web Logins</td>
<td>Select to allow the sysadmin to have multiple simultaneous logins to the web interface. Disabled by default.</td>
</tr>
<tr>
<td>Sysadmin Access Limited to Console Port</td>
<td>Select to limit sysadmin logins to the physical SLB Console Port only. Disabled by default. <strong>Note:</strong> For security purposes, full administrative access to the SLB via the default sysadmin local user account can be limited to only the front console port of the SLB unit. See Limiting Sysadmin User Access (on page 45).</td>
</tr>
</tbody>
</table>
Authenticate only remote users who are in the remote users list

Select the check box to authenticate users listed in the Remote Users list in the lower part of the page. Disabled by default.

3. Continue to set Local User Passwords:

Complex Passwords

Select to enable the SLB unit to enforce rules concerning the password structure (e.g., alphanumeric requirements, number of characters, punctuation marks). Disabled by default.

Complexity rules:

Passwords must be at least eight characters long.

They must contain one upper case letter (A-Z), one lower case letter (a-z), one digit (0-9), and one punctuation character ( !(@#$%^&*-+=\[]:;"'<>,.?/_).

Allow Reuse

Select to enable users to continue to reuse old passwords. If you disable the check box, they cannot use any of the Reuse History number of passwords. Enabled by default.

Reuse History

The number of passwords the user must use before reusing an old password. The default is 4.

For example, if you set reuse history to 4, the user may reuse an old password after using 4 other passwords.

Password Lifetime (days)

The number of days until the password expires. The default setting is 90.

Warning Period (days)

The number of days ahead that the system warns that the user's password will expire. The default setting is 7.

Max Login Attempts

The number of times (up to 8) the user can attempt to log in unsuccessfully before the system locks the user out. The default setting is 0 (disabled).

Lockout Period (minutes)

The number of minutes (up to 90) the locked-out user must wait before trying to log in to the web interface again. The default setting is 0 (disabled).

4. Click the Apply button.

Sysadmin Account Default Login Values

On factory default SLB units, the local user sysadmin account has the following default login values.

SLB units manufactured after the release of SLB firmware 7.0.0.0:

username: sysadmin

password: the last 8 characters of the Device ID (ConsoleFlow ID). If the Device ID is not set, the password is the last 8 characters of the serial number.

SLB units manufactured before the release of SLB firmware 7.0.0.0:

username: sysadmin

password: PASS

If you don’t know when the SLB unit was manufactured, you can do the following to identify whether the device-unique sysadmin password is supported and enabled on the SLB hardware. View the About SLB page or run the CLI admin version command and look for the following in the result: Admin Password Unique to Device: enabled (or disabled). If that string is absent from the result or the result is set to “disabled”, it indicates that the device doesn’t support the device-unique sysadmin password.
**Note:** It is recommended that you change the default password on initial setup. The sysadmin password and the front panel (LCD) Factory Default password should be recorded and stored in a secure place accessible by at least two authorized system administrators. Recovering an SLB if both of these passwords are unknown is cumbersome and time consuming. To change the sysadmin password, see the next topic Adding, Editing or Deleting a User.

To restore the SLB unit to factory default, see *Firmware & Configurations on page 237.*

**Adding, Editing or Deleting a User**

Through this User Authentication > Local/Remote Users page, you can delete a user listed in the table or open a page for adding or editing a user.

*To add a user:*

2. Enter the following information for the user:

<table>
<thead>
<tr>
<th>Login</th>
<th>User ID of selected user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Select the type of authenticated user:</td>
</tr>
<tr>
<td></td>
<td>◆ Local: User listed in the SLB database.</td>
</tr>
<tr>
<td></td>
<td>◆ Remote: User not listed in the SLB database.</td>
</tr>
<tr>
<td>UID</td>
<td>A unique numeric identifier the system administrator assigns to each user. Valid UIDs are 101-4294967295.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The UID must be unique. If it is not, SLB branch office manager automatically increments it. Starting at 101, the SLB unit finds the next unused UID.</td>
</tr>
<tr>
<td>Listen Ports</td>
<td>The device ports that the user may access to view data using the connect listen command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15).</td>
</tr>
<tr>
<td>Data Ports</td>
<td>The device ports with which the user may interact using the connect direct command. Enter the port numbers or the range of port numbers.</td>
</tr>
<tr>
<td>Clear Port Buffers</td>
<td>The device port buffers the users may clear using the set locallog clear command. Enter the port numbers or the range of port numbers.</td>
</tr>
<tr>
<td>Access Outlets</td>
<td>The outlets the user may monitor and configure.</td>
</tr>
</tbody>
</table>
### 11: User Authentication

<table>
<thead>
<tr>
<th>Enable for Dial-back</th>
<th>Select to grant a local user dial-back access. Users with dial-back access can dial into the SLB branch office manager and enter their login and password. Once the SLB unit authenticates them, the modem hangs up and dials them back. Disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial-back Number</td>
<td>The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number (specified on the Device Port - Settings page), or on a number that is associated with the user’s login (specified here).</td>
</tr>
<tr>
<td>Escape Sequence</td>
<td>A single character or a two-character sequence that causes the SLB unit to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is <code>Esc+A</code> (escape key, then uppercase “A” performed quickly but not simultaneously). You would specify this value as <code>\x1bA</code>, which is hexadecimal (<code>\x</code>) character 27 (1B) followed by an A. This setting allows the user to terminate the <code>connect direct</code> command on the command line interface when the endpoint of the command is deviceport, tcp, or udp.</td>
</tr>
<tr>
<td>Break Sequence</td>
<td>A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is <code>Esc+B</code> (escape key, then uppercase “B” performed quickly but not simultaneously). You would specify this value as <code>\x1bB</code>, which is hexadecimal (<code>\x</code>) character 27 (1B) followed by a B.</td>
</tr>
<tr>
<td>Custom Menu</td>
<td>If custom menus have been created, you can assign a default custom menu to the user. The custom menu will display at login. <em>Note: In the Local Users table, if the menu assigned to a local user no longer exists, it is marked with an asterisk (</em>).*</td>
</tr>
<tr>
<td>Display Menu at Login</td>
<td>If custom menus have been created, select to enable the menu to display when the user logs into the CLI.</td>
</tr>
<tr>
<td>Password / Retype Password</td>
<td>When a user logs into the SLB branch office manager, the SLB unit prompts for a password (up to 64 characters). The sysadmin establishes that password here.</td>
</tr>
<tr>
<td>Password Expires</td>
<td>If not selected, allows the user to keep a password indefinitely. If selected the user keeps the password for a set period. (See the section, Local and Remote User Settings (on page 199) for information on specifying the length of time before the password expires.)</td>
</tr>
<tr>
<td>Allow Password Change</td>
<td>Select to allow the user to change password.</td>
</tr>
<tr>
<td>Change Password on Next Login</td>
<td>Indicate whether the user must change the password at the next login.</td>
</tr>
<tr>
<td>Lock Account</td>
<td>Select to lock the account indefinitely.</td>
</tr>
<tr>
<td>Account Status</td>
<td>Displays the current account status:</td>
</tr>
<tr>
<td></td>
<td>- Active</td>
</tr>
<tr>
<td></td>
<td>- Locked</td>
</tr>
<tr>
<td></td>
<td>- Locked (invalid logins)</td>
</tr>
</tbody>
</table>

3. Assign rights to users. Each user is a member of a group that has a predefined user rights associated with it. You can assign or remove additional rights to the individual user.
4. Click the **Apply** button.

5. Click the **Back to Local/Remote Users** link to return to the Local/Remote User Settings page.

6. Add another user or click the **Back to Local/Remote Users** link. The Local/Remote Users page displays with the new user(s) listed in the table.

**Note:** The logged-in user’s name displays at the top of the web page. Only the tabs and options for which the user has rights display.

**Shortcut**

**To add a user based on an existing user:**

1. Display the existing user on the Local/Remote Users Settings page. The fields in the top part of the page display the current values for the user.

2. Change the Login to that of the new user. It is best to change the Password too.

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Users:</strong></td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td><strong>Power Users:</strong></td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td><strong>Administrators:</strong></td>
<td>This group has all possible rights.</td>
</tr>
<tr>
<td><strong>Custom Group:</strong></td>
<td>Select a custom group from the drop-down menu.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full Administrative</th>
<th>Right to perform any function on the SLB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>Right to enter network and routing settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system and audit logging, SSH and Telnet logins, SNMP, and SMTP. Includes NFS and CIFS.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage secure Lantronix units (e.g., SLP, Spider or SLB units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user. Includes configuring remote authentication methods and ordering.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create or edit a custom user menu for the CLI.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to shutdown or reboot the SLB.</td>
</tr>
<tr>
<td>Firmware &amp; Configuration</td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings).</td>
</tr>
<tr>
<td>Device Port Operations</td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td>Device Port Configuration</td>
<td>Right to enter device port settings.</td>
</tr>
<tr>
<td>USB</td>
<td>Right to enter modem settings for the USB.</td>
</tr>
<tr>
<td>Power Outlets</td>
<td>Right to view and enter settings for power outlets.</td>
</tr>
</tbody>
</table>
To edit a local user:
1. On the Local/Remote Users page, select the user and click the Add/Edit User button. The Local/Remote User Settings page displays.
2. Update values as desired.
3. Click the Apply button.

To delete a local user:
1. On the Local/Remote Users page, select the user.
2. Click the Delete User button.
3. Click the Apply button.

To change the sysadmin password:
1. On the Local/Remote Users page, select sysadmin and click the Add/Edit User button. The Local/Remote User Settings page displays.
2. Enter the new password in the Password and Retype Password fields.
3. Click the Apply button.

Note: You can change Escape Sequence and Break Sequence, if desired. You cannot delete the UID or change the UID, port permissions, or custom menu.

Local Users Commands
Go to Local Users Commands (on page 281) to view CLI commands which correspond to the web page entries described above.

NIS
The system administrator can configure the SLB branch office manager to use NIS to authenticate users attempting to log in to the SLB unit through the Web, SSH, Telnet, or the console port. If NIS does not provide port permissions, you can use this page to grant device port access to users who are authenticated through NIS.

All NIS users are members of a group that has predefined user rights associated with it. You can assign additional user rights that are not defined by the group.

To configure the SLB unit to use NIS to authenticate users:
1. Click the User Authentication tab and select the NIS option.
2. Enter the following:

| **Enable NIS** | Displays selected if you enabled this method on the Authentication Methods page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.  
**Note:** You can enable NIS here or on the first User Authentication page. If you enable NIS here, it automatically displays at the end of the order of precedence on the User Authentication page. |
| **NIS Domain** | The NIS domain of the SLB branch office manager must be the same as the NIS domain of the NIS server. |
| **Broadcast for NIS Server** | If selected, the SLB unit sends a broadcast datagram to find the NIS Server on the local network. |
| **NIS Master Server** (required) | The IP address or host name of the master server. |
| **NIS Slave Servers #1 - 5** | The IP addresses or host names of up to five slave servers. |
| **Custom Menu** | If custom menus have been created, you can assign a default custom menu to NIS users. |
11: User Authentication

In the **User Rights** section, select the user **Group** to which NIS users will belong:

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Users</strong>:</td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td><strong>Power Users</strong>:</td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td><strong>Administrators</strong>:</td>
<td>This group has all possible rights.</td>
</tr>
</tbody>
</table>

Assign or unassign **User Rights** for the specific user by checking or unchecking the following checkboxes:

<table>
<thead>
<tr>
<th>User Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Administrative</td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td>Networking</td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage secure Lantronix units (e.g., SLP, Spider, SLC and SLB units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create a custom user menu for the CLI for NIS users.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
</tbody>
</table>
5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**NIS Commands**

Go to *NIS Commands (on page 285)* to view CLI commands which correspond to the web page entries described above.

**LDAP**

The system administrator can configure the SLB branch office manager to use LDAP to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

LDAP allows SLB users to authenticate using a wide variety of LDAP servers, such as OpenLDAP and Microsoft Active Directory. The LDAP implementation supports LDAP servers that do not allow anonymous queries.

Users who are authenticated through LDAP are granted device port access through the port permissions on this page.

All LDAP users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

*To configure the SLB unit to use LDAP to authenticate users:*

1. Click the **User Authentication** tab and select **LDAP**. The following page displays.
2. Enter the following:

<table>
<thead>
<tr>
<th><strong>Enable LDAP</strong></th>
<th>Displays selected if you enabled this method on the first User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>The IP address or host name of the LDAP server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Number of the TCP port on the LDAP server to which the SLB unit talks. The default is 389.</td>
</tr>
<tr>
<td><strong>Base</strong></td>
<td>The name of the LDAP search base (e.g., dc=company, dc=com). May have up to 80 characters.</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Bind Name</strong></td>
<td>The name for a non-anonymous bind to an LDAP server. This item has the same format as LDAP Base. One example is cn=administrator,cn=Users,dc=domain,dc=com</td>
</tr>
<tr>
<td><strong>Bind Password / Retype Password</strong></td>
<td>Password for a non-anonymous bind. This entry is optional. Acceptable characters are a-z, A-Z, and 0-9. The maximum length is 127 characters.</td>
</tr>
<tr>
<td><strong>Bind with Login</strong></td>
<td>Select to bind with the login and password that a user is authenticating with. This requires that the Bind Name contain the $login token, which will be replaced with the current login. For example, if the Bind Name is uid=$login,ou=People,dc=lantronix,dc=com, and user roberts logs into the SLB branch office manager, LDAP will bind with uid=roberts,ou=People,dc=lantronix,dc=com and the password entered by roberts.</td>
</tr>
<tr>
<td><strong>User Login Attribute</strong></td>
<td>The attribute used by the LDAP server for user logins. If nothing is specified for the user filter, the SLB unit will use &quot;uid&quot;. For AD LDAP servers, the attribute for user logins is typically &quot;sAMAccountName&quot;.</td>
</tr>
<tr>
<td><strong>Group Filter Objectclass</strong></td>
<td>The objectclass used by the LDAP server for groups. If nothing is specified for the group filter, the SLB unit will use &quot;posixGroup&quot;. For AD LDAP servers, the objectclass for groups is typically &quot;Group&quot;.</td>
</tr>
<tr>
<td><strong>Group Member Attribute</strong></td>
<td>The attribute used by the LDAP server for group membership. This attribute may be use to search for a name (ie, &quot;msmith&quot;) or a Distinguished Name (ie, &quot;uid=msmith,ou=People,dc=lantronix,dc=com&quot;). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group membership attribute, the SLB branch office manager will use &quot;memberUID&quot; for name and &quot;uniqueMember&quot; for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of &quot;member&quot;.</td>
</tr>
<tr>
<td><strong>Group Member Value</strong></td>
<td>The attribute used by the LDAP server for group membership. This attribute may be use to search for a name (ie, &quot;msmith&quot;) or a Distinguished Name (ie, &quot;uid=msmith,ou=People,dc=lantronix,dc=com&quot;). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group membership attribute, the SLB unit will use &quot;memberUID&quot; for name and &quot;uniqueMember&quot; for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of &quot;member&quot;.</td>
</tr>
<tr>
<td><strong>Use LDAP Schema</strong></td>
<td>Select the check box to obtain remote user attributes (group/permissions and port access) from an Active Directory server's scheme via the user attribute &quot;secureLinxSLCPerms&quot;. For more information, see User Attributes &amp; Permissions from LDAP Schema or RADIUS VSA. By default, this option is disabled.</td>
</tr>
<tr>
<td><strong>Active Directory Support</strong></td>
<td>Select to enable. Active Directory is a directory service from Microsoft that is a part of Windows 2000 and later versions of Windows. It is LDAP- and Kerberos-compliant. By default, this option is disabled.</td>
</tr>
</tbody>
</table>
### Encrypt Messages
Select **Start TLS** or **SSL** to encrypt messages between the SLB unit and the LDAP server. If **Start TLS** is selected, the port will automatically be set to 389 and the StartTLS extension will be used to initiate a secure connection; if **SSL** is selected, the port will automatically be set to 636 and an SSL tunnel will be used for LDAP communication. The port number can be changed to a non-standard LDAP port; if the port number is set to anything other than 636, Start TLS will be used as the encryption method. Disabled by default.

A certificate can be uploaded to the SLB unit for peer authentication. The certificate file is a file of CA certificates in PEM format. The file can contain several CA certificates identified by:

```
-----BEGIN CERTIFICATE-----
(CA certificate in base64 encoding)
-----END CERTIFICATE-----
```

sequences. Before, between, and after the certificates text is allowed which can be used e.g. for descriptions of the certificates.

### Certificate
Click the **Upload File** link to upload a certificate file to the SLB unit for peer authentication. The certificate file is a file of CA certificates in PEM format. The file can contain several CA certificates identified by:

```
-----BEGIN CERTIFICATE-----
(CA certificate in base64 encoding)
-----END CERTIFICATE-----
```

sequences. Before, between, and after the certificates text is allowed which can be used e.g. for descriptions of the certificates.

### Custom Menu
If custom menus have been created, you can assign a default custom menu to LDAP users. ([See Custom Menus on page 234.](#))

### Escape Sequence
A single character or a two-character sequence that causes the SLB branch office manager to leave direct (interactive) mode. (To leave listen mode, press any key.)

A suggested value is **Esc+A** (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA, which is hexadecimal (\x) character 27 (\x1B) followed by an A.

This setting allows the user to terminate the `connect direct` command on the command line interface when the endpoint of the command is deviceport, tcp, or udp.

### Break Sequence
A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB, which is hexadecimal (\x) character 27 (\x1B) followed by a B.

### Enable for Dial-back
Select to grant a user dial-back access. Users with dial-back access can dial into the SLB unit and enter their login and password. Once the SLB unit authenticates them, the modem hangs up and dials them back. Disabled by default.

### Dial-back Number
The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user’s login (specified here).

### Data Ports
The ports users are able to monitor and interact with using the `connect direct` command.

### Listen Port
The ports users are able to monitor using the `connect listen` command.

### Clear Port Buffers
The ports whose port buffer users may clear using the `set locallog clear` command.

### Access Outlets
The outlets the user may monitor and configure.
3. In the **User Rights** section, select the user group to which LDAP users will belong:

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the LDAP users will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Users</td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td>Power Users</td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td>Administrators</td>
<td>This group has all possible rights.</td>
</tr>
</tbody>
</table>

4. Select or clear the checkboxes for the following rights:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Administrative</strong></td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td><strong>Secure Lantronix Network</strong></td>
<td>Right to view and manage secure Lantronix units (e.g., SLP, Spider and SLB units) on the local subnet.</td>
</tr>
<tr>
<td><strong>Date/Time</strong></td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td><strong>Local Users</strong></td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td><strong>Remote Authentication</strong></td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td><strong>SSH Keys</strong></td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td><strong>User Menus</strong></td>
<td>Right to create a custom user menu for the CLI for LDAP users.</td>
</tr>
<tr>
<td><strong>Web Access</strong></td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td><strong>Diagnostics &amp; Reports</strong></td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td><strong>Reboot &amp; Shutdown</strong></td>
<td>Right to use the CLI or shut down the SLB branch office manager and then reboot it.</td>
</tr>
<tr>
<td><strong>Firmware &amp; Configuration</strong></td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects <strong>Reboot &amp; Shutdown</strong>.</td>
</tr>
<tr>
<td><strong>Device Port Operations</strong></td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td><strong>Device Port Configuration</strong></td>
<td>Right to enter device port settings.</td>
</tr>
<tr>
<td><strong>USB</strong></td>
<td>Right to enter modem settings for USB devices.</td>
</tr>
<tr>
<td><strong>Power Outlets</strong></td>
<td>Right to configure power outlets.</td>
</tr>
</tbody>
</table>

5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**LDAP Commands**

Go to *LDAP Commands (on page 280)* to view CLI commands which correspond to the web page entries described above.
RADIUS

The system administrator can configure the SLB unit to use RADIUS to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

Users who are authenticated through RADIUS are granted device port access through the port permissions on this page.

All RADIUS users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

To configure the SLB branch office manager to use RADIUS to authenticate users:

1. Click the User Authentication tab and select RADIUS. The following page displays.

2. Enter the following:
### Enable RADIUS
Displays selected if you enabled this method on the User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.

**Note:** You can enable RADIUS here or on the first User Authentication page. If you enable RADIUS here, it automatically displays at the end of the order of precedence on the User Authentication page.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Server #1</strong></td>
<td>IP address or hostname of the primary RADIUS server. This RADIUS server may be a proxy for SecurID. SecurID is a two-factor authentication method based on the user's SecurID token and pin number. The SecurID token displays a string of digits called a token code that changes once a minute (some tokens are set to change codes every 30 seconds).</td>
</tr>
<tr>
<td><strong>Server #1 Port</strong></td>
<td>Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLB unit uses the default RADIUS port (1812).</td>
</tr>
<tr>
<td><strong>Server #1 Secret</strong></td>
<td>Text that serves as a shared secret between a RADIUS client and the server (SLB). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.</td>
</tr>
<tr>
<td><strong>RADIUS Server #2</strong></td>
<td>IP address or host name of the secondary RADIUS server. This server can be used as a SecurID proxy.</td>
</tr>
<tr>
<td><strong>Server #2 Port</strong></td>
<td>Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLB branch office manager uses the default RADIUS port (1812).</td>
</tr>
<tr>
<td><strong>Server #2 Secret</strong></td>
<td>Text that serves as a shared secret between a RADIUS client and the server (SLB). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The number of seconds (1-30) after which the connection attempt times out. The default is 30 seconds.</td>
</tr>
<tr>
<td><strong>Use VSA</strong></td>
<td>Select the check box to obtain remote user attributes (group/permissions and port access) from the RADIUS server via the Vendor-Specific Attribute (VSA). For details on the format of the VSA, see User Attributes &amp; Permissions from LDAP Schema or RADIUS VSA on page 216.</td>
</tr>
<tr>
<td><strong>Custom Menu</strong></td>
<td>If custom menus have been created, you can assign a default custom menu to RADIUS users.</td>
</tr>
<tr>
<td><strong>Escape Sequence</strong></td>
<td>A single character or a two-character sequence that causes the SLB unit to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is <code>Esc+A</code> (escape key, then uppercase &quot;A&quot; performed quickly but not simultaneously). You would specify this value as <code>\x1bA</code>, which is hexadecimal (<code>\x</code>) character 27 (<code>1B</code>) followed by an <code>A</code>. This setting allows the user to terminate the `connect direct command on the command line interface when the endpoint of the command is deviceport, tcp, or udp.</td>
</tr>
<tr>
<td><strong>Break Sequence</strong></td>
<td>A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is <code>Esc+B</code> (escape key, then uppercase &quot;B&quot; performed quickly but not simultaneously). You would specify this value as <code>\x1bB</code>, which is hexadecimal (<code>\x</code>) character 27 (<code>1B</code>) followed by a <code>B</code>.</td>
</tr>
<tr>
<td><strong>Enable for Dial-back</strong></td>
<td>Select to grant a user dial-back access. Users with dial-back access can dial into the SLB unit and enter their login and password. Once the SLB branch office manager authenticates them, the modem hangs up and dials them back. Disabled by default.</td>
</tr>
</tbody>
</table>
11: User Authentication

<table>
<thead>
<tr>
<th>Dial-back Number</th>
<th>The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user’s login (specified here).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Ports</td>
<td>The ports users are able to monitor and interact with using the connect direct command.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The ports users are able to monitor using the connect listen command.</td>
</tr>
<tr>
<td>Clear Port Buffers</td>
<td>The ports whose port buffer users may clear using the set locallog clear command.</td>
</tr>
<tr>
<td>Access Outlets</td>
<td>The power outlets users may monitor and configure.</td>
</tr>
</tbody>
</table>

**Note:** Older RADIUS servers may use 1645 as the default port. Check your RADIUS server configuration.

3. In the **User Rights** section, select the user group to which RADIUS users will belong.

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the RADIUS users will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td> Default Users:</td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td> Power Users:</td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td> Administrators:</td>
<td>This group has all possible rights.</td>
</tr>
</tbody>
</table>

4. Select or clear the checkboxes for the following rights:

<table>
<thead>
<tr>
<th>Full Administrative</th>
<th>Right to add, update, and delete all editable fields.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage secure Lantronix units (e.g., SLP, Spider and SLB units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create a custom user menu for the CLI for NIS users.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to use the CLI or shut down the SLB unit and then reboot it.</td>
</tr>
<tr>
<td>Firmware &amp; Configuration</td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects <strong>Reboot &amp; Shutdown</strong>.</td>
</tr>
<tr>
<td>Device Port Operations</td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td>Device Port Configuration</td>
<td>Right to access to port settings.</td>
</tr>
<tr>
<td>USB</td>
<td>Right to enter modem settings for USB devices.</td>
</tr>
<tr>
<td>Power Outlets</td>
<td>Right to configure power outlets.</td>
</tr>
</tbody>
</table>
5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**RADIUS Commands**

Go to [*RADIUS Commands (on page 286)*](#) to view CLI commands which correspond to the web page entries described above.

