



## SLB™ Branch Office Manager User Guide

## Copyright & Trademark

© 2013 Lantronix, Inc. All rights reserved. No part of the contents of this book 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 United States and other countries. *SLB*, *SLC*, *SLM*, *SLP*, *Detector* and *Spider* 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. *Opera* is a trademark of Opera Software ASA Corporation Norway. *Safari* is a registered trademark of Apple, 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). Redistribution or incorporation of BSD or GPL licensed software into hosts other than this product must be done under their terms. A machine readable copy of the corresponding portions of GPL licensed source code is available at the cost of distribution.

Such 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.

A copy of the licenses is available from Lantronix. The GNU General Public License is available at <http://www.gnu.org/licenses/>.

## Contacts

### **Lantronix, Inc. Corporate Headquarters**

167 Technology Drive  
Irvine, CA 92618, USA

Toll Free: 800-526-8766  
Phone: 949-453-3990  
Fax: 949-453-3995

### **Technical Support**

Online: [www.lantronix.com/support/](http://www.lantronix.com/support/)

## Sales Offices

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

---

## Disclaimer & Revisions

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.

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

Date	Rev.	Comments
September 2007	A	Initial Release
May 2008	B	New web page design with tabbed menus. Added support for the following: Sensorsoft devices; SecureID over Radius; command and status of the SLP power manager expansion chassis; escape and break sequences for remote users; password aging, iGoogle Gadget; SNMP v3 encryption; ability to copy boot bank; host lists for outgoing modem and direct connection at the CLI; new option for local users to display a custom menu at login.
October 2013	C	Updated product name and trademark information.

## Warranty

For details on the Lantronix warranty replacement policy, please go to our web site at <http://www.lantronix.com/support/warranty/index.html>.

---

## Table of Contents

Copyright & Trademark	2
Open Source Software	2
Contacts	2
Sales Offices	2
Disclaimer & Revisions	3
Disclaimer & Revisions	3
Warranty	3
<b>1: About This Guide</b>	<b>10</b>
Purpose and Audience	10
Chapter Summaries	10
Additional Documentation	11
<b>2: Overview</b>	<b>12</b>
Features	12
Console Management	12
Power Management Outlets for Power Connectivity	12
Ethernet Switch	12
Integration with Other Secure IT Management Products	12
Meets Needs of Branch Offices	13
Typical Equipment	14
Types of Business	14
Benefits	14
Models	15
System Features	16
Protocols Supported	17
Access Control	17
Power Outlet Control	17
Device Port Buffer	17
Configuration Options	17
Application Example	18
Hardware Features	19
Serial Connections	20
Network Connections	21
PC Card Interface	21
<b>3: Installation</b>	<b>22</b>
What's in the Box	22
Product Information Label	23
Technical Specifications	23
Physical Installation	24
Connecting to a Device Port	25
Connecting to a Network Port	25
Connecting a Terminal	25
Connecting to a Power Source	26

---

Connecting Devices to Power Outlets _____	26
Connecting Devices to the 8-Port Ethernet Switch _____	27
Typical Installations _____	27
<b>4: Quick Setup _____</b>	<b>29</b>
IP Address _____	29
Method #1 Using the Front Panel Display _____	30
Before You Begin _____	30
Front Panel LCD Display and Pushbuttons _____	30
Navigating _____	31
Entering the Settings _____	31
Restoring Factory Defaults _____	33
Method #2 Quick Setup on the Web Page _____	33
Method #3 Quick Setup on the Command Line Interface _____	37
Next Step _____	39
<b>5: Web and Command Line Interfaces _____</b>	<b>40</b>
Web Interface _____	40
Logging in _____	42
Logging off _____	42
Web Page Help _____	42
Command Line Interface _____	43
Logging in _____	43
Logging out _____	43
Command Syntax _____	44
Command Line Help _____	45
Tips _____	45
General CLI Commands _____	46
<b>6: Basic Parameters _____</b>	<b>47</b>
Requirements _____	47
Ethernet Counters _____	51
Network Commands _____	52
IP Filter _____	53
Viewing IP Filters _____	53
Enabling IP Filters _____	54
Configuring IP Filters _____	54
Updating an IP Filter _____	56
Deleting an IP Filter _____	56
Mapping a Rule Set _____	56
IP Filter Commands _____	57
Routing _____	58
Equivalent Routing Commands _____	59
<b>7: Services _____</b>	<b>60</b>
System Logging and Other Services _____	60
SSH/Telnet/Logging _____	60
SNMP _____	64
SNMP, SSH, Telnet, and Logging Commands _____	66