**User Attributes & Permissions from LDAP Schema or RADIUS VSA**

Remote user attributes (group/permissions and port access) can be obtained from an Active Directory server's schema via the user attribute 'secureLinxSLCPerms', or from a RADIUS server's Vendor-Specific Attribute (see below). This attribute is a set of parameter-value pairs. Each parameter and value is separated by a space, and a space separates each parameter-value pair. Whitespace is not supported in the value strings. The parameters that are supported are:

- **rights** - User rights. The value string is a comma-separated list of two letter user permissions. Example: "nt,wb,ra".
- **data** - Data port access. The value string specifies the list of ports the user has 'direct' access to. Example: "2,4-18,U,L".
- **listen** - Listen port access. The value string specifies the list of ports the user has 'listen' access to.
- **clear** - Clear port access. The value string specifies the list of port buffers the user has the right to clear.
- **outlet** - Outlet port access. The value string is the list of SLB outlets the user has rights for.
- **group** - User group. Valid values for the value string are "default", "power", and "admin".
- **esceq** - Escape sequence. The value string specifies the user's escape sequence. Use "\x" to specify non-printable characters. For example, "\x1bA" specifies the sequence "ESC-A".
- **brkseq** - Break sequence. The value string specifies the user's break sequence.
- **menu** - Custom user menu. The value string specifies the user's custom user menu.
- **display** - Display custom user menu when a user logs into the CLI. Valid values for the value string are "yes" and "no".
- **dbnumber** - Dial-back number. The value string specifies the user's dial-back number for modem dial-back connections.
- **allowdb** - Allow a user to have dial-back access. Valid values for the value string are "yes" and "no".

RADIUS servers will need to be configured to support the Lantronix Vendor-Specific Attribute. For example, on a FreeRADIUS server, the dictionary will need be updated with the Lantronix definition by including the contents below in a file named `dictionary.lantronix`, and including it in the RADIUS server dictionary definitions by adding the appropriate `$INCLUDE` directive to the main dictionary file.

```plaintext
# dictionary.lantronix
#
# Lantronix SLB Branch Office Manager
# Provides SLB-specific user attributes
#
VENDOR Lantronix 244
```
BEGIN-VENDOR Lantronix

ATTRIBUTE Lantronix-User-Attributes 1 string

END-VENDOR Lantronix

Once this is complete, the users file can be updated to include the Lantronix VSA for any user:

myuser    Auth-Type := Local, User-Password == "myuser_pwd"
Reply-Message = "Hello, %u",
Lantronix-User-Attributes = "data 1-4 listen 1-6 clear 1-4 group power"
Kerberos

Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

The system administrator can configure the SLB branch office manager to use Kerberos to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

Users who are authenticated through Kerberos are granted device port access through the port permissions on this page.

All Kerberos users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

To configure the SLB unit to use Kerberos to authenticate users:

1. Click the User Authentication tab and select the Kerberos option. The following page displays.
2. Enter the following:

<table>
<thead>
<tr>
<th>Enable Kerberos</th>
<th>Displays selected if you enabled this method on the User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> You can enable Kerberos here or on the first User Authentication page. If you enable Kerberos here, it automatically displays at the end of the order of precedence on the User Authentication page.</td>
<td></td>
</tr>
<tr>
<td>Realm</td>
<td>Enter the name of the logical network served by a single Kerberos database and a set of Key Distribution Centers. Usually, realm names are all uppercase letters to differentiate the realm from the Internet domain. Realm is similar in concept to an NT domain.</td>
</tr>
<tr>
<td>KDC</td>
<td>A key distribution center (KDC) is a server that issues Kerberos tickets. A ticket is a temporary set of electronic credentials that verify the identity of a client for a particular service. Enter the KDC in the fully qualified domain format (FQDN). An example is SLB.local.</td>
</tr>
<tr>
<td>KDC IP Address</td>
<td>Enter the IP address of the Key Distribution Center (KDC).</td>
</tr>
<tr>
<td>KDC Port</td>
<td>Port on the KDC listening for requests. Enter an integer with a maximum value of 65535. The default is 88.</td>
</tr>
<tr>
<td>Use LDAP</td>
<td>Indicate whether Kerberos should rely on LDAP to look up user IDs and Group IDs. This setting is disabled by default. <strong>Note:</strong> Make sure to configure LDAP if you select this option.</td>
</tr>
<tr>
<td>Custom Menu</td>
<td>If custom menus have been created, you can assign a default custom menu to RADIUS users.</td>
</tr>
<tr>
<td>Escape Sequence</td>
<td>A single character or a two-character sequence that causes the SLB unit to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is Esc+A (escape key, then uppercase &quot;A&quot; performed quickly but not simultaneously). You would specify this value as \x1bA, which is hexadecimal (\x) character 27 (1B) followed by an A. This setting allows the user to terminate the connect direct command on the command line interface when the endpoint of the command is deviceport, tcp, or udp.</td>
</tr>
<tr>
<td>Break Sequence</td>
<td>A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase &quot;B&quot; performed quickly but not simultaneously). You would specify this value as \x1bB, which is hexadecimal (\x) character 27 (1B) followed by a B.</td>
</tr>
<tr>
<td>Enable for Dial-back</td>
<td>Select to grant a user dial-back access. Users with dial-back access can dial into the SLB branch office manager and enter their login and password. Once the SLB unit authenticates them, the modem hangs up and dials them back. Disabled by default.</td>
</tr>
<tr>
<td>Dial-back Number</td>
<td>The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user’s login (specified here).</td>
</tr>
<tr>
<td>Data Ports</td>
<td>The ports users are able to monitor and interact with using the connect direct command.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The ports users are able to monitor using the connect listen command.</td>
</tr>
<tr>
<td>Clear Port Buffers</td>
<td>The ports whose port buffer users may clear using the set locallog clear command.</td>
</tr>
<tr>
<td>Access Outlets</td>
<td>The power outlets users may monitor and configure.</td>
</tr>
</tbody>
</table>
3. In the **User Rights** section, select the user group to which Kerberos users will belong.

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the Kerberos users will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>Default Users</strong>: This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Power Users</strong>: This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Administrators</strong>: This group has all possible rights.</td>
</tr>
</tbody>
</table>

4. Select or clear the checkboxes for the following rights:

<table>
<thead>
<tr>
<th>Full Administrative</th>
<th>Right to add, update, and delete all editable fields.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage secure Lantronix units (e.g., SLP, Spider and SLB units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create a custom user menu for the CLI for Kerberos users.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to use the CLI or shut down the SLB units and then reboot it.</td>
</tr>
<tr>
<td>Firmware &amp; Configuration</td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot &amp; Shutdown.</td>
</tr>
<tr>
<td>Device Port Operations</td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td>Device Port Configuration</td>
<td>Right to access to port settings.</td>
</tr>
<tr>
<td>USB</td>
<td>Right to enter modem settings for USB devices.</td>
</tr>
<tr>
<td>Power Outlets</td>
<td>Right to configure power outlets.</td>
</tr>
</tbody>
</table>

5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**Kerberos Commands**

Go to *Kerberos Commands (on page 279)* to view CLI commands which correspond to the web page entries described above.
11: User Authentication

TACACS+

Similar to RADIUS, the main function of TACACS+ is to perform authentication for remote access. The SLB branch office manager supports the TACACS+ protocol (not the older TACACS or XTACACS protocols).

The system administrator can configure the SLB branch office manager to use TACACS+ to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

Users who are authenticated through Kerberos are granted device port access through the port permissions on this page.

All TACACS+ users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

TACACS+ Groups

This section describes how a `priv_lvl` assigned to a TACACS+ user can be mapped to a SLB custom `Groups`, which will set the permissions and port rights for a TACACS+ user when they login to the SLB.

TACACS+ users are typically configured to have a privilege level 0-15, with each level representing a privilege level that is a superset of the next lower value. The privilege level can be assigned to individual users, or to groups that the user is a member of. When the SLB authenticates a TACACS+ user, it will first send an authentication request to the TACACS+ server, and wait for an authentication reply. If the user is successfully authenticated, the SLB will next send an authorization request to the TACACS+ server with the Service and optional Protocol.

The SLB will wait for an authorization response that will indicate if the user was successfully authorized for the requested service and protocol, and also contains a set of attribute-value pairs which define the attributes associated with the TACACS+ user.

The `priv_lvl` or `priv-lvl` is the only attribute sent from the TACACS+ server that the SLB will recognize and utilize. The privilege level number will be used to map to a SLB custom user group by finding a group with a name that ends in the same number as the `priv_lvl`. For example, a SLB group called "admin15" will map to any TACACS+ users with `priv_lvl` equal to 15; a SLB group called "manager8" will map to any TACACS+ users with `priv_lvl` equal to 8, and a SLB group called "readonly0" will map to any TACACS+ users with `priv_lvl` equal to 0. If two SLB groups ending with the same number exist, the SLB will select the first matching group it finds while searching the group list; for consistency it is recommended that only one SLB group exist for each `priv_lvl`.

When a TACACS+ user authenticates to the SLB, the Authentication Log will record any `priv_lvl` attribute-value pair returned by the TACACS+ server:

```
Sep 21 15:44:38 2017 slc431d SLC-SLB/x15login[2839]:
pam_sm_authenticate: server returned attribute `PRIV_LVL=14'
```

Any `priv_lvl` obtained for a TACACS+ user can also be viewed at the CLI with the show user command.
To configure the SLB unit to use TACACS+ to authenticate users:

1. Click the **TACACS+** tab and select **TACACS+**. The following page displays.

   **Figure 11-8 User Authentication > TACACS+**

2. Enter the following:

   **Enable TACACS+** Displays selected if you enabled this method on the User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.

   You can enable TACACS+ here or on the first User Authentication page. If you enable TACACS+ here, it automatically displays at the end of the order of precedence on the User Authentication page.

   **TACACS+ Servers 1-3** IP address or host name of up to three TACACS+ servers.

   **Secret/Retype Secret** Shared secret for message encryption between the SLB branch office manager and the TACACS+ server. Enter an alphanumeric secret of up to 127 characters.
### Encrypt Messages
Select the checkbox to encrypt messages between the SLB unit and the TACACS+ server. Selected by default.

### Authentication Service
The type of service used to pass the authentication tokens (e.g., login and password) between the SLB and the TACACS+ server. Options are: ASCII Login (login and password are transmitted in clear, unencrypted text), PPP/PAP (login and password are transmitted in clear, unencrypted text via a PAP protocol packet), and PPP/CHAP (the TACACS+ server sends a challenge that consists of a session ID and an arbitrary challenge string, and the user name and password are encrypted before they are sent back to the server). PPP/PAP is the default.

### Service
The service to use when sending a TACACS+ authorization message to the server to obtain an authenticated user's priv lvl. The priv lvl is used to assign a SLB custom group to the authenticated user for permissions and port rights (see TACACS+ Groups). Suggested values are "slip", "ppp", "arap", "shell", "ttydaemon", "connection", "system" and "firewall". The default is "shell".

### Protocol
The optional protocol associated with the Service, which is included in the TACACS+ authorization message sent to the server to obtain an authenticated user's priv lvl. The priv lvl is used to assign a SLB custom group to the authenticated user for permissions and port rights (see TACACS+ Groups). Suggested values are "lcp", "ip", "ipx", "atalk", "vines", "lat", "xremote", "tn3270", "telnet", "login", "pad", "vpad", "ftp", "http", "deccp", "osicp" and "unknown".

### Timeout
The timeout in seconds when attempting to connect to a TACACS+ server.

### Custom Menu
If custom menus have been created (see Custom Menus), you can assign a default custom menu to TACACS+ users.

### Escape Sequence
A single character or a two-character sequence that causes the SLB unit to leave direct (interactive) mode. (To leave listen mode, press any key.)

A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA, which is hexadecimal (\x) character 27 (1B) followed by an A.

This setting allows the user to terminate the connect direct command on the command line interface when the endpoint of the command is deviceport, tcp, or udp.

### Break Sequence
A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB, which is hexadecimal (\x) character 27 (1B) followed by a B.

See Custom Menus for notes on key sequence precedence and behavior.

### Enable for Dial-back
Select to grant a user dial-back access. Users with dial-back access can dial into the SLB unit and enter their login and password. Once the SLB branch office manager authenticates them, the modem hangs up and dials them back. Disabled by default.

### Dial-back Number
The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).

### Data Ports
The ports users are able to monitor and interact with using the connect direct command.

### Listen Ports
The ports users are able to monitor using the connect listen command.

### Clear Port Buffers
The ports whose port buffer users may clear using the set locallog clear command.

### Access Outlets
The power outlets users may monitor and configure.
3. In the **User Rights** section, select the user group to which TACACS+ users will belong.

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the TACACS+ users will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Users</strong></td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td><strong>Power Users</strong></td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td><strong>Administrators</strong></td>
<td>This group has all possible rights.</td>
</tr>
</tbody>
</table>

4. Select or clear the checkboxes for the following rights:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Administrative</strong></td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td><strong>Secure Lantronix Network</strong></td>
<td>Right to view and manage secure Lantronix units (e.g., SLP, Spider and SLB units) on the local subnet.</td>
</tr>
<tr>
<td><strong>Date/Time</strong></td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td><strong>Local Users</strong></td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td><strong>Remote Authentication</strong></td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td><strong>SSH Keys</strong></td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td><strong>User Menus</strong></td>
<td>Right to create a custom user menu for the CLI for TACACS+ users.</td>
</tr>
<tr>
<td><strong>Web Access</strong></td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td><strong>Diagnostics &amp; Reports</strong></td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td><strong>Reboot &amp; Shutdown</strong></td>
<td>Right to use the CLI or shut down the SLB unit and then reboot it.</td>
</tr>
<tr>
<td><strong>Firmware &amp; Configuration</strong></td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot &amp; Shutdown.</td>
</tr>
<tr>
<td><strong>Device Port Operations</strong></td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td><strong>Device Port Configuration</strong></td>
<td>Right to access to port settings.</td>
</tr>
<tr>
<td><strong>USB</strong></td>
<td>Right to enter modem settings for USB devices.</td>
</tr>
<tr>
<td><strong>Power Outlets</strong></td>
<td>Right to configure power outlets.</td>
</tr>
</tbody>
</table>

5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**TACACS+ Commands**

Go to [TACACS+ Commands (on page 287)](#) to view CLI commands which correspond to the web page entries described above.
Groups

The SLB branch office manager has 3 pre-defined groups: Administrators, Power Users, and Default Users. Custom groups can also be created; each custom group is a set of user attributes and permissions. Local Users and Remote Users defined on the SLB unit can be assigned to one of the pre-defined groups or a custom group. When a user authenticates, if they belong to custom group, they will be granted the custom group attributes and permissions, rather than their individual attributes and permissions. The SLB unit supports querying a LDAP server for groups that a LDAP user is a member of; if any of the LDAP group names match a (Custom Group Name), the LDAP user will be granted the rights of the custom group.

A custom group cannot be given the name of one of the pre-defined groups: “Admin”, “Power” or “Default” (or any version of these names where the case of the letters is different) since these names are used for the SLB pre-defined groups. Any LDAP group that matches one of these pre-defined group names will be ignored and not used to assign rights to a user.

To configure Groups in the SLB:

1. From the main menu, select User Authentication - Groups. The following page displays.

Note: If the fields in the lower part of the page have been populated by viewing another group, the fields can be cleared by selecting the Reset Group button.
2. Enter the following:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Enter a name for the group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen Ports</td>
<td>The ports users are able to monitor using the <code>connect listen</code> command.</td>
</tr>
<tr>
<td>Data Ports</td>
<td>The ports users are able to monitor and interact with using the <code>connect direct</code> command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15). U1 denotes the USB port on the front of the SLB unit. For SLB models with an internal modem, U2 denotes the internal modem.</td>
</tr>
<tr>
<td>Clear Port Buffers</td>
<td>The ports whose port buffer users may clear using the <code>set locallog clear</code> command.</td>
</tr>
<tr>
<td>Access Outlets</td>
<td>The power outlets users may monitor and configure. (SLB only)</td>
</tr>
<tr>
<td>Enable for Dial-back</td>
<td>Select to grant a user. Users with dial-back access can dial into the SLB unit and enter their login and password. Once the SLB unit authenticates them, the modem hangs up and dials them back. Disabled by default.</td>
</tr>
<tr>
<td>Dial-back Number</td>
<td>The phone number the modem dials back on depends on this setting for the device port. The user is either on a fixed number, or on a number that is associated with the user's login (specified here).</td>
</tr>
</tbody>
</table>
11: User Authentication

| Escape Sequence | A single character or a two-character sequence that causes the SLB branch office manager to leave direct (interactive) mode. (To leave listen mode, press any key.)
|                 | A suggested value is Esc+A (escape key, then uppercase “A” performed quickly but not simultaneously). You would specify this value as \x1bA, which is hexadecimal (\x) character 27 (1B) followed by an A.
|                 | This setting allows the user to terminate the connect direct command on the command line interface when the endpoint of the command is deviceport, tcp, or udp. |

| Break Sequence  | A series of one to ten characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase “B” performed quickly but not simultaneously). You would specify this value as \x1bB, which is hexadecimal (\x) character 27 (1B) followed by a B. |

| Custom Menu     | If custom menus have been created you can assign a default custom menu to the group. See Custom Menus for more information. |

| Display Menu at Login | Check the checkbox to display the menu at login. |

3. Select or clear the checkboxes for the following rights:

- **Full Administrative**: Right to add, update, and delete all editable fields.
- **Networking**: Right to enter network settings.
- **Services**: Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
- **Secure Lantronix Network**: Right to view and manage secure Lantronix units (e.g., SLP, Spider, and SLB units) on the local subnet.
- **Date/Time**: Right to set the date and time.
- **Local Users**: Right to add or delete local users on the system.
- **Remote Authentication**: Right to assign a remote user to a user group and assign a set of rights to the user.
- **SSH Keys**: Right to set SSH keys for authenticating users.
- **User Menus**: Right to create or edit a custom user menu for the CLI.
- **Web Access**: Right to access Web-Manager.
- **Diagnostics & Reports**: Right to obtain diagnostic information and reports about the unit.
- **Reboot & Shutdown**: Right to use the CLI or shut down the SLB unit and then reboot it.
- **Firmware & Configuration**: Right to upgrade the firmware on the unit and save or restore a configuration (all settings).
- **Device Port Operations**: Right to enter control device ports.
- **Device Port Configuration**: Right to enter device port settings.
- **USB**: Right to enter modem settings for USB devices.
- **Power Outlets**: Right to view and enter settings for power outlets (SLB unit only).

4. Click the Add Group button.

**To view or update a group:**

1. In the Groups table, select the group and click the View Group button. The group attributes and permissions will be displayed in the lower section of the page.

2. Modify the group attributes and permissions and click the Edit Group button.
To delete a group:

1. Select the group in the Groups table.
2. Click the Delete Group button.

**SSH Keys**

The SLB branch office manager can import and export SSH keys to facilitate shared key authentication for all incoming and outgoing SSH connections. By using a public/private key pair, a user can access multiple hosts with a single passphrase, or, if a passphrase is not used, a user can access multiple hosts without entering a password. In either case, the authentication is protected against security attacks because both the public key and the private key are required to authenticate. For both imported and exported SSH keys, the SLB unit supports both RSA and DSA keys, and can import and export keys in OpenSSH and SECSH formats. Imported and exported keys are saved with the SLB configuration, and the administrator has the option of retaining the SSH keys during a reset to factory defaults.

The SLB unit can also update the SSH RSA1, RSA and DSA host keys that the SSH server uses with site-specific host keys or reset them to the default values.

**Imported Keys**

Imported SSH keys must be associated with an SLB local user. The key can be generated on host "MyHost" for user "MyUser," and when the key is imported into the SLB, it must be associated with either "MyUser" (if "MyUser" is an existing SLB local user) or an alternate SLB local user. The public key file can be imported via SCP or FTP; once imported, you can view or delete the public key. Any SSH connection into the SLB branch office manager from the designated host/user combination uses the SSH key for authentication.

**Exported Keys**

The SLB unit can generate SSH keys for SSH connections out of the SLB unit for any SLB user. The SLB branch office manager retains both the private and public key on the SLB unit, and makes the public key available for export via SCP, FTP, or copy and paste. The name of the key is used to generate the name of the public key file that is exported (for example, <keyname>.pub), and the exported keys are organized by user and key name. Once a key is generated and exported, you can delete the key or view the public portion. Any SSH connection out of the SLB branch office manager for the designated host/user combination uses the SSH key for authentication.
To configure the SLB unit to use SSH keys to authenticate users:

1. From the main menu, select User Authentication - SSH Keys. The following page displays.

   **Figure 11-10** User Authentication > SSH Keys

<table>
<thead>
<tr>
<th>Imported SSH Keys</th>
<th>View</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Host</td>
<td>Type</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exported SSH Keys</th>
<th>View</th>
<th>Download</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Key Name</td>
<td>Type</td>
<td></td>
</tr>
</tbody>
</table>

2. Enter the following:
11: User Authentication

Imported Keys (SSH In)

*Host & User Associated with Key*

These entries are required in the following cases:
- The imported key file does not contain the host that the user will be making an SSH connection from, or
- The SLB local user login for the connection is different from the user name the key was generated from or is not included in the imported key file.

If either of these conditions is true, or the imported file is in SECSH format, you must specify the user and host. The following is an example of a public key file that includes the user and host:

```
ssh-rsa AAAAB3NzaC1yc2EAAAAB3IwAAAEEEApUHCX9ESwSt+jmUGXa1YC3us
ABYxIXUhSU1N+NU9HNaUADUfj8LYz8/gUnUSH4Ksm9GRT7/8/Sn9jCVfGPh
UQ== asallaway@winserver
```

- **Host**
  - Host name or IP address from which the SSH connections to the SLB branch office manager will be made.
- **User**
  - The User ID of the user being given secure access to the SLB unit.

Host & Login for Import

- **Import via**
  - Select SCP or FTP as the method for importing the SSH keys. SCP is the default.
- **Filename**
  - Name of the public key file (for example, mykey.pub). May contain multiple keys.
- **Host**
  - IP address of the remote server from which to SCP or FTP the public key file.
- **Path**
  - Optional pathname to the public key file.
- **Login**
  - User ID to use to SCP or FTP the file.
- **Password / Retype Password**
  - Password to use to SCP or FTP the file.

Exported Keys (SSH Out)

- **Export**
  - Enables you to export created public keys. Select one of the following:
    - **New Key for User**: Enables you to create a new key for a user and export the public key in a file.
    - **All Previously Created Keys**: Does not create any keys, but exports all previously created public keys in one file.
- **User**
  - User ID of the person given secure access to the remote server.
- **Key Name**
  - Name of the key. This will generate the public key filename (e.g., <keyname>.pub).
- **Key Type**
  - Select either the RSA or the DSA encryption standard. RSA is the default.
- **Number of Bits**
  - Select the number of bits in the key (512 or 1024). The default is 512.
- **Passphrase / Retype Passphrase**
  - Optionally, enter a passphrase associated with the key. The passphrase may have up to 50 characters. The passphrase is an optional password that can be associated with an SSH key. It is unique to each user and to each key.
- **SECSH Format**
  - Indicate whether the keys will be exported in SECSH format (by default the key is exported in OpenSSH format).
- **Public Key Filename**
  - Filename of the public host key.
Host and Login for Export

<table>
<thead>
<tr>
<th><strong>Export via</strong></th>
<th>Select the method (SCP, FTP, HTTPS or Copy/Paste) of exporting the key to the remote server. Copy/Paste, the default, requires no other parameters for export.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>IP address of the remote server to which the SLB unit will SCP or FTP the public key file.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>Optional path of the file on the host to SCP or FTP the public key too.</td>
</tr>
<tr>
<td><strong>Login</strong></td>
<td>User ID to use to SCP or FTP the public key file.</td>
</tr>
<tr>
<td><strong>Password / Retype Password</strong></td>
<td>Password to use to SCP or FTP the public key file.</td>
</tr>
</tbody>
</table>

**To view or delete a key:**

1. Select the key from the appropriate table. The View and Delete buttons become active.
2. To view the key, click the View button. A pop-up page displays the key.

**Imported key for sysadmin@DaveSLM:**

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxGxPGY9HsG9VqroDo98B89Cf
haqB6jG//OttMkkb3zrpPu0HHAxaiVXHAvv7lAte31VToXdLAXN0uCvuJLfa/LvvGmoEWBuBSu5051QHfL70ijxZW0EVTJGFqUQTSq8Ls3/v31kJUJEX5ln
2AIQx0F40I5wNECo+m3d5QF+FKc= sysadmin@DaveSLM
```

3. To delete the key, click the Delete button.

**To view, reset, or import SSH RSA, DSA, ECDSA and ED25519 host keys:**

1. On the User Authentication - SSH Keys page, click the SSH Server/Host Keys link at the top right. The following page displays the current host keys. In the example below, the current keys are the defaults.
Figure 11-11  Current Host Keys

Current Host RSA Public Key (Default Key)

ssh-rsa AAAAE3NzCz1Cy2EQAADQABAAABAABQD8EyrzC4Axvxw74qhckcT63DR13bID/F2h2eGmD/0 S0hI2ZtHh2Jh2pVcYD1PSz8nFtP+Enez81l1y2zYiYF19Fw8b4W65Gb2hcmQ3b6e3m33k113190 KG1DKxkTzUtjeMTUtaNgZmd3/vYF1v14OapuOz1hHpxyGLP2sluLMlVkyVaa19qGwRY1U6C8xT7u5ib Dkkc9aB02fa8i8TTs5rV7w/nzYAT811L7-cen7yWp3j89jcr1BmvoPARyLYV6u/07X8eS/umG8YRF9cpFsKsK+y 4v0L1shqF0jYN6uW1g5s6r103P+rAqI686hSB7G81x2n5j1XAngOtalCyHxT3-root@sl2b2956 (RSA)

Current Host DSA Public Key (Default Key)

ssh-dss AAAAE3NzCz1Cy2EQAADQABAAABAABQD8EyrzC4Axvxw74qhckcT63DR13bID/F2h2eGmD/0 S0hI2ZtHh2Jh2pVcYD1PSz8nFtP+Enez81l1y2zYiYF19Fw8b4W65Gb2hcmQ3b6e3m33k113190 KG1DKxkTzUtjeMTUtaNgZmd3/vYF1v14OapuOz1hHpxyGLP2sluLMlVkyVaa19qGwRY1U6C8xT7u5ib Dkkc9aB02fa8i8TTs5rV7w/nzYAT811L7-cen7yWp3j89jcr1BmvoPARyLYV6u/07X8eS/umG8YRF9cpFsKsK+y 4v0L1shqF0jYN6uW1g5s6r103P+rAqI686hSB7G81x2n5j1XAngOtalCyHxT3-root@sl2b2956 (RSA)

Current Host ECDSA Public Key (Default Key)

ecdsa-sha2-nistp256 AAAA82YJZIHHLWvNTYt1-bldzMH4YMYTYAAdABBABBFDPUAD a/9WVaRcsxazaE27dHkRh8vh8m49kABwvPcRqHwve2ic6szT40phc6u5shX13qkBqSaAF79gf9qS6UvC = root@E0ACS (ECSA)

Current Host ECDSA Public Key (Default Key)

ssh-ed25519 AAAACn8zA1I0Z1NFET65AAAAAB836uSb+T9fysKlv6Cvu61l217rzxi2lyFt9nK6UvF root@E0ACS (ECSA)

Note: changing a host key requires a reboot for the update to take effect.
2. View or enter the following:

<table>
<thead>
<tr>
<th><strong>Reset to Default Host Key</strong></th>
<th>Select the <strong>All Keys</strong> checkbox to reset all default key(s), or select one or more checkboxes to reset defaults for <strong>RSA, DSA, ECDSA, or ED25519</strong> keys. All checkboxes are unselected by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import Host Key</strong></td>
<td>To import a site-specific host key, select the checkbox. Unselected by default.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>From the drop-down list, select the type of host key to import.</td>
</tr>
<tr>
<td><strong>Import via</strong></td>
<td>From the drop-down list, select the method of importing the host key (SCP or SFTP). The default is <strong>SCP</strong>.</td>
</tr>
<tr>
<td><strong>Public Key Filename</strong></td>
<td>Filename of the public host key.</td>
</tr>
<tr>
<td><strong>Private Key Filename</strong></td>
<td>Filename of the private host key.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Host name or IP address of the host from which to import the key.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>Path of the directory where the host key will be stored.</td>
</tr>
<tr>
<td><strong>Login</strong></td>
<td>User ID to use to SCP or SFTP the file.</td>
</tr>
<tr>
<td><strong>Password / Retype Password</strong></td>
<td>Password to use to SCP or SFTP the file.</td>
</tr>
</tbody>
</table>

3. Click the **Apply** button.

4. Repeat steps 2-3 for each key you want to import.

5. To return to the SSH Keys page, click the **Back to SSH Keys** link.

**SSH Key Commands**

Go to **SSH Key Commands (on page 338)** to view CLI commands which correspond to the web page entries described above.
Custom Menus

Users can have custom user menus as their command line interface, rather than the standard CLI command set. Each custom user menu can contain up to 50 commands ('logout' is always the last command). Instead of typing each command, the user enters the number associated with the command. Each command can also have a nickname associated with it, which can be displayed in the menu instead of the command. The commands `showmenu <Menu Name>` and `returnmenu` can be entered to display another menu from a menu, or to return to the prior menu. The command `returncli` can be used to break out of a menu and return to the regular CLI.

To add a custom menu:

1. Click the **User Authentication** tab and select the **Custom Menus** option. The Custom Menus page displays:
2. In the lower section of the page, enter the following:

**Note:** To clear fields in the lower part of the page, click the **Clear Custom Menu** button.

<table>
<thead>
<tr>
<th>Menu Name</th>
<th>Enter a name for the custom menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Enter an optional title which will be displayed about the menu at the CLI.</td>
</tr>
<tr>
<td>Nicknames</td>
<td>Select to enable nicknames to be displayed in the menu instead of the commands. If the custom menu will have nicknames, this should also be selected prior to entering the commands in the web page, as this will facilitate entry of the nicknames.</td>
</tr>
<tr>
<td>Redisplay Menu</td>
<td>Select to redisplay the custom menu each time before the CLI prompt is displayed.</td>
</tr>
</tbody>
</table>

3. You have the following options:
   - To save the custom menu without any more commands than the default *logout* command, click the **Add Custom Menu** button.
   - To add menu commands, select the **QuickEdit Mode** box. This will move the cursor from **Command** to **Nickname** and back to **Command** (if **Nicknames** is selected), or keep the cursor on Command (if Nicknames is not selected). Commands (and the optional nicknames) are added to the **Menu Commands/Nicknames** list when carriage return is entered at the **Command** field (if **Nicknames** is not selected) or the **Nickname** field (if **Nicknames** is selected). Most browsers have a "Select All" keystroke (such as Control-A) which allow you to select all of the text in a field; this can be used in conjunction with the Delete key to clear the contents of a field before entering a new command or nickname. The **Clear Command & Nickname** button can also be used to delete the contents of the Command and Nickname fields.

   Commands can also be added to the list when **QuickEdit Mode** is not selected. Enter the command and the optional nickname and click the **right** arrow. The command will be added before the logout command (if a command/nickname is not selected in the list) or will replace the currently selected command/nickname in the list. The **Unselect Command & Nickname** button can be used to unselect the currently selected command/nickname in the list.

4. To add more commands to the custom menu, repeat step 3.

5. You also have the following options:
   - To edit a command/nickname in the custom menu, select the command in the **Commands/Nicknames List** box and select the **left** arrow button. Change the command and/or the nickname, and with the same command still selected in the list, select the **right** arrow button.
   - To remove a command/nickname from the custom menu, select the command in the **Commands/Nicknames List** box and select the **Delete Command & Nickname** button.
   - To move a command higher up in the menu (the commands are shown in the order they will be presented in the custom menu, with command #1 listed first), select the command in the **Commands/Nicknames List** box and click the **up** arrow.
   - To move a command further down in the menu, select the menu in the **Commands/Nicknames List** box and click the **down** arrow.

6. Click the **Add Custom Menu** button.
To view or update a custom menu:

1. In the Custom Menus table, select the custom menu and click the View Custom Menu button. The custom menu attributes appear in the lower part of the page.
2. Update the menu attributes following the instructions for adding a menu above.
3. Click the Edit Custom Menu button.

To delete a custom menu:

1. Select the custom menu in the Custom Menus table.
2. Click the Delete Custom Menu button.

To create a new custom menu from an existing custom menu:

1. Select the custom menu in the Custom Menus table.
2. Enter a name for the new menu in the New Menu Name field.
3. Click the Copy Custom Menu button.

Custom User Menu Commands

Go to Custom User Menu Commands (on page 301) to view CLI commands which correspond to the web page entries described above.
12: Maintenance

The system administrator performs maintenance activities and operates the SLB branch office manager using the options for the Maintenance tab and additional commands on the command line interface.

Firmware & Configurations

The Maintenance > Firmware & Configurations page allows the system administrator to:

- Configure the FTP, SFTP, or TFTP server that will be used to provide firmware updates and save/restore configurations. (TFTP is only used for firmware updates and configurations restored via DHCP/TFTP Zero Touch Provisioning.)
- Set up the location or method that will be used to save or restore configurations (default, FTP, SFTP, NFS, CIFS, or USB). Update the version of the firmware running on the SLB.
- Save a snapshot of all settings on the SLB unit (save a configuration).
- Restore the configuration, either to a previously saved configuration, or to the factory defaults.
- For dual boot SLB units, view the firmware version on each boot bank, select the bank to boot from, and copy the contents of one boot bank to the other.
- View the firmware version on each boot bank, select the bank to boot from, and copy the contents of one boot bank to the other.

Factory Reset with External Storage Device

In the event that a reset to factory defaults cannot be performed via the web UI or CLI or LCD, a factory reset can be initiated by attaching an external storage device to the console manager with a file in the top level directory of the storage device.

To perform a factory reset using external storage device:

1. Create a file FACTORY_DEFAULT in the top-level directory of an external storage device (USB thumb drive). The file should contain the MAC address of the Eth1 Ethernet port in a single line, with or without colons (case insensitive).
2. Insert the external storage device into SLB.
3. Reboot the SLB unit. After the message "Starting <model>..." the console manager attempts to mount an external storage device. If it successfully mounts a storage device, and finds the appropriate FACTORY_DEFAULT file in the top level directory, it will perform a reset to factory defaults. A message appears on the console manager indicating that the FACTORY_DEFAULT file is detected in the external storage and the device is performing a factory reset.

Note: If the external storage device with the FACTORY_DEFAULT file is left connected to the console manager and it is rebooted, a reset to factory default will be performed again. Therefore, we recommend you remove the storage device after a reset to factory defaults.

To configure settings:

1. Click the Maintenance tab. The Maintenance > Firmware & Configurations page displays.
2. Enter the following:

**Reboot**
Select this option to reboot the SLB branch office manager immediately. The default is **No**.

*Note:* The front panel LCD displays the “Rebooting the SLB” message, and the normal boot sequence occurs.

**Shutdown**
Check this option to shut down the SLB. The default is **Unchecked**.
# 12: Maintenance

## Internal Temperature

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>Displays current temperature.</td>
</tr>
<tr>
<td>Low (°C)</td>
<td>Sets the acceptable minimum for the internal temperature of the SLB unit. If the temperature of the SLB unit changes to be outside of this range, the SLB branch office manager will issue an SNMP trap.</td>
</tr>
<tr>
<td>High (°C)</td>
<td>Sets the acceptable maximum for the internal temperature of the SLB unit. If the temperature of the SLB branch office manager changes to be outside of this range, the SLB unit will issue an SNMP trap.</td>
</tr>
<tr>
<td>Calibrate Offset (°C)</td>
<td>An offset for calibrating the internal temperature of the SLB unit. The offset will be applied one hour after setting the calibration value. Zerоing the offset will take effect immediately and will cancel any current and/or pending calibration.</td>
</tr>
</tbody>
</table>

## Site Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Rack Row</td>
<td>Set these fields to define the rack row the SLB unit is located within a large data center. The default for these fields is 1.</td>
</tr>
<tr>
<td>Data Center Rack Cluster</td>
<td>Set these fields to define the rack cluster the SLB unit is located within a large data center. The default for these fields is 1.</td>
</tr>
<tr>
<td>Data Center Rack</td>
<td>Set these fields to define the rack the SLB unit is located within a large data center. The default for these fields is 1.</td>
</tr>
<tr>
<td>Site Tag</td>
<td>Tag or description used to identify the location or some other attribute of the SLB</td>
</tr>
</tbody>
</table>

## SLB Firmware

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Version</td>
<td>Displays the current firmware version.</td>
</tr>
</tbody>
</table>
| Update Firmware | ◆ To update the SLB firmware, select the checkbox. If you select this option, the SLB branch office manager reboots after you apply the update. The first time boot for each bank may take up to 5 minutes. Subsequent boot times will be approximately 2 minutes.  
◆ To view a log of all prior firmware updates, click the Firmware Update Log link.  
**Note:** For dual boot SLB units, the non-active boot bank is updated during the firmware update, without requiring a reboot. The configuration on the current boot bank may optionally be copied to the non-active boot bank during the firmware update. For both single boot and dual boot SLB units, prior to firmware update, the current configuration is saved to the Local Disk location with the name "before_MMDDYY_HHMM". |
| Firmware Filename | The name of the firmware update file downloaded from the Lantronix web site.                                      |
| Key             | A key for validating the firmware file. The key is provided with the firmware file (32 hex characters).            |
| Load Firmware via | From the drop-down list, select the method of loading the firmware. Options are FTP, TFTP, HTTPS, NFS, USB, and SFTP (Secure FTP). TFTP is the default. If you select HTTPS, the Upload File link becomes active. Select the link to open a popup window that allows you to browse to a firmware update file to upload. |
Boot Banks

Note: The first time boot for each bank may take up to 5 minutes. Subsequent boot times will be approximately 2 minutes.

<table>
<thead>
<tr>
<th>Bank 1</th>
<th>Displays the version of SLB firmware in bank 1. Note: The word “current” displays next to the bank from which the SLB branch office manager booted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank 2</td>
<td>Displays the version of SLB firmware in bank 2.</td>
</tr>
<tr>
<td>Next Boot Bank</td>
<td>Displays the current setting for bank to boot from at next reboot.</td>
</tr>
<tr>
<td>Switch to Bank 2</td>
<td>If desired, select the alternate bank to boot from at next reboot.</td>
</tr>
<tr>
<td>Copy configuration from Bank 1 to Bank 3 during firmware update</td>
<td>If checked, will copy the configuration from the current bank to the bank being updated. The two numbers are automatically generated so that the first number is the current bank.</td>
</tr>
<tr>
<td>Copy contents of Bank 1 to Bank 2</td>
<td>If checked, enables you to copy the current boot bank to the alternate boot bank. This process takes a few minutes to complete.</td>
</tr>
</tbody>
</table>

Load Firmware Via Options

HTTPS
NFS Mounted Dir
USB Port
FTP/SFTP/TFTP Server
Path
Login
Password / Retype Password
One Time Login/Password

Configuration Management

<table>
<thead>
<tr>
<th>Configuration Management</th>
<th>From the option list, select one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>No Save/Restore:</strong> Does not save or restore a configuration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Restore Factory Defaults:</strong> Restores factory defaults. If you select this option, the SLB unit reboots after you apply the update. Select the SSH Keys checkbox to save any imported or exported SSH keys. Select the SSL Certificate checkbox to save an imported certificate. Select the Scripts checkbox to save any interface or batch scripts. Disabled by default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Restore Saved Configuration:</strong> Returns the SLB settings to a previously saved configuration. If you select this option, the SLB reboots after you apply the update.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Save Configuration:</strong> Saves all settings to file, which can be backed up to a location that is not on the SLB. If Tarball Format is checked, the configuration will be saved in the old (insecure) compressed tar file format, instead of the password protected zip file format. The Tarball Format is only available for saving a configuration via HTTPS.</td>
</tr>
</tbody>
</table>
3. Click **Apply**.

*Note:* If you selected an option that forces a reboot (restore configuration, update firmware, or reset factory defaults), the SLB unit automatically reboots at the end of the process.

### Zero Touch Provisioning Configuration Restore

The Zero Touch Provisioning feature allows a factory defaulted SLB to acquire a default configuration from a DHCP server and TFTP server when it is booted. At boot-time, before the normal startup process, a unit will attempt to acquire network parameters and a configuration file, first over Eth1, and then over Eth2:

- The unit will broadcast on the Eth1 network port for a DHCP server on the local subnet, requesting DHCP options “TFTP Server” (DHCP option #66) and "Boot Filename" (DHCP option #67).
- If it receives both options from the DHCP server, and the Boot Filename is a valid SLB configuration filename ending in "-slccfg.tgz", it will attempt to download the Boot Filename from the TFTP Server.

---

**Save with Config or Preserve with Restore**

- Select the **SSH Keys** checkbox to save any imported or exported SSH keys.
- Select the **SSL Certificate** checkbox to save an imported certificate.
- Select the **Scripts** checkbox to save any interface or batch scripts. Disabled by default.

**Preserve Configuration after Restore**

Allows the user to keep a subset of the current configuration after restoring a configuration or resetting to factory defaults.

Select the checkbox for each part of the current configuration you want to keep, for example, Networking, Services, or Device Ports.

**Configuration Name to Save To or Restore From**

If you selected to save or restore a configuration, enter a name for the configuration file (up to 12 characters).

**Location for Save, Restore, or Manage**

If you selected to save or restore a configuration, select one of the following options:

- **Local Disk – Saved Configurations**: If restoring, select a saved configuration from the drop-down list.
- **FTP Server**: The FTP server specified in the FTP/SFTP/TFTP section. If you select this option, select FTP or SFTP to transfer the configuration file.
- **NFS Mounted Directory**: Local directory of the NFS server for mounting files.
- **CIFS Share – Saved Configurations**: If restoring, select a saved configuration from the drop-down list.
- **USB**: If a USB thumb drive is loaded into one of the USB ports of the SLB branch office manager, and properly mounted, the configuration can be saved to or restored from this location. If you select this option, select the port in which the USB thumb drive is mounted; then click a saved configuration from the drop-down list.
- **HTTPS**: For saving, the browser will prompt the user to save the configuration. For restoring, the configuration will be uploaded to the Local Disk location.
- **Manage**: The **Manage** option allows you to view and delete all configurations saved to the selected location. This feature is available for the default, CIFS Share, and USB locations.

**Preserve Configuration after Restore**

Allows the user to keep a subset of the current configuration after restoring a configuration or resetting to factory defaults.

Select the checkbox for each part of the current configuration you want to keep, for example, Networking, Services, or Device Ports.
If it is able to download the Boot Filename from the TFTP Server, it will restore the configuration onto the SLB, and begin the normal startup process.

If any of these steps fail for the Eth1 network port, it will repeat the process of trying to acquire a configuration over the Eth2 network port.

After attempting to acquire a configuration over the Eth2 network port, the unit will begin the normal startup process.

Any results of attempting to acquire and restore a configuration file will be output to the console port and the system log. Configurations for firmware versions that are newer than the firmware version running on the unit will not be restored. Spaces are not supported in either the directory or filename portion of the Boot Filename path.

To manage configuration files:

The Manage option on the Maintenance > Firmware & Configurations page allows you to view all configurations saved to the selected location and delete any of the configurations. This feature is available for the default, CIFS Share, and USB locations.

1. On the Maintenance > Firmware & Configurations page, click the Manage link. The following page displays the name and the time and date the file was saved:

   ![Manage Configuration Files](Figure 12-2)

2. To delete files, select one or more files and click the Delete File button.
3. To download a new firmware file, click the Download File button.
4. To rename a listed file, select the file, type the new file name into the New File Name field, and click the Rename File button.

Administrative Commands

Go to Administrative Commands (on page 267) to view CLI commands which correspond to the web page entries described above.
System Logs

The Maintenance > System Logs page allows you to view various system logs. (See Chapter 7: Services on page 87 for more information about system logs.) You can also clear logs on this page.

To view system logs:

1. Click the Maintenance tab and select the System Logs option. The following page displays:

   ![Figure 12-3 Maintenance > System Logs](image)

   - **Log**: Select the type(s) of log you want to view:
     - All
     - Network
     - Services
     - Authentication
     - Device Ports
     - Diagnostics
     - General
     - Software

   - **Level**: Select the alert level you want to view for the selected log:
     - Error
     - Warning
     - Info
     - Debug

2. Enter the following to define the parameters of the log you would like to view:

   - **Starting at**: September 21, 2001, 08:22:55 am
   - **Ending at**: September 21, 2001, 08:22:55 am

   - **View Log**
   - **Clear Log**
3. Click the **View Log** button. Your specified system log displays. For example, if you select the type **All** and the level **Error**, the SLB branch office manager displays a log similar to this:

```
From a queried system log (i.e., Figure 12-4), you may email this information to a specific individual or to Lantronix Technical Support. See **Emailing Logs and Reports (on page 251)**.

**To clear system logs:**

1. From the **Maintenance > System Logs** page, select **SLB Maintenance - System Logs**.
2. Click the **Clear Log** button to clear all log information.

**System Log Commands**

Go to **System Log Commands (on page 343)** to view CLI commands which correspond to the web page entries described above.
Audit Log

The Maintenance > Audit Log page displays a log of all actions that have changed the configuration of the SLB. The audit log is disabled by default. Use the Services > SSH/Telnet/ Logging page (Chapter 7: Services) to enable the audit log and to configure its maximum size.

Each entry in the log file contains a date/time stamp, user login, and the action performed by the user. The user may clear the log file and sort the log by date/time, user, and command. The audit log is saved through SLB branch office manager reboots.

1. Click the Maintenance tab and select the Audit Log option. The following page displays:

   ![Figure 12-5: Maintenance > Audit Log](image)

   **Sorted by: Date/Time**

   2. To select a sort option, click the appropriate button:
      - To sort by date and time, click the Date/Time button (this is the default) to sort by Date/Time.
      - To sort by user, click the Sort by User button.
      - To sort by command/action, click the Command button.

3. To email this log, follow the instructions in Emailing Logs and Reports (on page 251).
4. To clear the log, click the Clear Log button.
5. To freeze or stop automatic refreshing of the log, click the Stop Refresh button.
Email Log

The *Maintenance > Email Log* page displays a log of all attempted emails. The log file can be cleared from here. The email log is saved through SLB unit reboots.

1. Click the Maintenance tab and select the Email Log option. The following page displays:

2. To email this log, follow the instructions in *Emailing Logs and Reports (on page 251).*

3. To clear the log, click the **Clear Log** button.
Diagnostics

The Maintenance > Diagnostics page provides methods for diagnosing problems such as network connectivity and device port input/output problems. You can use equivalent commands on the command line interface. An additional diagnostic, loopback, is only available as a command.

1. Click the Maintenance tab and select the Diagnostics option. The following page displays:

![Figure 12-7 Maintenance > Diagnostics]

2. Select Diagnostics from checklist (one or more diagnostic methods you want to run, or select All to run them all):

<table>
<thead>
<tr>
<th>Diagnostic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Table</td>
<td>Address Resolution Protocol (ARP) table used to view the IP address-to-hardware address mapping.</td>
</tr>
<tr>
<td>Netstat</td>
<td>Displays network connections. If you select the checkbox, select the TCP or UDP protocol, or select All for both protocols to control the output of the Netstat report.</td>
</tr>
<tr>
<td>Host Lookup</td>
<td>Select to verify that the SLB branch office manager can resolve the host name into an IP address (if DNS is enabled). If selected, also enter a host name in the corresponding Hostname field.</td>
</tr>
</tbody>
</table>
### Ping
Select to verify that the host is up and running. If selected, also do the following:
- Enter a host name in the corresponding **Hostname** field
- Specify Ethernet Port (Both, Eth1 or Eth2)
- Check IPv6 if... need text.

### Send Packet
This option sends an Ethernet packet out one of the Ethernet ports, mainly as a network connectivity test. For UDP, the number of times the string is sent is equal to the number of packets sent. For TCP, the number of times the string is sent may (or may not) be equal to the number of packets sent, because TCP controls how data is packetized and sent out. Enter the following:
- **Protocol**: Select the type of packet to send (TCP or UDP).
- **Hostname**: Specify a host name or IP address of the host to send the packet to.
- **Port**: Specify a TCP or UDP port number of the host to send the packet to.
- **String**: Enter a set of up to 64 characters. The string is encapsulated in the packet (so you could use a network sniffer to track the packet and, by looking at its contents, verify that it was sent).
- **Count**: The count is the number of times the string is sent.

### Loopback
Specify loopback information:
- **Device Port**
- Select either an **Internal** or **External** test

### SLB Internals
Select to display information on the internal memory, storage and processes of the SLB.

3. Click the **Run Diagnostics** button. The **Diagnostics Report** page displays.

![Diagnostics Report](image)

**Figure 12-8 Diagnostics Report**

### Diagnostic Commands
Go to **Diagnostic Commands (on page 309)** to view CLI commands which correspond to the web page entries described above.

4. To email this report, follow the instructions in *Emailing Logs and Reports (on page 251).*

**Diagnostic Commands**

Go to **Diagnostic Commands (on page 309)** to view CLI commands which correspond to the web page entries described above.
Status/Reports

On this page, you can view the status of the SLB ports and power supplies and generate a selection of reports.

Note: Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, you must reload the web page.

1. Click the Maintenance tab and select the Status/Reports option. The following page displays:

   Figure 12-9 Maintenance > Status/Reports

   The top half of the page displays the status of each port, power supply, and power outlet:

   - **Green** indicates that the port connection or power supply is active and functioning correctly.
   - **Red** indicates an error or failure or that the device is off.

2. Select the desired reports to view under View Report:
View Report

<table>
<thead>
<tr>
<th>All</th>
<th>Displays all reports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Status</td>
<td>Displays the status of each device port: mode, user, any related connections, and serial port settings.</td>
</tr>
<tr>
<td>Port Counters</td>
<td>Displays statistics related to the flow of data through each device port.</td>
</tr>
<tr>
<td>IP Routes</td>
<td>Displays the routing table.</td>
</tr>
<tr>
<td>Connections</td>
<td>Displays all active connections for the SLB: Telnet, SSH, TCP, UDP, device port, and modem.</td>
</tr>
<tr>
<td>System Configuration – Complete</td>
<td>Displays a complete snapshot of the SLB settings.</td>
</tr>
<tr>
<td>System Configuration – Basic</td>
<td>Displays a snapshot of the SLB’s basic settings (for example, network, date/time, routing, services, console port).</td>
</tr>
<tr>
<td>System Configuration – Authentication</td>
<td>Displays a snapshot of authentication settings only (including a list of all local users).</td>
</tr>
<tr>
<td>System Configuration – Devices</td>
<td>Displays a snapshot of settings for each device port, USB Port, Modem, and Host Lists.</td>
</tr>
</tbody>
</table>

3. Click the Generate Report button. In the upper left of the Generated Status/Reports page displays a list of reports generated.

Figure 12-10 Generated Status/Reports

<table>
<thead>
<tr>
<th>Report(s):</th>
<th>Email Output</th>
<th>Comment:</th>
<th>to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Status</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. To email these report(s), follow the instructions in *Emailing Logs and Reports (on page 251)*.

**Status Commands**
Go to *Status Commands (on page 341)* to view CLI commands which correspond to the web page entries described above.

**Emailing Logs and Reports**
The following logs and reports can be directly emailed to a specific individual or to Lantronix Technical Support directly from the log page:

- System Log (i.e., *Figure 12-4*)
- Audit Log (i.e., *Figure 12-5*)
- Email Log (i.e., *Figure 12-6*)
- Diagnostic Reports (i.e., *Figure 12-8*)
- Status/Reports (i.e., *Figure 12-10*)

**To email a log to an individual:**

1. In the **Comment** field of a particular log or report page, enter a comment (if desired).
2. Select the **to** field beside the empty field where you then enter the person's email address.
3. Press the **Email Output** button. An email is immediately sent out and a confirmation appears on the screen.
Events

On this Maintenance > Events page, you can define what action you want to take for events that may occur in the SLB.

1. Click the Maintenance tab and select the Events option. The following page displays:
2. Enter the following:

**Event Trigger**
From the drop-down list, select the type of incident that triggers an event. Currently, the options are:
- Receive Trap
- Temperature Over/Under Limit (for Sensorsoft devices)
- Humidity Over/Under Limit (for Sensorsoft devices)
- Device Port Data Drop
- Current Over Threshold
- Power Inlet Status Change
- No Internal Modem Dial Tone

**Action**
From the drop-down list, select the action taken because of the trigger. For example, the action can be writing an entry into the syslog with details of the event or sending the trap(s) to the Ethernet or modem connection.

**Ethernet**
For actions that require an Ethernet connection (for example, Forward All Traps to Ethernet), select the Ethernet port to use.

**Modem Connection**
For actions that require a modem connection (for example, Forward All Traps to a Modem Connection), select which device port or USB port with a modem connection to use.

**NMS/Host to forward trap to**
For actions that forward a trap, enter the IP address of the computer to forward the trap to. The computer does not have to be an SNMP NMS; it just has to be capable of receiving SNMP traps.

**SNMP Community**
Forwarded traps are sent with this SNMP community value. There is no default.
3. You have the following options:
   - To add the defined event, click the **Add Event** button. The event displays in the Events table at the bottom of the page.
   - To edit an event, select the event from the Events table and click the **Edit Event** button. The *Maintenance > Events* page displays the event.
   - To delete an event, select the event from the Events table and click the **Delete Event** button. A message asks for confirmation. Click **OK**.

4) To save, click **Apply**.

**Events Commands**

Go to *Events Commands (on page 312)* to view CLI commands which correspond to the web page entries described above.

**LCD/Keypad**

The LCD has a series of screens, consisting of 2 lines of 24 characters each. Specific screens and the display order can be configured. The keypad associated with the LCD can also be configured. The types of screens include: current time, network settings, console settings, date and time, release version, location, and custom user strings.

Enabling the **Auto-Scroll LCD Screens** option enables scrolling through the screens and pausing the number of seconds specified by the **Scroll Delay** between each screen. After any input to the keypad, the LCD waits until the keypad has been idle for the number of seconds specified by the **Idle Delay** before scrolling of the screens continues.

**To configure the LCD and Keypad:**

1. Click the **Maintenance** tab and select the **LCD/Keypad** option.
To configure the LCD through the SLB user interface:

The screens that are currently enabled are displayed in order in the left Enabled screens list.

**Note:** See Front Panel LCD Display and Keypads (on page 41) to set up the basic parameters using the SLB unit.

1. Select a screen to be removed from the **Enabled Screens** and click the ➡️ button. The screen moves to the **Disabled Screens** list to the right.

2. Select a screen to be added from the **Disabled Screens** list and click the⬅️ button. The screen is added to the **Enabled Screens** to the left.

3. Select a screen in the **Enabled Screens** list and click the ⬆️ or ⬇️ button to change the order of the screens.

**Note:** The User Strings screen displays the 2 lines defined by the User Strings - Line 1 and Line 2 fields. By default, these user strings are blank.

4. Click **Apply** to save.
To configure the Keypad:

1. Enter the following fields.

<table>
<thead>
<tr>
<th>Keypad Locked</th>
<th>Select this to lock out any input to the keypad. The default is for the keypad to be unlocked.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore FactoryDefaults Password / Retype Password</td>
<td>Enter the 6 digit key sequence entered at the keypad to restore the SLB unit to factory defaults. The default is 999999.</td>
</tr>
</tbody>
</table>

2. Click Apply to save.

LCD/Keypad Commands

Go to Administrative Commands (on page 267) to view CLI commands which correspond to the web page entries described above.

Banners

The Maintenance > Banners page allows the system administrator to customize text messages that display to users.

To configure banner settings:

1. Click the Maintenance tab and select Banners option.

<table>
<thead>
<tr>
<th>Welcome Banner</th>
<th>The text to display on the web interface or command line interface before the user logs in. May contain up to 1024 characters. Single quote and double quote characters are not supported. Welcome to the SLB is the default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note:</td>
<td>To create more lines use the \n character sequence.</td>
</tr>
</tbody>
</table>
### System Info

The **System Info** page allows you to generate a ZIP file containing log data that can be used for debugging SLB or for sending to Lantronix Tech Support. The ZIP file contains network information, current configuration, logs, port information, and internal diagnostic information.

To generate the **System Info** file:

1. Click **Maintenance** and then click **System Info**. The **System Info** page appears.

---

<table>
<thead>
<tr>
<th>Login Banner</th>
<th>The text to display on the command line interface after the user logs in. May contain up to 1024 characters. Single quote and double quote characters are not supported. Default is blank.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> To create more lines, use the \n character sequence.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logout Banner</th>
<th>The text to display on the command line interface after the user logs out. May contain up to 1024 characters. Single quote and double quote characters are not supported. Default is blank.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> To create more lines use, the \n character sequence.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSH Banner</th>
<th>The text to display when a user logs into the SLB unit via SSH, prior to authentication. Single quote and double quote characters are not supported. May contain up to 1024 characters. Blank by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> To create more lines use the \n character sequence.</td>
<td></td>
</tr>
</tbody>
</table>
### 2. Enter the following information:

<table>
<thead>
<tr>
<th><strong>ZIP File Name</strong></th>
<th>The name of the System Info ZIP file, without the .zip extension. Up to 40 characters can be entered.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password to encrypt ZIP file/ Retype Password</strong></td>
<td>An optional password that can be used to encrypt the ZIP file, and will be required to unpack the ZIP file.</td>
</tr>
<tr>
<td><strong>Include System Logs</strong></td>
<td>If selected, will include all of the system log files in the ZIP file. This can significantly increase the size of the ZIP file.</td>
</tr>
<tr>
<td><strong>Save File via</strong></td>
<td>The method of saving the ZIP file. The available options are FTP, SFTP, SCP, HTTP, NFS, and USB. By default, FTP is the default selected. For NFS, a NFS share needs to be configured and mounted on the console manager. For information about NFS, see <a href="#">NFS and SMB/CIFS Commands</a>. For USB, external media needs to be present and mounted on the console manager. For information about USB, see <a href="#">Chapter 9: USB Port</a>.</td>
</tr>
<tr>
<td><strong>NFS Mounter Dir</strong></td>
<td>The mount directory of NFS. This option is available only when you select the NFS option in Save File via.</td>
</tr>
<tr>
<td><strong>USB Port</strong></td>
<td>Select the USB port to save the System Info file.</td>
</tr>
<tr>
<td><strong>FTP/SFTP/TFTP Server</strong></td>
<td>The IP address or host name of the server used for saving the System Info file. It may consist of 64 alphanumeric characters, hyphens, and underscores.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>The optional directory on the FTP/SFTP/SCP server to use for saving the ZIP file.</td>
</tr>
<tr>
<td><strong>Login/Password/ Retype Password</strong></td>
<td>The user login credentials of the FTP/SFTP/SCP server.</td>
</tr>
</tbody>
</table>

3. Click **Generate System Info File**. The **System Info ZIP** file is saved.
13: Application Examples

Each SLB branch office manager has multiple serial ports and two network ports. Each serial port can be connected to the console port of an IT device. Using a network port (in-band) or a modem (out-of-band) for dial-up connection, an administrator can remotely access any of the connected IT devices using Telnet or SSH.

This chapter includes three typical scenarios for using the SLB unit. The scenarios assume that the SLB unit is connected to the network and has already been assigned an IP address. In the examples, we use the command line interface. You can do the same things using the web page interface except for directly interacting with the SLB unit (direct command).

Telnet/SSH to a Remote Device

The following figure shows a Sun server connected to port 2 of the SLB.

In this example, the sysadmin would:
1. Display the current settings for device port 2:

   [SLB]> show deviceport port 2
   | Current Device Port
   | Settings________________________________________________
   | Number: 2 Name: Port-2
   | Modem Settings---------Data Settings--------IP Settings------
   | Modem State: disabled Baud Rate: 9600 Telnet: disabled
   | Modem Mode: text Data Bits: 8 Telnet Port: 2002
   | Timeout Logins: disabled Stop Bits: 1 SSH: disabled
   | Local IP: negotiate Parity: none SSH Port: 3002
   | Authentication: PAP Logins: disabled
   | CHAP Host: <none> Break Sequence: \x1bB
   | CHAP Secret: <none> Check DSR: disabled
   | NAT: disabled Close DSR: disabled
   | Dial-out Login: <none>
   | Dial-out Password: <none>
   | Dial-out Number: <none>
   | Dial-back Number: usernumber
   | Initialization Script: <none>

   Logging Settings-----------------------------------------------
   | Local Logging: disabled USB Logging: disabled
   | Email Logging: disabled Log to: upper slot
   | Byte Threshold: 100 Max number of files: 10
   | Email Delay: 60 seconds Max size of files: 2048
   | Restart Delay: 60 seconds
   | Email To: <none>
   | Email Subject: Port %d Logging
   | Email String: <none>
   | NFS File Logging: disabled
   | Directory to log to: <none>
   | Max number of files: 10
   | Max size of files: 2048

2. Change the baud to 57600 and disable flow control:

   [SLB]> set deviceport port 2 baud 57600 flowcontrol none
   Device Port settings successfully updated.

3. Connect to the device port:

   [SLB]> connect direct deviceport 2

4. View messages from the SUN server console:

   Mar 15 09:09:44 tssf280r sendmail[292]: [ID 702911 mail.info] starting daemon (8.12.2+Sun): SMTP-queueing@00:15:00
   Mar 15 09:09:44 tssf280r sendmail[293]: [ID 702911 mail.info] starting daemon (8.12.2+Sun): queueing@00:15:00
   Mar 15 14:44:40 tssf280r sendmail[275]: [ID 702911 mail.info] starting daemon (8.12.2+Sun): SMTP-queueing@00:15:00
   Mar 15 14:44:40 tssf280r sendmail[276]: [ID 702911 mail.info] starting daemon (8.12.2+Sun): queueing@00:15:00
5. Reboot the SUN server:

```
Reboot
<shutdown messages from SUN>
```

6. Use the escape sequence to escape from direct mode back to the command line interface.

---

### Dial-in (Text Mode) to a Remote Device

This example shows a modem connected to an SLB device port, and a Sun server connected to another SLB device port. You can configure the modem for text mode dial-in, so a remote user can dial into the modem using a terminal emulation program and access the Sun server. (HyperTerminal™, which comes with the Microsoft® Windows™ operating system, is an example of a terminal emulation program.)

![Figure 13-3 Dial-in (Text Mode) to a Remote Device](image)

In this example, the sysadmin would:

1. Configure the device port that the modem is connected to for dial-in:

   ```
   [SLB]> set deviceport port 1 modemmode text
   Device Port settings successfully updated.
   [SLB]> set deviceport port 1 initscript "AT&F&K3&C1&D2%C0A"
   Device Port settings successfully updated.
   [SLB]> set deviceport port 1 auth pap
   Device Port settings successfully updated.
   [SLB]> set deviceport port 1 localsecret "password"
   Device Port settings successfully updated.
   [SLB]> set deviceport port 1 modemstate dialin
   Device Port settings successfully updated.
   [SLB]>
   ```

2. Configure the device port that is connected to the console port of the Sun UNIX server:

   ```
   [SLB]> set deviceport port 2 baud 57600 flowcontrol none
   Device Port settings successfully updated.
   ```

3. Dial into the SLB branch office manager via the modem using a terminal emulation program on a remote PC. A command line prompt displays.

4. Log into the SLB.

```
CONNECT 57600
Welcome to the SLB
login: sysadmin
Password:
```
Welcome to the Secure Lantronix Branch Office Manager
Model Number: SLB882
For a list of commands, type 'help'.

[SLB]>

5. Connect to the SUN Unix server using the direct command.

[SLB] > connect direct deviceport 2
SunOS 5.7
login: frank
Password:
Last login: Wed Jul 14 16:07:49 from computer
Sun Microsystems Inc.SunOS 5.7Generic October 1998
SunOS computer 5.7 Generic_123485-05 sun4m sparc SUNW,SPARCstation-20
$

6. Use the escape sequence to escape from direct mode back to the command line interface.

Local Serial Connection to Network Device via Telnet

This example shows a terminal device connected to an SLB device port, and a Sun server connected over the network to the SLB. When a connection is established between the device port and an outbound Telnet session, users can access the Sun server as though they were directly connected to it. (See Chapter 10: Connections on page 190).

In this example, the sysadmin would:

1. Display the current settings for device port 2:

[SLB] > show deviceport port 2
__Current Device Port Settings__
Number: 2 Name: Port-2
Modem Settings-------------------Data Settings-------------------IP Settings-------------------
Modem State: disabled Baud Rate: 9600 Telnet: disabled
Modem Mode: text Data Bits: 8 Telnet Port: 2002
Timeout Logins: disabled Stop Bits: 1 SSH: disabled
Local IP: negotiate Parity: none SSH Port: 3002
Authentication: PAP Logins: disabled
CHAP Host: <none> Break Sequence: \x1BB
CHAP Secret: <none> Check DSR: disabled
NAT: disabled Close DSR: disabled
Dial-out Login: <none>
Dial-out Password: <none>
Dial-out Number: <none>
Dial-back Number: usernumber
Initialization Script: <none>

Logging Settings
-------------------
Local Logging: disabled   USB Logging: disabled
Email Logging: disabled   Log to: upper slot
Byte Threshold: 100      Max number of files: 10
Email Delay: 60 seconds  Max size of files: 2048
Restart Delay: 60 seconds
Email To: <none>
Email Subject: Port %d Logging
Email String: <none>
NFS File Logging: disabled
Directory to log to: <none>
Max number of files: 10
Max size of files: 2048

2. Change the serial settings to match the serial settings for the vt100 terminal - changes baud to 57600 and disables flow control:

[SLB]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.

3. Create a connection between the vt100 terminal connected to device port 2 and an outbound telnet session to the server. (The IP address of the server is 192.168.1.1):

[SLB]> connect bidirection 2 telnet 192.168.1.1
Connection settings successfully updated.

4. At the VT100 terminal, hit <return> a couple of times. The Telnet prompt from the server displays:

Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^[].

Sun OS 8.0
login:

At this point, a user can log in and interact with the Sun server at the VT100 terminal as if directly connected to the server.
14: Command Reference

After an introduction to using commands, this chapter lists and describes all of the commands available on the SLB command line interface accessed through Telnet, SSH, or a serial connection. The commands are in alphabetical order by category.

Introduction to Commands

Following is some information about command syntax, command line help, and tips for using commands.

Command Syntax

Commands have the following format:

```
<action> <category> <parameter(s)>
```

where

- `<action>` is set, show, connect, admin, diag, or logout.
- `<category>` is a group of related parameters whose settings you want to configure or view. Examples are ntp, deviceport, and network.
- `<parameter(s)>` is one or more name-value pairs in one of the following formats:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`&lt;parameter name&gt; &lt;aa</td>
<td>bb&gt;`</td>
</tr>
<tr>
<td><code>&lt;parameter name&gt; &lt;Value&gt;</code></td>
<td>User must specify an appropriate value, for example, an IP address. The parameter values are in mixed case. Square brackets [] indicate optional parameters.</td>
</tr>
</tbody>
</table>

**Table 14-1 Actions and Category Options**

<table>
<thead>
<tr>
<th>Action</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>accesslist</td>
</tr>
<tr>
<td>show</td>
<td>accesslist</td>
</tr>
<tr>
<td>connect</td>
<td>bidirection</td>
</tr>
<tr>
<td>diag</td>
<td>arp</td>
</tr>
</tbody>
</table>
Command Line Help

*For general Help and to display the commands to which you have rights, type:*

```
help
```

*For general command line Help, type:*

```
help command line
```

*For more information about a specific command, type help followed by the command, for example:*

```
help set network or help admin firmware
```

**Tips**

- Type enough characters to identify the action, category, or parameter name uniquely. For parameter values, type the entire value. For example, you can shorten:
  
  ```
  set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0
  ```
  
  to
  
  ```
  se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
  ```

- Use the Tab key to automatically complete action, category, or parameter names. Type a partial name and press Tab either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, Tab displays all possible names.

- Should you make a mistake while typing, backspace by pressing the Backspace key and/or the Delete key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the left and right arrow keys to move within a command.

- Use the up and down arrows to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.

- To clear an IP address, type 0.0.0.0, or to clear a non-IP address value, type CLEAR.

- When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until the user is ready to continue. To display the next line, press Enter, and to display the page, press the space bar. You can override the number of lines (or disable the feature altogether) with the set cli command.

- Keyboard Shortcuts:

  Control-a: move to the start of the line

<table>
<thead>
<tr>
<th>Action</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>banner</td>
</tr>
<tr>
<td>logout</td>
<td>Terminates CLI session.</td>
</tr>
</tbody>
</table>
Access List Commands

**set accesslist add|edit**

*Syntax*

set accesslist add|edit <Access List Name> [parameters]

*Parameters*

name <New Access List Name>
response <hangup|ignore>

*Description*

Configure an access list of phone numbers to be granted access for modem dial-in connections.
Create or edit an access list (when creating a list, the user will be prompted for the list entries):

**set accesslist add|edit**

*Syntax*

set accesslist add|edit <Access List Name>
entry <Entry Number> phonenumber <Phone Number>

*Description*

Add a phone number entry to a list or edit an existing entry:

**set accesslist delete**

*Syntax*

set accesslist delete <Access List Name> [entry <Entry Number>]

*Description*

Delete an access list, or a single phone number entry from an access list:
showaccesslist

Syntax
show accesslist <all|names|Access List Name>

Description
Show access list settings.

Administrative Commands

admin banner

Syntax
admin banner welcome <Banner Text>
admin banner login <Banner Text>
admin banner logout <Banner Text>
admin banner ssh <Banner Text>
admin banner show

Description
Configures the banners displayed prior to login (welcome), after login, after logout, or prior to SSH authentication. Line feeds can be inserted in the banner with the "\n" character sequence.

Note: To go to the next line, type \n and press Enter.

admin clear

Syntax
admin clear tmpdir

Description
Clears the directory holding temporary files.

Syntax
admin clear sshknownhosts

Description
Removes the SSH Known Hosts keys.
admin config save

Syntax

admin config save <Config Name> location
  <default|ftp|sftp|nfs|cifs|usb> [nfsdir <NFS Mounted Dir>]
  [usbport <u1>] [savesshkeys <enable|disable>]
  [savesslcert <enable|disable>] [savesscripts <enable|disable>]
  [onetimepassword <enable|disable>]

Description

Saves the current SLB configuration to a selected location.

admin config restore

Syntax

admin config restore <Config Name> location
  <default|ftp|sftp|nfs|cifs|usb> [nfsdir <NFS Mounted Dir>]
  [usbport <u1>] [savesshkeys <enable|disable>]
  [savesslcert <enable|disable>] [savesscripts <enable|disable>]
  [onetimepassword <enable|disable>]
  [preserveconfig <Config Params to Preserve>]

<Config Params to Preserve> is a comma-separated list of current configuration parameters to retain after the config restore or factorydefaults:

| nt | Networking |
| sv | Services   |
| dt | Date/Time  |
| po | Power Outlets |
| lu | Local Users |
| dp | Device Ports |
| ub | USB Port   |

Description

Restores a saved configuration to the SLB.
A reboot will automatically be done after a successful config restore or factorydefaults.

admin config factorydefaults

Syntax

admin config factorydefaults [savesshkeys <enable|disable>]
  [savesslcert <enable|disable>] [savesscripts <enable|disable>]
  [preserveconfig <Config Params to Preserve>]
<Config Params to Preserve> is a comma-separated list of current configuration parameters to retain after the config restore or factorydefaults:

| nt | Networking |
| sv | Services   |
| dt | Date/Time  |
| po | Power Outlets |
| lu | Local Users |
| dp | Device Ports |
| ub | USB Port    |

**Description**
Restores the SLB branch office manager to factory default settings. A reboot will automatically be done after a successful config restore or factorydefaults.

**admin config rename|delete**

**Syntax**

```
admin config rename|delete <Config Name> location <default|nfs|cifs|usb> [nfsdir <NFS Mounted Directory>] [usbport <u1>]
```

**Description**
Deletes or renames a configuration (the user is prompted for the new name for renames).

**admin config copy**

**Syntax**

```
admin config copy"<current|Config Name> [location <local|nfs|cifs|usb> [nfsdir <NFS Mounted Directory>] [usbport <u1>] ]
```

**Description**
Copies the current configuration (or optionally, a configuration from another location) to the other bank (for dual-boot SLBs).

**admin config show**

**Syntax**

```
admin config show <default|ftp|sftp|nfs|cifs|usb> [nfsdir <NFS Mounted Dir>] [usbport <u1>]
```

**Description**
Lists the configurations saved to a location.
**admin firmware update**

**Syntax**

```
admin firmware update <ftp|tftp|sftp|> file <Firmware File>
  key <Checksum Key> [nfsdir <NFS Mounted Directory>]
  [usbport <U1>] [onetimepassword <enable|disable>]
```

**Description**

Updates SLB firmware to a new revision.

You should be able to access the firmware file using the settings admin ftp show displays. The SLB branch office manager automatically reboots after successful update.

**admin firmware bootbank**

**Syntax**

```
admin firmware bootbank <1|2>
```

**Description**

Sets the boot bank to be used at the next SLB reboot.

**admin firmware copybank**

**Syntax**

```
admin firmware copybank
```

**Description**

Copies the boot bank from the currently booted bank to the alternate bank (for dual-boot SLBs).

**admin firmware show**

**Syntax**

```
admin firmware show [viewlog <enable|disable>]
```

**Description**

Lists the current firmware revision, the boot bank status (for dual-boot SLBs), and optionally displays the log containing details about firmware updates.
admin ftp password

Syntax
admin ftp password

Description
Sets the FTP server password and prevent it from being echoed.

admin ftp server

Syntax
admin ftp server <IP Address or Hostname> [login <User Login>] [path <Directory>]

Description
Sets the FTP/TFTP/SFTP server used for firmware updates and configuration save/restore. The following list includes options which accept the CLEAR command:

Note: CLEAR must be in all caps.

admin ftp login, path

admin ftp show

Syntax
admin ftp show

Description
Displays FTP settings.

admin keypad

Syntax
admin keypad <lock|unlock>

Description
Locks or unlocks the LCD keypad.
If the keypad is locked, you can scroll through settings but not change them.
admin keypad password

Syntax
admin keypad password <Password>
Must be 6 digits.

Description
Changes the Restore Factory Defaults password used at the LCD to return the SLB unit to the factory settings.

admin keypad show

Syntax
admin keypad show

Description
Displays keypad settings.

admin lcd reset

Syntax
admin lcd reset

Description
Restarts the program that controls the LCD.

admin memory

Syntax
admin memory swap add <Size of Swap in MB> [usbport <u1>]
admin memory swap delete
admin memory show

Description
Displays information about SLB memory usage and allows configuration of a swap space if available memory is low. Creates a swap space on the SLB disk or an external storage device. Deletes the swap space from the SLB disk or an external storage device.
admin quicksetup

Syntax
admin quicksetup

Description
Runs the quick setup script.

admin reboot

Syntax
admin reboot

Description
Reboots the SLB.
The front panel LCD displays the “Rebooting the SLB” message, and the normal boot sequence occurs.

admin shutdown

Syntax
admin shutdown

Description
Prepares the SLB branch office manager to be powered off.
When you use this command to shut down the SLB, the LCD front panel displays the “Shutting down the SLB” message, followed by a pause, and then “Shutdown complete.” When “Shutdown complete” displays, it is safe to power off the SLB. This command is not available on the Web page.

admin site

Syntax
admin site row <Data Center Rack Row Number>
admin site cluster <Data Center Rack Group Number>
admin site rack <Data Center Rack Number>
admin site tag <Site Description>
admin site show
Description

Configures information about the site the where SLB unit is located.

admin sysinfo

Syntax

admin sysinfo save <ZIP File Name>
location<ftp|sftp|scp|nfs|usb|sdcard>
[nfsdir <NFS Mounted Directory>]
[host <IP Address or Name>] [login <User Login>]
[path <Path to Save File>]
[comment <an optional comment describing the system info file being generated.>]

Description

Saves the current SLB system info to a selected location in ZIP format.

admin version

Syntax

admin version

Description

Displays current hardware and software version information.

admin web timeout

Syntax

admin web timeout <disable|5-120>

Description

Configures the timeout for web sessions.

admin web cipher

Syntax

admin web cipher <highest|high|himed>
Description
Configures the strength of the cipher used by the web server (high is 256 or 128 bit, medium is 128 bit)

**admin web sha2**

**Syntax**
admin web sha2 <enable|disable>

**Description**
Enable using only SHA2 or higher ciphers

**admin web tlsv10**

**Syntax**
admin web tlsv10 <enable|disable>

**Description**
Enables or disables TLS v1.0.

**admin web tlsv11**

**Syntax**
admin web tlsv11 <enable|disable>

**Description**
Enables or disables TLS v1.1.

**admin web gadget**

**Syntax**
admin web gadget <enable|disable>

**Description**
Enables or disables iGoogle Gadget web content.
admin web group

*Syntax*
admin web group <Local or Remote Group Name>

*Description*
Configures the group that can access the web.

admin web server

*Syntax*
admin web server <enable|disable>

*Description*
Enables or disables running the web server (TCP ports 80 and 443):

admin web banner

*Syntax*
admin web banner <Banner Text>

*Description*
Configures the banner displayed on the web home page.

admin web iface

*Syntax*
admin web iface <none,eth1,eth2,ppp>

*Description*
Defines a list of network interfaces the web is available on.

admin web terminate

*Syntax*
admin web terminate <Session ID>

*Description*
Terminates a web session.
admin web certificate

Syntax

admin web certificate import via <sftp|scp>
   [rootfile <Cert Authority File>] [certfile <Certificate File>]
   [privfile <Private Key File>] host <IP Address or Name>
   login <User Login> [path <Path to Files>]
admin web certificate reset
admin web certificate show

Description

Imports a SSL certificate, or reset the web server certificate to the default, or show the web server certificate.

admin web certificate custom

Syntax

admin web certificate custom

Description

Generate custom self-signed SSL certificate

admin web restart

Syntax

admin web restart

Description

Restart the web server:

admin web show

Syntax

admin web show [viewcipherlist <enable|disable>]
   [viewslmsessions <enable|disable>]

Description

Displays current settings, with optional extra sessions or current ciphers.

The following list includes options which accept the CLEAR command:
Note: CLEAR must be in all caps.

admin web group, banner

Audit Log Commands

show auditlog

Syntax

show auditlog [command|user|clear]

Description

Displays audit log. By default, shows the audit log sorted by date/time. You can sort it by user or command, or clear the audit log.

Authentication Commands

set auth

Syntax

set auth <one or more parameters>

Parameters

authusenextmethod <enable|disable>
kerberos <1-6>
ldap <1-6>
localusers <1-6>
nis <1-6>
radius <1-6>
tacacs+ <1-6>

Description

Sets ordering of authentication methods and how authentication methods are used. Authentication can occur using all methods, in the order of their precedence, until a successful authentication is obtained, or using only the first authentication method that responds (in the event that a server is down).

Local Users authentication is always the first method used. Any methods omitted from the command are disabled.
show auth

Syntax

show auth

Description
Displays authentication methods and their order of precedence.

show user

Syntax

show user

Description
Displays attributes of the currently logged in user.

Kerberos Commands

set kerberos

Syntax

set kerberos <one or more parameters>

Parameters

accessoutslets <Outlet List>
clearports <Port List>
custommenu <Menu Name>
dataports <Port List>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
group <default|power|admin>
ipaddr <Key Distribution Center IP Address>
kdc <Key Distribution Center>
listenports <Port List>
permissions <Permission List>

Note: See User Permissions Commands (on page 289) for information on groups and user rights.

port <Key Distribution Center TCP Port>
realm <Kerberos Realm>
state <enable|disable>
useldapforlookup <enable|disable>
Description

Configures the SLB device to use Kerberos to authenticate users who log in via the Web, SSH, Telnet, or the console port.

The following list includes options which accept the CLEAR command:

Note:  CLEAR must be in all caps.

set kerberos  realm, kdc, custommenu, escapeseq, breakseq, dialbacknumber, accessoutlets, listenports, dataports, clearports

show kerberos

Syntax

show kerberos

Description

Displays Kerberos settings.

LDAP Commands

set ldap

Syntax

set ldap <one or more parameters>

Set the LDAP bind password (any extra parameters will be ignored):

set ldap bindpassword

Parameters

state <enable|disable>
server <IP Address or Name>
port <TCP Port>
base <LDAP Base>
bindname <Bind Name>
bindwithlogin <enable|disable>
useldapschema <enable|disable>
adsupport <enable|disable>
filteruser <User Login Attribute>
filtergroup <Group Objectclass>
grmemberattr <Group Membership Attribute>
grmembervalue <dn|name>
encrypt <enable|disable>
 dataports <Port List>
listenports <Port List>
clearports <Port List>
accessoutlets <Outlet List>
escapeseq <1-10 Chars>
breakseq <1-10 Chars>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
group <default|power|admin>
permissions <Permission List>
Default is 389.

**Note:** See User Permissions Commands (on page 289) for information on groups and user rights.

**Description**

Configures the SLB branch office manager to use LDAP to authenticate users who log in via the Web, SSH, Telnet, or the console port.

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

```
set ldap custommenu, escapeseq, breakseq, dialbacknumber, base, bindname, bindpassword, filteruser, filtergroup, grmemberattr, accessoutlets, listenports, dataports, clearports
```

```
show ldap
```

**Syntax**

```
show ldap
```

**Description**

Displays LDAP settings:

**Local Users Commands**

```
set localusers state
```

**Syntax**

```
set localusers state <enable|disable>
```
**Description**

Enables or disables authentication of local users. Configure local accounts (including sysadmin) to authenticate users who login to the SLB via SSH, Telnet, the Web or the Console Port.

```plaintext
set localusers add|edit
```

**Syntax**

```plaintext
set localusers add|edit <User Login> <one or more parameters>
```

**Parameters**

- `accessoutlets <Outlet List>`
- `allowdialback <enable|disable>`
- `breakseq <1-10 Chars>`
- `changernextlogin <enable|disable>`
- `changepassword <enable|disable>`
- `clearports <Port List>`
- `dataports <Port List>`
- `dialbacknumber <Phone Number>`
- `displaymenu <enable|disable>`
- `escapeseq <1-10 Chars>`
- `listenports <Port List>`
- `custommenu <Menu Name>`
- `uid <User Identifier>`
- `group <default|power|admin|Custom Group Name>`
- `passwordexpires <enable|disable>`
- `permissions <Permission List>`

**Note:**

- See User Permissions Commands (on page 289) for information on groups and user rights.
- Remove Escape and Break Sequences for users making raw binary connections to Device Ports.

**Description**

Configures local accounts (including sysadmin) who log in to the SLB unit by means of the Web, SSH, Telnet, or the console port.

The following list includes options which parameters accept the CLEAR command:

```plaintext
CLEAR must be in all caps.
```

```plaintext
set localusers custommenu, escapeseq, breakseq, dialbacknumber, accessoutlets, listenports, dataports, clearports
```
set local users

Syntax
set localusers complexpasswords <enable|disable>

Description
Sets whether a complex login password is required.

Syntax
set localusers allowreuse <enable|disable>

Description
Sets whether a login password can be reused.

Note: Password reuse is insecure.

Syntax
set localusers reusehistory <Number of Passwords>

Description
Sets the number of passwords the user must use before reusing an old password. The default is 4.

Syntax
set localusers lifetime <Number of Days>

Description
Sets the number of days the login password may be used. The default is 90 days.

Syntax
set localusers periodwarning <Number of Days>

Description
Sets the number of days the system warns the user that the password will be expiring. The default is 7 days.

Syntax
set localusers maxloginattempts <Number of Logins>

Description
Sets the maximum number of login attempts before the account is locked. Disabled by default.
**Syntax**

set localusers periodlockout <Number of Minutes>

**Description**

Sets the number of minutes after a lockout before the user can try to log in again. Disabled by default.

**Syntax**

set localusers multipleadminlogins <enable|disable>

**Description**

Sets whether the sysadmin is allowed to have multiple simultaneous logins to the web interface. Disabled by default.

**Syntax**

set localusers consoleonlyadmin <enable|disable>

**Description**

Sets whether to limit sysadmin logins to the physical SLB Console Port only. Disabled by default.

**set localusers password**

**Syntax**

set localusers password <User Login>

**Description**

Sets a login password for the local user.

**set localusers delete**

**Syntax**

set localusers delete <User Login>

**Description**

Deletes a local user.
show localusers

**Syntax**

show localusers [user <User Login>]

**Description**

Displays local users.

**NIS Commands**

set nis

**Syntax**

set nis <one or more parameters>

**Parameters**

accessoutlets <Outlet List>
broadcast <enable|disable>
clearports <Port List>
custommenu <Menu Name>
dataports <Port List>
domain <NIS Domain Name>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
group <default|power|admin>
listenports <Port List>
master <IP Address or Hostname>
permissions <Permission List>

**Note:** See User Permissions Commands on page 289 for information on groups and user rights.

slave1 <IP Address or Hostname>
slave2 <IP Address or Hostname>
slave3 <IP Address or Hostname>
slave4 <IP Address or Hostname>
slave5 <IP Address or Hostname>
state <enable|disable>

**Description**

Configures the SLB branch office manager to use NIS to authenticate users who log in via the Web, SSH, Telnet, or the console port.

The following list includes options which accept the CLEAR command:
**Note:** CLEAR must be in all caps.

```
set nis
custommenu, escapeseq, breakseq, dialbacknumber, domain, accessoutlets, listenports, dataports, clearports
```

```
show nis
```

**Syntax**
```
show nis
```

**Description**
Displays NIS settings.

### RADIUS Commands

```
set radius
```

**Syntax**
```
set radius <one or more parameters>
```

**Parameters:**
- `accessoutlets <Outlet List>`
- `state <enable|disable>`
- `clearports <Port List>`
- `custommenu <Menu Name>`
- `dataports <Port List>`
- `breakseq <1-10 Chars>`
- `escapeseq <1-10 Chars>`
- `group <default|power|admin>`
- `listenports <Port List>`
- `permissions <Permission List>`

**Note:** See User Permissions Commands on page 289 for information on groups and user rights.

```
timeout <enable|1-30>
```

**Note:** Sets the number of seconds after which the connection attempt times out. It may be 1-30 seconds.
**Description**

Configures the SLB branch office manager to use RADIUS to authenticate users who log in via the Web, SSH, Telnet, or the console port.

```
set radius server
```

**Syntax**

```
set radius server <1|2> host <IP Address or Hostname> secret <Secret> [port <TCP Port>]
```

**Description**

Identifies the RADIUS server(s), the text secret, and the number of the TCP port on the RADIUS server.

*Note:* The default port is 1812.

The following list includes options which accept the CLEAR command:

*Note:* CLEAR must be in all caps.

```
set radius custommenu, escapeseq, breakseq, dialbacknumber, secret, accessoutlets, listenports, dataports, cleardrops
```

```
show radius
```

**Syntax**

```
show radius
```

**Description**

Displays RADIUS settings.

**TACACS+ Commands**

```
set tacacs+
```

**Syntax**

```
set tacacs+ <one or more parameters>
```

**Parameters**

```
accessoutlets <Outlet List>
```
allowdialback <enable|disable>
authservice <login|pap|chap>
breaqseq <1-10 Chars>
clearports <Port List>
custommenu <Menu Name>
dataports <Port List>
dialbacknumber <Phone Number>
encrypt <enable|disable>
escapeseq <1-10 Chars>
group <default|power|admin>
listenports <Port List>
permissions <Permission List>
protocol <Protocol for Service>
service <IP Address or Name>
server1 <IP Address or Name>
server2 <IP Address or Name>
server3 <IP Address or Name>
state <enable|disable>
timeout <1-10 seconds>

**Note:** See User Permissions Commands (on page 289) for information on groups and user rights.

Set the TACACS+ secret (any extra parameters will be ignored):

```
set tacacs+ secret
show tacacs+
```

**Description**

Configures the SLB unit to use TACACS+ to authenticate users who log in via the Web, SSH, Telnet, or the console port.

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

```
set tacacs+ custommenu, escapeseq, breakseq, dialbacknumber, secret, accessoutlets, listenports, dataports, clearports
```

**Show tacacs+**

**Syntax**

```
show tacacs+
```

**Description**

Displays TACACS+ settings.
User Permissions Commands

set localusers group

Syntax
set localusers add|edit <user> group <default|power|admin>

Description
Adds a local user to a user group or changes the group the user belongs to.

set localusers lock

Syntax
set localusers lock <User Login>

Description
Blocks (locks) a user's ability to login.

set localusers unlock

Syntax
set localusers unlock <User Login>

Description
Allows (unlocks) a user's ability to login.

set localusers permissions

Syntax
set localusers add|edit <user> permissions <Permission List>
where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, do, ub, dp, do, ub, rs, rc, dr, wb, sn, ad, po

To remove a permission, type a minus sign before the two-letter abbreviation for a user permission.

Description
Sets a local user's permissions (not defined by the user group).
set remoteusers add|edit

**Syntax**

set remoteusers add|edit <User Login> [<parameters>]

**Parameters**

accessoutlets <Outlet List>
dataports <Port List>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
listenports <Port List>
clearports <Port List>
go<default|power|admin|Custom Group Name>
permissions <Permissions List>

**where**

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, do, ub, rs, rc, dr, wb, sn, ad, po

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

**Description**

Sets attributes for users who log in by a remote authentication method.

**set remoteusers listonlyauth**

**Syntax**

set remoteusers listonlyauth <enable|disable>

**Description**

Sets whether remote users who are not part of the remote user list will be authenticated.

**set remoteusers delete**

**Syntax**

set remoteusers delete <User Login>

**Description**

Removes a remote user.
show remoteusers

Syntax
show remoteusers

Description
Displays settings for all remote users
The following list includes options which accept the CLEAR command:

Note: CLEAR must be in all caps.

set remoteusers custommenu, escapeshq, breakseq, dialbacknumber, accessoutlets, listenports, dataports, clearports

set <nis|ldap|radius|kerberos|tacacs+> group

Syntax
set <nis|ldap|radius|kerberos|tacacs> group <default|power|admin>

Description
Sets a permission group for remotely authorized users.

set <nis|ldap|radius|kerberos|tacacs+> permissions

Syntax
set <nis|ldap|radius|kerberos|tacacs> permissions <Permission List>
where
<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, do, ub, rs, rc, dr, wb, sn, ad, po

Description
Sets permissions not already defined by the assigned permissions group.

show user

Syntax
show user

Description
Displays the rights of the currently logged-in user:
CLI Commands

**set cli**

**Syntax**

set cli scscommands <enable|disable>

Commands:  
info         direct <Device Port # or Name>
version      listen <Device Port # or Name>
reboot       clear <Device Port # or Name>
poweroff     telnet <IP Address or Name>
listdev      ssh <IP Address or Name>

**Parameters**

set cli scscommands <enable|disable>  
set cli terminallines <disable|Number of Lines>  
set cli menu <start|Menu Name>  
show cli

**Description**

Allows you to use SCS-compatible commands as shortcuts for executing commands. Enabling this feature enables it only for the current cli session. It is disabled by default.

**Note:** Settings are retained between CLI sessions for local users and users listed in the remote users list.

**set cli terminallines**

**Syntax**

set cli terminallines <disable|Number of lines>

**Description**

Sets the number of lines in the terminal emulation (screen) for paging through text one screenful at a time, if the SLB device cannot detect the size of the terminal automatically.

**Note:** Settings are retained between CLI sessions for local users and users listed in the remote users list.

**set localusers lock**

**Syntax**

set localusers lock <User Login>
**Description**

Block (lock out) a user's ability to log in.

```
set localusers unlock
```

**Syntax**

```
set localusers unlock <User Login>
```

**Description**

Allow (unlock) a user's ability to log in.

```
show cli
```

**Syntax**

```
show cli
```

**Description**

Displays current CLI settings.

```
show user
```

**Syntax**

```
show user
```

**Description**

Displays attributes of the currently logged in user.

```
set history clear
```

**Description**

Clears the commands that have been entered during the command line interface session.
show history

Syntax

show history

Description

Displays the last 100 commands entered during the session.

Connection Commands

call connect bidirection

Syntax

connect bidirection <Port # or Name> <endpoint> <one or more Parameters>

Parameters

Endpoint is one of:
charcount <# of Chars>
charseq <Char Sequence>
charxfer <toendpoint|fromendpoint>
date <MMDDYYhhmm[ss]>
deviceport <Device Port # or Name>
exclusive <enable|disable>
ssh <IP Address or Name> [port <TCP Port>] [<SSH flags>]

where <SSH flags> is one or more of:
user <Login Name>
version <1|2>
command <Command to Execute>

ver">KR"Cfftguu@"|rgtv">VER"Rqttv@
telnet <IP Address or Name> [port <TCP Port>]
trigger <now|datetime|chars>

If the trigger is datetime (establish connection at a specified date/time), enter the date parameter. If the trigger is chars (establish connection on receipt of a specified number or characters or a character sequence), enter the charxfer parameter and either the charcount or the charseq parameter.

udp <IP Address> [port <UDP Port>]

Description

Connects a device port to another device port or an outbound network connection (data flows in both directions).
**connect direct**

**Syntax**

```bash
connect direct <endpoint>
```

**Parameters**

Endpoint is one of:
- `deviceport <Device Port # or Name>`
- `ssh <IP Address or Name> [port <TCP Port>] [SSH flags]`
  where `<SSH flags>` is one or more of:
  - `user <Login Name>`
  - `version <1|2>`
  - `command <Command to Execute>`
- `tcp <IP Address> [port <TCP Port>]`
- `telnet <IP Address or Name> [port <TCP Port>]`
- `udp <IP Address> [port <UDP Port>]`

**Description**

Connects to a device port to monitor and/or interact with it, or establishes an outbound network connection.

**connect global outgoingtimeout**

**Syntax**

```bash
connect global outgoingtimeout <disable|1-9999 seconds>
```

**Description**

Sets the amount of time the SLB branch office manager will wait for a response (sign of life) from an SSH/Telnet server that it is trying to connect to.

*Note:* This is not a TCP timeout.

**connect listen deviceport**

**Syntax**

```bash
connect listen deviceport <Device Port # or Name>
```

**Description**

Monitors a device port.
**connect terminate**

**Syntax**

connect terminate <Connection ID>

**Description**

Terminates a bidirectional or unidirectional connection.

**connect unidirection**

**Syntax**

connect unidirection <Device Port # or Name> dataflow <toendpoint> <fromendpoint> <endpoint>

**Parameters**

*Endpoint is one of:*
charcount <# of Chars>
charseq <Char Sequence>
datetime <MMDDYYhhmm[ss]>
deviceport <Port # or Name>
exclusive <enable|disable>
ssh <IP Address or Name> [port <TCP Port>][<SSH flags>]

`where <SSH flags> is one or more of:`
user <Login Name>
version <1|2>
command <Command to Execute>
tcp <IP Address> [port <TCP Port>]
telnet <IP Address or Name> [port <TCP Port>]
trigger <now|datetime|chars>

*If the trigger is datetime (establish connection at a specified date/time), enter the date parameter. If the trigger is chars (establish connection on receipt of a specified number or characters or a character sequence), enter either the charcount or the charseq parameter.*

udp <IP Address> [port <UDP Port>]

**Description**

Connects a device port to another device port or an outbound network connection (data flows in one direction).

**show connections**

**Syntax**

show connections [email <Email Address>]

---

*SLB™ Branch Office Manager User Guide*
Description
Displays connections and their IDs. You can optionally email the displayed information.
The connection IDs are in the left column of the resulting table. The connection ID associated with a particular connection may change if the connection times out and is restarted.

show connections connid

Syntax
show connections connid <Connection ID> [email <Email Address>]

Description
Displays details for a single connection. You can optionally email the displayed information.
ConsoleFlow Commands

**set cflow client**

*Syntax*

```
set cflow client <enable|disable>
```

*Description*
Configure interaction with ConsoleFlow management server. The communication with the server is enabled by default, and can be disabled.

**set cflow statusinterval**

*Syntax*

```
set cflow statusinterval <1-60 minutes> fwconfiginterval <1-72 hours>
```

*Description*
Set interval between status updates, and firmware and configuration checks.

**set cflow fwupdate**

*Syntax*

```
set cflow fwupdate <enable|disable> configupdate <enable|disable>
```

*Description*
Enable or disable firmware and configuration updates via ConsoleFlow.

**set cflow rebootafterupdate**

*Syntax*

```
set cflow rebootafterupdate <enable|disable>
```

*Description*
Enable or disable reboots after firmware or configuration updates.

**set cflow auditlogmessages**

*Syntax*

```
set cflow auditlogmessages <enable|disable>
```

*Description*
Enable or disable sending audit log messages.
set cflow connection

Syntax

set cflow connection <cloud|onpremise> [one or more parameters]

Parameters

host <IP Address or Name>
port <TCP Port>
secureport <enable|disable>
validatecerts <enable|disable>
mqttstate <enable|disable>

Description

Configure ConsoleFlow Cloud or On-Premise settings.

set cflow devicename

Syntax

set cflow devicename <Device Name> description <Device Description>

Description

Configure the device name and description used for registration.

set cflow timeoutcli

Syntax

set cflow timeoutcli <1-1800 seconds>
set cflow timeoutdp <1-1800 seconds>

Description

Configure the timeout for the ConsoleFlow Web Terminal sessions.

set cflow id

Syntax

set cflow id

Description

Set the device ID.

set cflow key

Syntax

set cflow key
**Description**
Set the Device key

```
set cflow clear updatelog
```

**Syntax**
```
set cflow clear updatelog
```

**Description**
Clear the Firmware/Config updates log

```
show cflow
```

**Syntax**
```
show cflow
show cflow status
show cflow perfmon
show cflow scripts
show cflow clicommands
```

**Description**
Show ConsoleFlow settings

---

**Console Port Commands**

```
set consoleport
```

**Syntax**
```
set consoleport <one or more parameters>
```

**Parameters**
- **baud** <300-115200>
- **databits** <7|8>
- **flowcontrol** <none|xon/xoff|rts/cts>
- **group** <Local or Remote Group Name>
- **parity** <none|odd|even>
- **showlines** <enable|disable>
- **stopbits** <1|2>
- **timeout** <disable|1-30>

**Description**
Configures console port settings.
show consoleport

**Syntax**

show consoleport

**Description**

Displays console port settings.
The following list includes options which accept the CLEAR command:

**Note:** CLEAR *must be in all caps.*

console port group

---

**Custom User Menu Commands**

When creating a custom user menu, note the following limitations:

- Maximum of 20 custom user menus.
- Maximum of 50 commands per custom user menu (*logout* is always the last command).
- Maximum of 15 characters for menu names.
- Maximum of five nested menus can be called.
- No syntax checking. (Enter each command correctly.)

**set localusers**

**Syntax**

set localusers add|edit <User Login> menu <Menu Name>

**Description**

Assigns a custom user menu to a local user.

**set menu add**

**Syntax**

set menu add <Menu Name> [command <Command Number>]

**Description**

Creates a new custom user menu or adds a command to an existing custom user menu.
set menu edit

Syntax
set menu edit <Menu Name> <parameter>

Parameters
command <Command Number>
nickname <Command Number>
redisplaymenu <enable|disable>
shownicknames <enable|disable>
title <Menu Title>

Description
Changes a command within an existing custom user menu.
Changes a nickname within an existing custom user menu.
Enables or disables the redisplay of the menu before each prompt.
Enables or disables the display of command nicknames instead of commands.
Sets the optional title for a menu.

set menu delete

Syntax
set menu delete <Menu Name> [command <Command Number>]

Description
Deletes a custom user menu or one command within a custom user menu.
The following list includes options which accept the CLEAR command:

Note:  CLEAR must be in all caps.

set menu edit nickname

set <nis|ldap|radius|kerberos|tacacs+> custommenu

Syntax
set <nis|ldap|radius|kerberos|tacacs> custommenu <Menu Name>

Description
Sets a default custom menu for remotely authorized users.
show menu

**Syntax**

show menu <all|Menu Name>

**Description**

Displays a list of all menu names or all commands for a specific menu.

---

**Date and Time Commands**

**set datetime**

**Syntax**

set datetime <one date/time parameter>

**Parameters**

date <MMDDYYhhmm[ss]>

timezone <Time Zone>

**Note:** If you type an invalid time zone, the system guides you through the process of selecting a time zone.

**Description**

Sets the local date, time, and local time zone (one parameter at a time).

**show datetime**

**Syntax**

show datetime

**Description**

Displays the local date, time, and time zone.

**set ntp**

**Syntax**

set ntp <one or more ntp parameters>
**Parameters**

localserver1 <IP Address or Hostname>
localserver2 <IP Address or Hostname>
localserver3 <IP Address or Hostname>
poll <local|public>
publicserver <IP Address or Hostname>
state <enable|disable>
sync <broadcast|poll>

**Description**

Synchronizes the SLB branch office manager with a remote time server using NTP.

```
show ntp
```

**Syntax**

```
show ntp
```

**Description**

Displays NTP settings.

**Device Commands**

```
set command
```

**Syntax**

```
set command <Device Port # or Name or List> <one or more parameters>
```

**Parameters**

slp auth login <User Login>
Establishes the authentication information to log into the SLP power manager attached to the device port.
slp restart
Issues the CLI command the SLP device uses to restart itself.
slp outletcontrol state <on|off|cyclepower> [outlet <Outlet #>][tower <A|B>]
Outlet # is 1-8 for SLP8 and 1-16 for SLP16 units.
The outletcontrol parameters control individual outlets.
slp outletstate [outlet <Outlet #>]
The outletstate parameter shows the state of all outlets or a single outlet.
slp envmon
Displays the environmental status (e.g., temperature and humidity) of the SLP power manager.

slp infeedstatus
Displays the infeed status and load of the SLP unit.

slp system
Provides system information for the SLP power manager.

sensorsoft lowtemp <Low Temperature in C.>
Sets the lowest temperature permitted for the port.

sensorsoft hightemp <High Temperature in C.>
Sets the highest temperature permitted for the port.

sensorsoft lowhumidity <Low Humidity %>
Sets the lowest humidity permitted for the port.

sensorsoft highhumidity <High Humidity %>
Sets the highest humidity permitted for the port.

sensorsoft traps <enable|disable>
Enables or disables traps when specified conditions are met.

sensorsoft status
Displays the status of the port.

Description
Sends commands to (or control) a device connected to an SLB device port over the serial port.

Note: Currently the only devices supported for this type of interaction are the SLP power manager and Sensorsoft devices.

Device Port Commands

set deviceport port

Syntax
set deviceport port <Device Port # or List or Name> <one or more parameters>

Example
set deviceport port 2-5,6,12,15-16 baud 2400 locallogging enable

Parameters
auth <pap|chap>
banner <Banner Text>
baud <300-230400>
breakseq <1-10 Chars>
calleridcmd <Modem Command String>
calleridlogging <enable|disable>
cbcpnocallback <enable|disable>
cbctype <admin|user>
chapauth <chaphost|localusers>
chaphost <CHAP Host or User Name>

*The user defines the secret.*

checkdsrc <enable|disable>
closedsrc <enable|disable>
databits <7|8>
device <none|slp8|slp16|slp8|exp8|slp8exp16||exp8|slp8exp16|slp16exp8
|slp16exp16|sensorsoft|servertech>
dialback+ondemand|cbcpclient|cbcpserver>
dialbackdelay <PPP Dial-back Delay>
dialbacknumber <username|Phone Number>
dialbackretries <1-10>
dialinhostlist|dialondemand|dialin+ondemand|
dialinlist <Host List for Dial-in>
dialoutnumber <Phone Number>
dialoutlogin <Remote User Login>
dialbacknumber <username|Phone Number>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
emaildelay <Email Delay>
emaillogging <disable|bytecnt|charstr>
emailrestart <Restart Delay>
emailsend <email|trap|both>
emailstring <Regex String>
emailsubj <Email Subject>
emailthreshold <Threshold>
emailto <Email Address>
flowcontrol <none|xon/xoff|rts/cts>
group <Local or Remote Group Name>
idletimeout <disable|1-9999 seconds>
ipaddr <IP Address>
initscript <Initialization Script>

*A script that initializes a modem.*

localipaddr <negotiate|IP Address>
locallogging <enable|disable>
logins <enable|disable>
maxdirect <1-10>
maxdirect <1-10>
modemmode <text|ppp>
modemstate <disable|dialout|dialin|dialback|dialondemand|
dialin+dialondemand|dialinhostlist>
modemtimeout <disable|1-9999 seconds>
name <Device Port Name>
nat <enable|disable>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmaxfiles <Max # of Files>
nfsmaxsize <Size in Bytes>
parity <none|odd|even>
portlogseq <1-10 Chars>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
showlines <enable|disable>
slmlogging <enable|disable>
slmmms <NMS IP Address>
slmthreshold <Threshold>
slmtime <Time Frame>
sshauth <enable|disable>
sshin <enable|disable>
sshoport <TCP Port>
sshtimeout <disable|1-1800 seconds>
stopbits <1|2>
sysloglogging <enable|disable>
tcpauth <enable|disable>
tcpin <enable|disable>
tcpport <TCP Port>
tcptimeout <disable|1-1800 seconds>
telnetauth <enable|disable>
telnetin <enable|disable>
telnetport <TCP Port>
telnettimeout <disable|1-1800 sec>
timeoutlogins <disable or 1-30>
usblogging <enable|disable>
usbmaxfiles <Max # of Files>
usbmaxsize <Size in Bytes>
usbport <U1>
usesites <enable|disable>
viewportlog <enable|disable>

Description

Configures a single port or a group of ports.

set deviceport global

Syntax

set deviceport global <one or more parameters>

Parameters

uujrqtv">VER"Rqtv@
telnetport <TCP Port>
tcpport <TCP Port>
maxdirect <1-10>

Description

Configures settings for all or a group of device ports.
The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

```
set deviceport dialinlist, nfslir, nfslir, breakseq, banner, group, portlogseq, chaphost, chapsecret, dodchaphost, dodchapsecret, initscript, dialoutlogin, dialbacknumber, emailsubj, emailstring, emailto
```

**show deviceport global**

**Syntax**

```
show deviceport global
```

**Description**
Displays global settings for device ports.

**show deviceport names**

**Syntax**

```
show deviceport names
```

**Description**
Displays a list of all device port names.

**show deviceport port**

**Syntax**

```
show deviceport port <Device Port List or Name>
```

**Description**
Displays the settings for one or more device ports.

**show portcounters**

**Syntax**

```
show portcounters [deviceport <Device Port List or Name>] [email <Email Address>]
```
**Description**

Displays device port statistics and errors for one or more ports. You can optionally email the displayed information.

`show portcounters zerocounters`

**Syntax**

`show portcounters zerocounters <Device Port List or Name>`

**Description**

Zeros the port counters for one or more device ports.

`show portstatus`

**Syntax**

`show portstatus [deviceport <Device Port List or Name>] [email <Email Address>]`

**Description**

Displays the modes and states of one or more device port(s). You can optionally email the displayed information.

**Diagnostic Commands**

`diag arp`

**Syntax**

`diag arp [email <Email Address>]`

**Description**

Displays the ARP table of IP address-to-hardware address mapping. You can optionally email the displayed information.

`diag internals`

**Syntax**

`diag internals`
**Description**

Displays information on the internal memory, storage and processes of the SLB.

**Note:** This command is available in the CLI but not the web.

```bash
diag netstat
```

**Syntax**

diag netstat [protocol <all|tcp|udp>] [email <Email Address>]

**Description**

To display a report of network connections. You can optionally email the displayed information.

```bash
diag nettrace
```

**Syntax**

diag nettrace <one or more parameters>

**Parameters**

- ethport <1|2>
- protocol <tcp|udp|icmp|esp>
- host <IP Address or Name>
- numpackets <Number of Packets>
- verbose <low|medium|high|disable>
- pcapfile <File Name>
- usbport <U1>

**Description**

Displays all network traffic, applying optional filters. This command is not available on the web page.

```bash
diag lookup
```

**Syntax**

diag lookup <Hostname> [email <Email Address>]

**Description**

Resolves a host name into an IP address. You can optionally email the displayed information.
**diag loopback**

**Syntax**

```
diag loopback <Device Port Number or Name>[<parameters>]
```

**Parameters**

```
test <internal|external>
xferdatasize <Size In Kbytes to Transfer>
```

Default is 1 Kbyte.

**Description**

Tests a device port by transmitting data out the port and verifying that it is received correctly.

A special loopback cable comes with the SLB. To test a device port, plug the cable into the device port and run this command. The command sends the specified Kbytes to the device port and reports success or failure. The test is performed at 9600 baud. Only an external test requires a loopback cable.

**End Device Commands**

**set command**

**Syntax**

```
set command <Device Port # or Name or List> <one or more parameters>
```

**Parameters**

```
slp auth login <User Login>
```

Establishes the authentication information to log into the SLP power manager attached to the device port.

```
slp envmon
```

Displays the environmental status (e.g., temperature and humidity) of the SLP.

```
slp outletcontrol state <on|off|cyclepower> [outlet <Outlet #>]
```

Outlet # is 1-8 for SLP8 and 1-16 for SLP16. The `outletcontrol` parameters control individual outlets.

```
slp outletstate [outlet <Outlet #>]
```

Shows the state of all outlets or a single outlet.

```
slp restart
```

Issues the CLI command the SLP uses to restart itself.

```
slp system
```

Displays system information for the SLP.
**Description**

Sends commands to (or controls) a device connected to an SLB device port over the serial port. Currently the only type of device supported for this type of interaction is the SLP device.

**Events Commands**

**admin events add**

**Syntax**

admin events add <trigger> <response>

<trigger> is one of:

- receivetraps, templimit, humidlimit, overcurrent, inletstatus, nomodemodial, or dpdatadrop.

<response> is one of:

- action <fwdalltrapseth|fwdseltrapseth> ethport <1|2> nms <SNMP NMS> community <SNMP Community> [oid <SNMP OID>]
- action <fwdalltrapsetsmodem|fwdseltrapsetsmodem> deviceport <Device Port # or Name> nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
- action <fwdalltrapsetsmodem|fwdseltrapsetsmodem> wudrqtv <u1> nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
- action <syslog>

**Description**

Defines events.

**admin events delete**

**Syntax**

admin events delete <Event ID>

**Description**

Deletes an event definition.

**admin events edit**

**Syntax**

admin events edit <Event ID> <parameters>
### Parameters

- `community <SNMP Community>`
- `deviceport <Device Port # or Name>`
- `ethport <1|2>`
- `nms <SNMP NMS>`
- `oid <SNMP Trap OID>`
- `wudrqtv <u1>`

### Description

Edits event definitions.

**admin events show**

#### Syntax

`admin events show`

#### Description

Displays event definitions.

---

### Global Commands

**set deviceport global**

#### Syntax

`set deviceport global <one or more parameters>`

#### Parameters

- `sshoprt <TCP Port>`
- `tcpport <TCP Port>`
- `telnetport <TCP Port>`

*Port is a port number between 1025 and 65528.*

To view global settings for device ports:

`show deviceport global`

#### Description

Configures settings for all or a group of device ports.
Group Commands

**set groups**

**Syntax**

```
set groups add|edit <Group Name> [parameters]
```

**Parameters**

```
dataports <Port List>
listenports <Port List>
clearports <Port List>
accessoutlets <Outlet List>
escapeseq <1-10 Chars>
brakeseq <1-10 Chars>
custommenu <Menu Name>
displaymenu <enable|disable>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
permissions <Permission List>
```

**Note:** See 'help user permissions' for information on user rights.

Rename a group:

```
set groups rename <Group Name> newname <New Group Name>
```

Delete a group:

```
set groups delete <Group Name>
show groups [name <Group Name>] members <enable|disable>
```

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

```
set groups custommenu, escapeseq, breakseq, dialbacknumber, outletlist, listenports, dataports, clearports
```
Host List Commands

```
set hostlist add|edit <Host List Name>"
```

**Syntax**

```
set hostlist add|edit <Host List Name> [parameters]
```

**Parameters**

- name <Host List Name> (edit only)
- retrycount <1-10>
  - Default is 3.
- auth <enable|disable>

**Description**

Configures a prioritized list of hosts to be used for modem dial-in connections.

```
set hostlist add|edit <Host List Name>"entry
```

**Syntax**

```
set hostlist add|edit <Host List Name> entry <Host Number> [parameters]
```

**Parameters**

- host <IP Address or Name>
- protocol <ssh|telnet|tcp>
- port <TCP Port>
- escapeseq <1-10 Chars>

**Description**

Adds a new host entry to a list or edit an existing entry.

```
set hostlist edit <Host List Name> move
```

**Syntax**

```
set hostlist edit <Host List Name> move <Host Number> position <Host Number>
```

**Description**

Moves a host entry to a new position in the host list.
set hostlist delete

Syntax
set hostlist delete <Host List> [entry <Host Number>]

Description
Deletes a host list, or a single host entry from a host list.

show hostlist

Syntax
show hostlist <all|names|Host List Name>

Description
Displays the members of a host list.

IP Filter Commands

set ipfilter state

Syntax
set ipfilter state <enable|disable> [testtimer <disable|1-120 minutes>]

Description
Enables or disables IP filtering for incoming network traffic.

set ipfilter mapping

Syntax
set ipfilter mapping <parameters>

Parameters
ethernet <1|2> state <disable>
ethernet <1|2> state <enable> ruleset <Ruleset Name>
deviceport <1..48> state <disable>
deviceport <1..48> state <enable> ruleset <Ruleset Name>
usbport <u1> state <disable>
usbport <u1> state <enable> ruleset <Ruleset Name>
Description

Maps an IP filter to an interface.

set ip filter rules

Syntax

set ipfilter rules <parameters>

Parameters

add <Ruleset Name>
delete <Ruleset Name>
edit <Ruleset Name> <Edit Parameters>

Edit Parameters:
append
insert <Rule Number>
replace <Rule Number>
delete <Rule Number>

Description

Sets IP filter rules.

Logging Commands

set deviceport port

Syntax

set deviceport port <Device Port List or Name> <one or more deviceport parameters>

Parameters

delay <Email Delay>
email <disable|bytecnt|charstr>
emaillogging <disable>
emailrestart <Restart Delay>
emailsend <email|trap|both>
emailstring <Regex String>
emailsubj <Email Subject>
emailthreshold <Byte Threshold>
emailto <Email Address>
filedir <Logging Directory>
filelogging <enable|disable>
filemaxfiles <Max # of Files>
filemaxsize <Max Size of Files>
locallogging <enable|disable>
name <Device Port Name>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmaxfiles <Max # of Files>
nfsmaxsize <Size in Bytes>
usblogging <enable|disable>
usbmaxfiles <Max # of Files>
usbmaxsize <Size in Bytes>
usbport <u1>
sysloglogging <enable|disable>

**Description**

Configures logging settings for one or more device ports.

Local logging must be enabled for a device port for the locallog commands to be executed. To use the set locallog clear command, the user must have permission to clear port buffers (see Chapter 11: User Authentication).

**Example**

set deviceport port 2-5,6,12,15-16 baud 2400 locallogging enable

**show locallog**

**Syntax**

show locallog <Device Port # or Name> [bytes <Bytes To Display>]

**Description**

Displays a specific number of bytes of data for a device port. 1K is the default.

**set locallog clear**

**Syntax**

set locallog clear <Device Port # or Name>

**Description**

Clears the local log for a device port.

The locallog commands can only be executed for a device port if local logging is enabled for the port. The set locallog clear command can only be executed if the user has permission to clear port buffers (see Chapter 11: User Authentication).
set log clear modem

**Syntax**

set log clear modem

**Description**

Clear the modem log (the modem log is automatically pruned when it reaches 50K).

set log modem ppplog

**Syntax**

set log modem ppplog <enable|disable>

**Description**

Enables PPP activity messages in the modem log.

set log modem pppdebug

**Syntax**

set log modem pppdebug <enable|disable>

**Description**

Enables PPP debugging messages in the modem log:

show log modem

**Syntax**

show log modem [display <head|tail>][numlines <Number of Lines>]

**Description**

View the modem activity log for external modems and USB modems:

show log local

**Syntax**

show log local|nfs|usb <Device Port # or Name> [<parameters>]

**Parameters**

display <head|tail>
numlines <Number of Lines>
bytes <Bytes to Display>
startbyte <Byte Index>
logfile <NFS or USB Log File>

Defaults: bytes=1000, startbyte=1, numlines=40

**Description**

View the log for local, NFS or USB logging (NFS and USB use the current logging settings for the Device Port). Default is to show the tail of the log:

```bash
show log files
```

**Syntax**

```bash
show log files nfs|usb [localdir <NFS Mount Local Directory>]
[usbport <u1>]
[deviceport <Device Port # or name>]
```

**Description**

Lists the NFS or USB log files, either for a specific device port, or all log files in a USB, or NFS location:

**Network Commands**

```bash
set network
```

**Syntax**

```bash
set network <parameters>
```

**Parameters**

- `interval <1-99999 Seconds>`
- `ipforwarding <enable|disable>`
- `probes <Number of Probes>`
- `startprobes <1-99999 Seconds>`

**Description**

Sets TCP Keepalive and IP Forwarding network parameters.

```bash
set network bonding
```

**Syntax**

```bash
set network bonding <disabled|active-backup|802.3ad|load-balancing>
```
**Description**

Configure Ethernet bonding.

**set network dns**

**Syntax**

```
set network dns <1|2|3> ipaddr <IP Address>
```

**Description**

Configures up to three DNS servers.

**set network gateway**

**Syntax**

```
set network gateway <parameters>
```

**Parameters**

- `default <IP Address>`
- `precedence <dhcp|default>`
- `failover <Fail-over Gateway IP Address>`
- `pingip <IP Address of Ping Device>`
- `ethport <1|2>`
- `pingdelay <1-250 seconds>`
- `failedpings <1-250>`
- `faildevice <none|sierra|g52x>`
- `faildevapn <Fail-over Device: APN of Mobile Carrier>`
- `faildevlockpin <enable|disable>`
- `faildevlogin <Fail-over Device: Admin login (Sierra:user, Lantronix G52x:admin)>`
- `faildevcelluser <Fail-over Device: SIM Login>`
- `faildevcelldialstr <Fail-over Device: Dialup Str>`
- `faildevcellroam <enable|disable>`
- `faildevpassthru <enable|disable>`
- `faildevethip <IP Address>`
- `faildevdhcp <enable|disable>`

Transfer firmware update files to the SLB to initiate a firmware update on the fail-over device:

```
set network gateway faildevupdate <ftp|sftp|scp|usb>
gwfile <Firmware File> radiofile <Radio File>
[host <IP Address or Name>] [login <User login>] [path <File Path>]
```

Reboot the fail-over device, or set the fail-over device SIM Card PIN #, SIM Personal Unblocking Key or Admin Password (any extra parameters are ignored):

```
set network gateway reboot
set network gateway faildevpin
```
set network gateway faildevpuk
set network gateway faildevcellpwd
set network gateway faildevpassword
    (Default faildevpassword Sierra:12345, Lantronix G52x:admin)

Description
Set default and fail-over gateway configuration parameters. The fail-over gateway is a backup
default gateway, used when it is determined through a fail-over trigger, that the primary default
gateway is no longer a viable route. A fail-over event happens when a Ping device reachable via
an Ethernet interface and the default gateway, becomes unreachable. Fail-back is when the Ping
device becomes reachable again, causing the primary default route to be restored.

set network host

Syntax
set network host <Hostname> [domain <Domain Name>]

Description
Sets the SLB host name and domain name.

set network port

Syntax
set network port <1|2> <parameters>

Parameters
mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full>
state <dhcp|bootp|static|disable> [ipaddr <IP Address> mask <Mask>]
                    [ipv6addr <IP v6 Address/Prefix>]
mtu <Maximum Transmission Unit>

Description
Configures Ethernet port 1 or 2.
The following list includes options which accept the CLEAR command:

Note: CLEAR must be in all caps.
    set network domain

show network dns

Syntax
show network dns
**Description**
Displays DNS settings.

`show network gateway`

**Syntax**
`show network gateway`

**Description**
Displays gateway settings.

`show network host`

**Syntax**
`show network host`

**Description**
Displays the network host name of the SLB.

`show network port`

**Syntax**
`show network port <1|2>`

**Description**
Displays Ethernet port settings and counters.

`show network all`

**Syntax**
`show network all`

**Description**
Displays all network settings.
NFS and SMB/CIFS Commands

**set nfs mount**

*Syntax*

```
set nfs mount <1|2|3> <one or more parameters>
```

*Parameters*

- `remdir <Remote NFS Directory>`
- `locdir <Directory>`
- `rw <enable|disable>`
- `mount <enable|disable>`

*Note:* `rw <enable|disable>` Enables or disables read/write access to remote directory.

*Defaults:* `rw=enable, mount=enable`

*Description*

Mounts a remote NFS share.

The `remdir` and `locdir` parameters are required, but if they have been specified previously, you do not need to provide them again.

**set nfs unmount**

*Syntax*

```
set nfs unmount <1|2|3>
```

*Description*

Unmounts a remote NFS share.

The following list includes options which accept the CLEAR command:

*Note:* **CLEAR must be in all caps.**

```
set localusers
```

`custommenu, escapeseq, breakseq, dialbacknumber, accessoutlets, listenports, dataports, clearports`

**set cifs**

*Syntax*

```
set cifs <one or more parameters>
```
Parameters

eth1 <enable|disable>
eth2 <enable|disable>
state <enable|disable>
workgroup <Windows workgroup>

Description

Configures the SMB/CIFS share, which contains the system and device port logs. The `admin config` command saves SLB configurations on the SMB/CIFS share.

```
set cifs password
```

Syntax

```
set cifs password
```

Description

Changes the password for the SMB/CIFS share login (default is `cifsuser`). Enables or disables authentication of local users. The following list includes options which accept the CLEAR command:

**Note:** `CLEAR must be in all caps.`

```
set cifs workgroup
```

```
show cifs
```

Syntax

```
show cifs
```

Description

Displays SMB/CIFS settings.

```
show nfs
```

Syntax

```
ujgy"phu
```

Description

Displays NFS share settings.
Performance Monitoring Commands

show perfmon

_Syntax_
show perfmon

_Parameters_
show perfmon [probe <all|Probe Id or Name>]

_Description_
Display global settings and all probes, or a selected probe.

show perfmon status

_Syntax_
show perfmon status

_Parameters_
show perfmon status [probe <Probe Id or Name>]

_Description_
Display the running status of all probes or a selected probe.

show perfmon operations

_Syntax_
show perfmon operations

_Parameters_
show perfmon operations <Probe Id or Name>

_Description_
Display list of completed operation sets for a probe.

set perfmon results

_Syntax_
set perfmon results
**Parameters**

```bash
show perfmon results <Probe Id or Name> [set <Operation Set Number>] [display <head|tail>] [numlines <Number of Lines>] [email <Email Address>]
```

**Description**

Display round trip times (RTT) for last completed operation set or selected set, and optionally email the complete results.

**show perfmon accumulated**

**Syntax**

```bash
show perfmon accumulated
```

**Parameters**

```bash
show perfmon accumulated <Probe Id or Name> [set <Operation Set Number>] [email <Email Address>]
```

**Description**

Display accumulated statistics for last completed operation set or selected set, and optionally email the statistics.

**set perfmon repo**

**Syntax**

```bash
set perfmon repo <local|usb> [usbport U1]
```

**Description**

Set repository where probe operations are stored.

**set perfmon keep**

**Syntax**

```bash
set perfmon keep <Number of Operations to Keep>
```

**Description**

Set number of operations stored for each probe.
set perfmon udpjitterresp

Syntax
set perfmon udpjitterresp <enable|disable>

Description
Enable responders for UDP jitter.

set perfmon udpechoresp

Syntax
set perfmon udpechoresp <UDP Port Number|disable>

Description
Enable responders for UDP echo.

set perfmon tcpconnectresp

Syntax
set perfmon tcpconnectresp <TCP Port Number|disable>

Description
Enable responders for TCP connect.

set perfmon add

Syntax
set perfmon add <Probe Name>
type <dns|http|icmp|tcpconnect|udpecho|udpjitter|udpjittervoip>

Parameters
name <Probe Name>
starttime <now|HH:MM[:SS]|MMDD|afterHH:MM:SS>
operations <Number of Operations to Perform>
frequency <Seconds between Operations>
packets <Number of Packets to Send>
interval <Milliseconds between Packets>
timeout <Milliseconds to Wait for Response>
host <Destination IP Address or Name>
port <Destination Port>
precision <milli|micro>
datasize <Payload Data Size in Bytes>
verifydata <enable|disable>
codec <g729a|g711alaw|g711mulaw>
tos <none|Type of Service>
interface <none|eth1|eth2>
nameserver <IPv4 Address>

**Description**
Add a new probe.

**set perfmon edit**

**Syntax**
set perfmon edit <Probe Id or Name> [parameters]

**Parameters**
name <Probe Name>
starttime <now|HH:MM[:SS][MMDD]|afterHH:MM:SS>
operations <Number of Operations to Perform>
frequency <Seconds between Operations>
packets <Number of Packets to Send>
interval <Milliseconds between Packets>
timeout <Milliseconds to Wait for Response>
host <Destination IP Address or Name>
port <Destination Port>
precision <milli|micro>
datasize <Payload Data Size in Bytes>
verifydata <enable|disable>
codec <g729a|g711alaw|g711mulaw>
tos <none|Type of Service>
interface <none|eth1|eth2>
nameserver <IPv4 Address>

**Description**
Edit an existing probe.

**set perfmon delete**

**Syntax**
set perfmon delete <Probe Id or Name> [data <all|# of Sets to Keep>]

**Description**
Delete a probe, or delete all operation data for a probe, or delete all but the most recent operation sets for a probe.
set perfmon state

**Syntax**

set perfmon state <all|Probe Id or Name> action <restart>

**Description**

Set the running state of all probes or a single a probe.

---

### Power Commands

set power alarmthreshold

**Syntax**

set power alarmthreshold <disable|Tenths of Amps>

**Description**

Number of amps (measured in tenths of an amp) above which the SLB branch office manager sends a trap. The maximum is 180.

*Note:* If the alarm goes off, a warning message displays on the CLI.

set power outlet

**Syntax**

set power outlet <Outlet # or List or Name> <one or more parameters>

**Parameters**

name <Outlet Name>

description <Outlet Description>

state <on|off>

wakeup <on|off|laststate>

reboot

**Description**

Configures and controls power outlets.

**Example**

set power outlet 1-2,4 state on
**set power switchingdelay**

**Syntax**

set power switchingdelay <Delay in msec>

**Description**

Sets the delay after switching on an outlet before switching on the next.

**show power**

**Syntax**

show power <Outlet # or Name>

**Description**

Displays power settings for all outlets or for a single outlet.

**Note:** The screen displays **PND** when the outlet is powering up and is waiting for the delay period to expire. It displays **RBT** when an outlet has been told to reboot and is waiting for the reboot interval to expire (default is 20 seconds.) The switching delay and the reboot interval are completely independent of each other.

**Output Example**

```
[slb2056] > show power
__Current Power Outlet Settings______________________________
Switching Delay: 2000 msec
Over Current Alarm Threshold: 1.0 Amps
Current Level for all Outlets: 0.3 Amps

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Status</th>
<th>Current (amps)</th>
<th>Power State</th>
<th>Wakeup Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PowerOutlet-1</td>
<td>Off</td>
<td>0.0</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>2</td>
<td>PowerOutlet-2</td>
<td>Off</td>
<td>0.0</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>3</td>
<td>PowerOutlet-3</td>
<td>Off</td>
<td>0.0</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>4</td>
<td>PowerOutlet-4</td>
<td>Off</td>
<td>0.0</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>5</td>
<td>PowerOutlet-5</td>
<td>On</td>
<td>0.0</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>6</td>
<td>PowerOutlet-6</td>
<td>On</td>
<td>0.0</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>7</td>
<td>PowerOutlet-7</td>
<td>On</td>
<td>0.0</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>8</td>
<td>PowerOutlet-8</td>
<td>On</td>
<td>0.0</td>
<td>on</td>
<td>off</td>
</tr>
</tbody>
</table>
```
Routing Commands

**set routing**

**Syntax**

```plaintext
set routing [parameters]
```

**Parameters**

- `rip <enable|disable>`
- `route <1-64> ipaddr <IP Address> mask <Netmask> gateway <IP Address>`
- `static <enable|disable>`
- `version <1|2|both>`

**Description**

Configures static or dynamic routing.

To delete a static route, set the IP address, mask, and gateway parameters to `0.0.0.0`.

**show routing**

**Syntax**

```plaintext
show routing [resolveip <enable|disable>] [email <Email Address>]
```

**Description**

Sets the routing table to display IP addresses (disable) or the corresponding host names (enable).

You can optionally email the displayed information.

Script Commands

**set script import**

**Syntax**

```plaintext
set script import <interface|batch|custom> via <ftp|scp|copypaste>
  [file <Script File>] [name <Script Name>] [host <IP Address or Name>]
  [login <User Login>] [path <Path to Script File>]
  [filetype <expect|tcl|python>]
```

**Note:** Interface scripts will be given default/do user rights; Batch and Custom scripts will be given admin/ad user rights. The name of the script will be the same as the file name (if it is a valid script name), otherwise a script name must be specified for import.
**Description**
Import a script.

`set script update`

**Syntax**

```
set script update <interface|batch|custom> name <Script Name>  
    [group <default|power|admin>] [permissions <Permission List>]
```

**Note:** See 'help user permissions' for information on groups and user rights.

**Description**
Update a script.

`set script rename`

**Syntax**

```
set script rename <interface|batch|custom> name <Script Name>  
    newname <New Script Name>
```

**Description**
Rename a script.

`set script delete`

**Syntax**

```
set script delete <interface|batch|custom> name <Script Name>
```

**Description**
Delete a script.

`set script runcli`

**Syntax**

```
set script runcli <Script Name> [parameters <Command Line Parameters>]  
    [debug <enable|disable>]
```

**Description**
Run a CLI batch or custom script one time (script output will be displayed in the current terminal; custom script output will be saved in the repository).
**connect script**

**Syntax**

```bash
connect script <Script Name> deviceport <Device Port # or Name>
  [parameters <Command Line Parameters>] debug
  <enable|disable>]
```

**Description**

Connect an interface or custom script to a Device Port and run it one time (script output will be displayed in the current terminal; custom script output will be saved in the repository).

**set script schedule**

**Syntax**

```bash
set script schedule <Script Name> [device <cli|Device Port # or Name>]
  [state <enable|disable|delete>] [parameters <Cmd Line Parameters>]
  [starttime <now|HH:MM[MMDD]|afterHH:MM>]
  [frequency <Hours/Days between each operation>]
  [stoptime <forever|HH:MM[MMDD]|afterHH:MM>]
```

**Description**

Schedule a custom script to be run at a certain time, either once or recurring; frequency is specified as hours (4H for 4 hours) or days (2D for 2 days).

**show script**

**Syntax**

```bash
show script [type <interface|batch|custom> [name <Script Name>]]
```

**Description**

Display list of scripts, or view the details and contents of a script.

**show script status**

**Syntax**

```bash
show script status [script <Script Name>]
```

**Description**

Display the running status of all custom scripts or a single custom script.
show script operations

Syntax

show script operations <Script Name>

Description

Display list of completed results for a custom script.

show script results

Syntax

show script results <Script Name> [set <all|Operation Set Number>]
[display <head|tail>] [numlines <Number of Lines>]
[email <Email Address>]

Description

Display the results for the last completed custom script operation or a selected operation, and
optionally email the results.

Services Commands

set services

Syntax

ugvx"ugtxkegu">qpg"qt"oqtg"ugtxkegu"rctcogvgtu@

Parameters

netlog <off|error|warning|info|debug>     snmp <enable|disable>
authlog <off|error|warning|info|debug>    traps <enable|disable>
diaglog <off|error|warning|info|debug>   nms1 <IP Address or Name>
servlog <off|error|warning|info|debug>    nms2 <IP Address or Name>
devlog <off|error|warning|info|debug>     location <Physical Location>
genlog <off|error|warning|info|debug>      contact <Admin Contact Info>
syslogserver1 <IP Address or Name>       rocommunity <Read-Only
Community>
syslogserver2 <IP Address or Name>       rwcommunity <Read-Write
Community>
auditlog <enable|disable>                trapcommunity <Trap Community>
auditsize <1-500 Kbytes>                 v3user <V3 RO User>
clicommands <enable|disable>             v3rwuser <V3 RW User>
includesyslog <enable|disable>           v3security
<noauth|auth|authencrypt>
telnet <enable|disable>                   v3auth <md5|sha>
timeouttelnet <disable|1-30 minutes> v3encrypt <des|aes>
webtelnet <enable|disable> alarmdelay <1-6000 Seconds>
escapeseqtelnet <1-10 Chars> v1 <enable|disable>
outgoingtelnet <enable|disable> v2c <enable|disable>
ssh <enable|disable> phonehome <enable|disable>
portssh <TCP Port> phoneip <IP Address>
sha2 <enable|disable> smtpserver <IP Address or Name>
timeoutssh <disable|1-30 minutes> smtpsender <Email Address>
dsakeys <enable|disable> termbufsize <Number of Lines>
webssh <enable|disable>

Set SNMP v3 read-only password/passphrase or read-write password/passphrase:
set services v3password|v3phrase|v3rwpassword|v3rwphrase

Defines the set of SNMP traps that are sent by the SLB:
set services trapenable

**Description**

Configure system and audit logging, SSH and Telnet access to the CLI, the SNMP agent, and the email (SMTP) server.

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

set services location, contact, v3phrase, v3rwphrase, phonenumber

**show services**

**Syntax**

show services

**Description**

Displays current services.

**show services trapenable**

**Syntax**

show services trap enable

**Description**

Defines the set of SNMP traps that are sent by the SLB.
Site Commands

set site

Syntax

Create or edit a site:

set site add|edit <Site Name> [parameters]

Description

Configure a set of site-oriented modem parameters that can be activated by various modem-related events (authentication, outbound network traffic for DOD connections, etc.). The site parameters will override any parameters configured for the modem. To use sites with a modem, enable ‘usesites’. Sites can be used with the following modem states: dialin, dialback, cbcpserver, dialondemand, dialin+ondemand, and dialback+ondemand.

Parameters

allowdialback <enable|disable>
auth <pap|chap>
cbcpnocallback <enable|disable>
deviceport <Device Port # or Name or none>
dialbackdelay <Dial-back Delay>
dialbacknumber <Phone Number>
dialbackretries <1-10>
dialoutlogin <User Login>
dialoutnumber <Phone Number>
localipaddr <negotiate|IP Address>
loginhost <User Login/CHAP Host>
modemtimeout <disable|1-9999 secs>
name <Site Name> (edit only)
nat <enable|disable>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
routegateway <Gateway>
routepaddr <IP Address>
routemask <Mask>
timeoutlogins <disable|1-30 minutes>
usbport <U1>

Set the site password and CHAP secret (any extra parameters will be ignored):

set site dialoutpassword <Site Name>
set site chapsecret <Site Name>

Deletes a site:

set site delete <Site Name>

show site <all|names|Site Name>
Secure Lantronix Network Commands

**set slcnetwork**

**Syntax**

set slcnetwork <one or more parameters>

**Parameters**

add <IP Address>
delete <IP Address>
search <localsubnet|ipaddrlist|both>

**Description**

Detects and displays all SLB branch office manager or user-defined IP addresses on the local network.

**show slcnetwork**

**Syntax**

show slcnetwork [ipaddrlist <all|Address Mask>]

**Description**

Detects and displays all SLBs on the local network.

Without the ipaddrlist parameter, the command searches the SLB network. With the ipaddrlist parameter, the command displays a sorted list of all IP addresses or displays the IP addresses that match the mask (for example, 172.19.255.255 would display all IP addresses that start with 172.19).

**SSH Key Commands**

**set sshkey all export**

**Syntax**

set sshkey allexport <ftp|scp|copypaste> [pubfile <Public Key File>] [host <IP Address or Name>] [login <User Login>] [path <Path to Copy Keys>]

**Description**

Exports the public keys all of the previously created SSH keys.
set sshkey delete

**Syntax**

set sshkey delete <one or more parameters>

**Parameters**

- keyhost <SSH Key Host>
- keyname <SSH Key Name>
- keyuser <SSH Key User>

**Description**

Deletes an ssh key.

Specify the keyuser and keyhost to delete an imported key; specify the keyuser and keyname to delete exported key.

set sshkey export

**Syntax**

set sshkey export <ftp|scp|copypaste> <one or more parameters>

**Parameters**

- [format <openssh|secsh>]
- [host <IP Address or Name>]
- [login <User Login>]
- [path <Path to Copy Key>]
- bits <512|1024|2048>
- keyname <SSH Key Name>
- keyuser <SSH Key User>
- type <rsa|dsa>

**Description**

Exports an sshkey.

set sshkey import

set sshkey import <ftp|scp|copypaste> <one or more parameters>

**Parameters**

- [keyhost <SSH Key IP Address or Name>]
- [keyuser <SSH Key User>]
- [path <Path to Public Key File>]
- file <Public Key File>
- host <IP Address or Name>
- login <User Login>
Description
Imports an SSH key.

**set sshkey server import**

**Syntax**

```
set sshkey server import type <rsa|dsa|ecdsa|ed25519> via <sftp|scp>
   pubfile <Public Key File> privfile <Private Key File>
   host <IP Address or Name> login <User Login> [path <Path to Key File>]
```

*Description*
Imports an SLB host key.

**set sshkey server reset**

**Syntax**

```
set sshkey server reset [type <all|rsa|dsa|ecdsa|ed25519>]
```

*Description*
Resets defaults for all or selected host keys.

**show sshkey export**

**Syntax**

```
show sshkey export <one or more parameters>
```

*Parameters*

- [keyhost <SSH Key IP Address or Name>]
- [keyuser <SSH Key User>]
- [viewkey <enable|disable>]

*Description*
Displays all exported keys or keys for a specific user, IP address, or name.

**show sshkey import**

**Syntax**

```
show sshkey import <one or more parameters>
```
Parameters

[keyhost <SSH Key IP Address or Name>]
[keyuser <SSH Key User>]
[viewkey <enable|disable>]

Description
Displays all keys that have been imported or keys for a specific user, IP address, or name.

show sshkey server

Syntax
show sshkey server [type <all|rsa1|rsa|dsa>]

Description
Displays host keys (public key only).

Status Commands

show connections

Syntax
show connections [email <Email Address>]

Description
Displays a list of current connections. Optionally emails the displayed information. The connection IDs are in the left column of the resulting table. The connection ID associated with a particular connection may change if the connection times out and is restarted.

show connections connid

Syntax
ujiqy"egppgevkqpu"eqppkf">Eqppgevkq"KP@"}gockn">Gockn"Cfftguu@_.

Description
Provides details, for example, endpoint parameters and trigger, for a specific connection. Optionally emails the displayed information.

Note: Use the basic show connections command to obtain the Connection ID.
show portcounters

**Syntax**

```
show portcounters [deviceport <Device Port List or Name>] [email <Email Address>]
```

**Description**

Generates a report for one or more ports. Optionally emails the displayed information.

---

show portstatus

**Syntax**

```
show portstatus [deviceport <Device Port List or Name>] [email <Email Address>]
```

**Description**

Displays device port modes and states for one or more ports. Optionally emails the displayed information.

---

show sysconfig

**Syntax**

```
show sysconfig [display <basic|auth|devices>] [email <Email Address>]
```

**Description**

Displays a snapshot of all configurable parameters. Optionally emails the displayed information.

---

show sysstatus

**Syntax**

```
show sysstatus [email <Email Address>]
```

**Description**

To display the overall status of all SLB devices. Optionally emails the displayed information.
System Log Commands

**show syslog**

*Syntax*

```plaintext
ujguy"u{unqi"}@rctcogvgtu_
```

*Parameters*

- [email <Email Address>]
- level <error|warning|info|debug>
- log <all|netlog|servlog|authlog|devlog|diaglog|genlog>
- display <head|tail> [numlines <Number of Lines>]
- starttime <MMDDYYhhmm[ss]>
- endtime <MMDDYYhhmm[ss]>

*Description*

Displays the system logs containing information and error messages.

*Note:* The level, display, and time parameters cannot be used simultaneously.

**show syslog clear**

*Syntax*

```plaintext
show syslog clear <all|netlog|servlog|authlog|devlog|diaglog|genlog>
```

*Description*

Clears one or all of the system logs.

Temperature Commands

**set temperature**

*Syntax*

```plaintext
set temperature
```

*Description*

Sets the temperature.
show temperature

Syntax

show temperature

Description

Shows the temperature.

USB Access Commands

set usb access

Syntax

set usb access <enable|disable>

Description

Enables or disables access to USB devices.

USB Modem Commands

set usb modem

Syntax

set usb modem <u1|u2> <parameters>

Parameters

accesslist <Access List Name>
auth <pap|chap>
baud <300-115200>
calleridcmd <Modem Command String>
calleridlogging <enable|disable>
cbcpnocallback <enable|disable>
cbctype <admin|user>
chapauth <chaphost|localusers>
chaphost <CHAP Host or User Name>
checkdialtone <disable|5-600 mins>
databits <7|8>
dialbackdelay <PPP Dialback Delay>
dialbacknumber <username|Phone Number>
dialbackretries <1-10>
dialinlist <Host List for Dial-in>
dialoutlogin <Remote User Login>
dialoutnumber <Phone Number>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
flowcontrol <none|xon/xoff|rts/cts>
group <Local or Remote Group Name>
initscript <Modem Init Script>
localipaddr <negotiate|IP Address>
modemmode <text|ppp>
modemtimeout <disable|1-9999 sec>
nat <enable|disable>
parity <none|odd|even>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
service <none|telnet|ssh|tcp>
sshauth <enable|disable>
sshport <TCP Port>
stopbits <1|2>
tcpauth <enable|disable>
tcpport <TCP Port>
telnetauth <enable|disable>
telnetport <TCP Port>
timeoutlogins <disable|1-30 minutes>
usesites <enable|disable>

**Description**

Configures a currently loaded USB modem.

**Description**

Configures a currently loaded USB Modem.

**Note:** *It is recommended that the initscript be prepended with 'AT' and include E1 V1 x4 Q0 so that the SLB may properly control the modem.*

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

```
set usb modem <U1|U2> dialinlist, chaphost, chapsecret, dodchaphost, dodchapsecret, initscript, dialoutlogin, dialoutpassword, dialbacknumber, group
```

Set the modem password and CHAP secrets (any extra parameters will be ignored):

```
set usb modem <U1|U2> dialoutpassword
set usb modem <U1|U2> chapsecret
set usb modem <U1|U2> dodchapsecret
```
show usb modem

Syntax
show usb modem

Description
Display product information and settings for any USB modem:

**USB Serial Commands**

set usb serial

Syntax
set usb serial <U1> <parameters>

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>baud</td>
<td>&lt;300-230400&gt;</td>
</tr>
<tr>
<td>parity</td>
<td>&lt;none</td>
</tr>
<tr>
<td>flowcontrol</td>
<td>&lt;none</td>
</tr>
<tr>
<td>telnetport</td>
<td>&lt;TCP Port&gt;</td>
</tr>
<tr>
<td>sshport</td>
<td>&lt;TCP Port&gt;</td>
</tr>
<tr>
<td>tcpport</td>
<td>&lt;TCP Port&gt;</td>
</tr>
<tr>
<td>databits</td>
<td>&lt;7</td>
</tr>
<tr>
<td>stopbits</td>
<td>&lt;1</td>
</tr>
<tr>
<td>service</td>
<td>&lt;none</td>
</tr>
<tr>
<td>telnetauth</td>
<td>&lt;enable</td>
</tr>
<tr>
<td>sshauth</td>
<td>&lt;enable</td>
</tr>
<tr>
<td>tcpauth</td>
<td>&lt;enable</td>
</tr>
</tbody>
</table>

Description
Configures a serial device connected to a USB port.

show usb serial

Syntax
show usb serial

Description
Display product information and settings for any USB serial device:
USB Storage Commands

set usb storage copy

Syntax
set usb storage copy <U1> file <Filename> newfile <New Filename>

Description
Copies a file on a thumb drive.

set usb storage delete

Syntax
set usb storage delete <U1> file <Current Filename>

Description
Removes a file on a thumb drive.

set usb storage dir

Syntax
set usb storage dir <u1>

Description
Displays a directory listing of a thumb drive

set usb storage format

Syntax
set usb storage format <U1> [filesystem <ext2|fat16|fat32>]

Description
Formats a thumb drive
Defaults: filesystem=ext2
set usb storage fsck <u1>

Syntax
set usb storage fsck <U1>

Description
Runs a filesystem check on a thumb drive (recommended if it does not mount):

set usb storage mount

Syntax
set usb storage mount <u1>

Description
Mounts a thumb drive for use as a storage device. The thumb drive can be used for saving configurations and device logging.

set usb storage unmount

Syntax
set usb storage unmount <u1>

Description
Unmounts a thumb drive. Enter this command before ejecting the card.

set usb storage rename

Syntax
set usb storage rename <U1> file <Filename> newfile <New Filename>

Description
Renames a file on a thumb drive:

show usb storage

Syntax
show usb storage
Description

Display product information and settings for any USB thumb drive:

VPN Commands

```
set vpn
```

**Syntax**

```
set vpn <parameters>
```

**Parameters**

- `tunnel <enable|disable>`
- `name <VPN Tunnel Name>`
- `ethport <defaultroute|1|2>`
- `auth <rsa|psk>`
- `remotefallback <Remote Host IP Address or Name>`
- `remoteid <Authentication Name>`
- `remotethop <IP Address>`
- `remotesubnet <one or more subnets in CIDR notation>`
- `localid <Authentication Name>`
- `localhop <IP Address>`
- `localsubnet <one or more subnets in CIDR notation>`
- `ikenegotiation <main|aggressive>`
- `ikeenc <any|3des|aes>`
- `ikeauth <any|sha1|md5>`
- `ikedhgroup <any|dh2|dh5>`
- `espenc <any|3des|aes>`
- `espauth <any|sha1|md5>`
- `espdhgroup <any|dh2|dh5>`
- `pfs <enable|disable>`
- `modeconfig <enable|disable>`
- `xauthclient <enable|disable>`
- `xauthlogin <User Login>`
- `startvpnfailoveronly <enable|disable>`

Enter RSA public key or Pre-Shared Key of remote host:

- `set vpn key`

Enter XAUTH password:

- `set vpn xauthpassword`

**Description**

Configure an IPsec VPN tunnel.

The following list includes options which accept the CLEAR command:
**Note:**  CLEAR must be in all caps.

```plaintext
set vpn name, remoteid, localid, remotesubnet, localsubnet, xauthlogin
```

**show vpn**

**Syntax**

Display all VPN settings and current status:
```plaintext
show vpn [email <Email Address>]
```
Display detailed VPN status:
```plaintext
show vpn status [email <Email Address>]
```
Display VPN logs:
```plaintext
show vpn viewlog [numlines <Number of Lines] [email <Email Address>]
```
Display RSA public key of the SLB:
```plaintext
show vpn rsakey
```

**Description**

Shows the vpn.
Appendix A: Bootloader

The vSLM management appliance provides a bootloader command interface. This interface is only accessible through the SLB unit’s console port.

Accessing the Bootloader

To access the bootloader command line interface (CLI):

1. Power on the SLB.
2. Type x15 within 10 seconds of power up.

The bootloader halts the boot procedure and displays a Lantronix command prompt.

Bootloader Commands

Table A-1 User Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Lists and prints the command list and online help.</td>
</tr>
<tr>
<td>?</td>
<td>An alias for help.</td>
</tr>
<tr>
<td>Boot</td>
<td>Boot default (runs bootcmd).</td>
</tr>
<tr>
<td>Bootcheck</td>
<td>Checks boot bank information.</td>
</tr>
<tr>
<td>Bootinfo</td>
<td>Displays boot bank information.</td>
</tr>
<tr>
<td>bootsel 1</td>
<td>2</td>
</tr>
<tr>
<td>IDE</td>
<td>Accesses the IDE sub-system.</td>
</tr>
<tr>
<td>Mtest</td>
<td>Performs a simple test of the RAM.</td>
</tr>
<tr>
<td>Ping</td>
<td>Sends a query to determine whether a connection exists.</td>
</tr>
<tr>
<td>Printenv</td>
<td>Displays the values of environment variables.</td>
</tr>
<tr>
<td>setenv</td>
<td>Assigns values to environment variables</td>
</tr>
<tr>
<td>su cust</td>
<td>admin</td>
</tr>
<tr>
<td>Version</td>
<td>Prints the bootloader version.</td>
</tr>
<tr>
<td>whoami</td>
<td>Displays information about the current user.</td>
</tr>
</tbody>
</table>
**Table A-2 Administrator Commands**

In addition to the commands that the user can issue, the administrator can issue the following:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imagecopy</td>
<td>Copies an image of the drive from the lower PCMCIA device to the internal CF card.</td>
</tr>
<tr>
<td>Passwd</td>
<td>Provides a new password for user admin. The default password for user admin is admin. User cust does not have a password.</td>
</tr>
<tr>
<td>Ping</td>
<td>Sends a ping request to the network host.</td>
</tr>
<tr>
<td>Printenv</td>
<td>Prints bootloader variables.</td>
</tr>
<tr>
<td>Setenv</td>
<td>Sets environment variables.</td>
</tr>
</tbody>
</table>
Appendix B: Security Considerations

The SLB branch office manager provides data path security by means of SSH or Web/SSL. Even with the use of SSH/SSL, however, do not assume you have complete security. Securing the data path is only one measure needed to ensure security. This appendix briefly discusses some important security considerations.

Security Practice

Develop and document a Security Practice. The Security Practice should state:

- The dos and don'ts of maintaining security. For example, the power of SSH and SSL is compromised if users leave sessions open or advertise their password.
- The assumptions that users can make about the facility and network infrastructure, for example, how vulnerable the CAT 5 wiring is to tapping.

Factors Affecting Security

External factors affect the security provided by the SLB unit, for example:

- Telnet sends the login exchange as clear text across Ethernet. A person snooping on a subnet may read your password.
- A terminal to the SLB unit may be secure, but the path from the SLB branch office manager to the end device may not be secure.
- With the right tools, a person having physical access to open the SLB unit may be able to read the encryption keys.
- There is no true test for a denial-of-service attack—there is always a legitimate scenario for a request storm. A denial-of-service filter locks out some high-performance automated/scripted requests. The SLB branch office manager will attempt to service all requests and will not filter out potential denial-of-service attacks.
Appendix C: Adapters and Pinouts

The serial device ports of the SLB products match the RJ45 pinouts of the console ports of many popular devices found in a network environment. The SLB branch office manager uses conventional straight-through Category 5 fully pinned network cables for all connections when used with Lantronix adapters. The cables are available in various lengths.

In most cases, you will need an adapter for your serial devices. Lantronix offers a variety of RJ45-to-serial connector adapters for many devices. These adapters convert the RJ45 connection on the SLB unit to a 9-pin or 25-pin serial connector found on other manufacturers' serial devices or re-route the serial signals for connections to other devices that use RJ45 serial connectors.

Please check the cabling database on the Lantronix Web site at www.lantronix.com for suggested cables and adapters for commonly used serial devices.

The console port is wired the same way as the device ports and has the same signal options.

Note: You can view or change the console port settings using the LCDs and keypads on the front panel, the Devices > Console Port page, or the command line interface show console port and set consoleport commands.

The adapters illustrated below are compatible with the Lantronix SLB models.

Figure C-1 RJ45 Receptacle to DB25M DCE Adapter for the SLB (PN 200.2066A)

Use PN 200.2066A adapter with a dumb terminal or with many SUN applications.
Figure C-2  RJ45 Receptacle to DB25F DCE Adapter for the SLB (PN 200.2067A)

Figure C-3  RJ45 Receptacle to DB9M DCE Adapter for the SLB (PN 200.2069A)
Appendix C: Adapters and Pinouts

Figure C-4  RJ45 Receptacle to DB9F DCE Adapter for the SLB (PN 200.2070A)

Use PN 200.2070A adapter with a PC’s serial port.

Figure C-5  RJ45 to RJ45 Adapter for Netra/Sun/Cisco and SLP (PNs 200.2225 and ADP010104-01)

Note: The cable ends of the ADP010104-01 are an RJ45 socket on one end and a RJ45 plug on the other instead of RJ45 sockets on both ends.

Use this adapter for SLP Remote Power Manager, Netra/SUN/CISCO, and others.
Appendix D: Protocol Glossary

**BOOTP (Bootstrap Protocol)**

Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

**CHAP (Challenge Handshake Authentication Protocol)**

A secure protocol for connecting to a system; it is more secure than the PAP.

**DHCP (Dynamic Host Configuration Protocol)**

Internet protocol for automating the configuration of computers that use TCP/IP.

**DNS (Domain Name Servers)**

A system that allows a network nameserver to translate text host names into numeric IP addresses.

**IPsec**

A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

**Kerberos**

A network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

**LDAP (Lightweight Directory Access Protocol)**

A protocol for accessing directory information.

**NAT (Network Address Translation)**

An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

**NFS (Network File System)**

A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user’s access to each file.

**NIS (Network Information System)**

System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

**NMS (Network Management System)**

NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP.
**NTP (Network Time Protocol)**
A protocol used to synchronize time on networked computers and equipment.

**PAP (Password Authentication Protocol)**
A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

**PPP (Point-to-Point Protocol)**
A protocol for creating and running IP and other network protocols over a serial link.

**RADIUS (Remote Authentication Dial-In User Service)**
An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

**SMB/CIFS**
(Server Message Block/Common Internet File System): Microsoft's protocol for allowing all applications as well as Web browsers to share files across the Internet. CIFS runs on TCP/IP and uses the SMB protocol in Microsoft Windows for accessing files. With CIFS, users with different platforms and computers can share files without having to install new software.

**SNMP (Simple Network Management Protocol)**
A protocol that system administrators use to monitor networks and connected devices and to respond to queries from other network hosts.

**SMTP (Simple Mail Transfer Protocol)**
TCP/IP protocol for sending email between servers.

**SSL (Secure Sockets Layer)**
A protocol that provides authentication and encryption services between a web server and a web browser.

**SSH (Secure Shell)**
A secure transport protocol based on public-key cryptography.

**TACACS+ (Terminal Access Controller Access Control System)**
A method of authentication used in UNIX networks. It allows a remote access server to communicate with an authentication server to determine whether the user has access to the network.

**Telnet**
A terminal protocol that provides an easy-to-use method of creating terminal connections to a network host.
Appendix E: Compliance Information

Manufacturer's Name & Address
Lantronix, Inc. 7535 Irvine Center Drive Suite 100 Irvine, CA 92618, USA

Declares that the following product:
Product Name(s): Lantronix® SLB™ Branch Office Manager

Conforms to the following standards or other normative documents:

Regulatory Compliance

Safety: Low Voltage Directive (2014/35/EC) and (2014/35/EU)

EMC: EMC Directive (2014/30/EU)

Emissions
♦ FCC Part 15 Subpart B
♦ Industry Canada ICES-003 Issue 5
♦ VCCI V-3/2013.04
♦ AS/NZS CISPR 22: 2009
♦ EN 55022: 2011

Immunity
♦ EN 55024: 2010
♦ EN 61000-4-2: 2009
♦ EN 61000-4-3: 2006 + A1: 2010
♦ EN 61000-4-4: 2012
♦ EN 61000-4-5: 2006
♦ EN 61000-4-6: 2009
♦ EN 61000-3-2: 2006/A2: 2009
♦ EN 61000-4-8: 2010
♦ EN 61000-3-3: 2008
♦ EN 61000-4-11: 2004

FCC NOTICE (U.S. Only)
This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference 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 manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

INDUSTRY CANADA NOTICE (Canada Only)
This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

RoHS Compliance
This product meets the requirements of 2002/95/EC European RoHS and also complies with the SJ/T 11363-2006 Peoples Republic of China, Requirements for Concentration Limits on Certain Hazardous Substances in Information Technology Products.

Additional Agency Approvals and Certifications
- VCCI
- UL/CUL
- C-Tick
- PSE
- CCC*

Note: *Only applies to 200-240 VAC SLB (specifically P/Ns SLB8824KIT-AP and SLB8824KIT-WW).

RoHS, REACH and WEEE Compliance Statement