---

NFS and SMB/CIFS _____	69
NFS and SMB/CIFS Commands _____	71
Secure Lantronix Network _____	72
Secure Lantronix Network Commands _____	76
Date and Time _____	76
Date and Time Commands _____	78
<b>8: Device Ports _____</b>	<b>80</b>
Connection Methods _____	80
Permissions _____	81
Device Status _____	81
Global Port Settings _____	81
Global Commands _____	83
Global Commands _____	84
Device Ports – Settings _____	84
Port Status and Counters _____	91
Device Ports – SLP Power Manager _____	91
Device Port – Sensorsoft Device _____	93
Device Port Commands _____	94
Device Commands _____	96
Interacting with a Device Port _____	97
Device Ports – Logging _____	98
Local Logging _____	98
NFS File Logging _____	99
PC Card Logging _____	99
Email/SNMP Notification _____	99
Sylog Logging _____	100
Logging Commands _____	103
Console Port _____	104
Console Port Commands _____	105
Power Outlets _____	106
Power Outlet Commands _____	108
Host Lists _____	108
Host List Commands _____	112
<b>9: PC Cards _____</b>	<b>114</b>
Storage Settings _____	115
Data Settings _____	118
ISDN Settings _____	119
GSM/GPRS Settings _____	119
Text Mode _____	120
PPP Mode _____	120
IP Settings _____	121
PC Card Commands _____	122
PC Card Modem Commands _____	123
<b>10: Connections _____</b>	<b>125</b>
Typical Setup Scenarios for the SLB Device _____	126
Terminal Server _____	126

---

Remote Access Server _____	126
Reverse Terminal Server _____	127
Multipoint Device Server _____	127
Console Server _____	127
Connection Configuration _____	129
Connection Commands _____	131
<b>11: User Authentication _____</b>	<b>134</b>
Authentication Commands _____	136
Local and Remote Users _____	137
Local/Remote User Settings _____	138
Local Users Commands _____	143
Local User Rights Commands _____	144
Remote User Commands _____	144
NIS _____	145
NIS Commands _____	148
LDAP _____	149
LDAP Commands _____	153
RADIUS _____	154
RADIUS Commands _____	157
Kerberos _____	158
Kerberos Commands _____	162
TACACS+ _____	163
TACACS+ Commands _____	166
SSH Keys _____	166
Imported Keys _____	167
Exported Keys _____	167
SSH Commands _____	172
Custom User Menus _____	174
Custom User Menu Commands _____	174
Example _____	176
<b>12: Maintenance and Operation _____</b>	<b>179</b>
SLB Maintenance _____	179
Firmware & Configurations – Web Sessions _____	184
Firmware & Configurations – SSL Certificate _____	184
iGoogle Gadgets _____	186
Administrative Commands _____	187
System Logs _____	190
System Log Command _____	193
Audit Log _____	193
Diagnostics _____	194
Diagnostic Commands _____	198
Status/Reports _____	199
Status Commands _____	202
Events _____	202
Events Commands _____	204

---

<b>13: Application Examples</b>	<b>206</b>
Telnet/SSH to a Remote Device _____	207
Dial-in (Text Mode) to a Remote Device _____	208
Local Serial Connection to Network Device via Telnet _____	210
<b>14: Command Reference</b>	<b>212</b>
Introduction to Commands _____	212
Command Syntax _____	212
Command Line Help _____	213
Tips _____	213
Administrative Commands _____	214
Audit Log Commands _____	220
Authentication Commands _____	220
Kerberos Commands _____	221
LDAP Commands _____	222
Local Users Commands _____	223
NIS Commands _____	226
RADIUS Commands _____	227
TACACS+ Commands _____	228
User Permissions Commands _____	228
CLI Commands _____	231
Connection Commands _____	232
Console Port Commands _____	235
Custom User Menu Commands _____	236
Date and Time Commands _____	237
Device Commands _____	238
Device Port Commands _____	239
Diagnostic Commands _____	242
End Device Commands _____	244
Events Commands _____	245
Host List Commands _____	246
IP Filter Commands _____	247
Logging Commands _____	248
Network Commands _____	249
NFS and SMB/CIFS Commands _____	251
PC Card Storage Commands _____	253
PC Card Modem Commands _____	254
Power Commands _____	255
Routing Commands _____	256
Services Commands _____	257
SLB Network Commands _____	258
SSH Key Commands _____	259
Status Commands _____	261
System Log Commands _____	262
<b>A: Bootloader</b>	<b>264</b>



---

Accessing the Bootloader .....	264
Bootload Commands .....	264
User Commands .....	264
Administrator Commands .....	265
<b>B: Security Considerations .....</b>	<b>266</b>
Security Practice .....	266
Factors Affecting Security .....	266
<b>C: Safety Information .....</b>	<b>267</b>
Safety Precautions .....	267
<b>D: Adapters and Pinouts .....</b>	<b>269</b>
<b>E: Protocol Glossary .....</b>	<b>275</b>
<b>F: Compliance Information .....</b>	<b>278</b>

## List of Figures

Figure 2-1. SLB 8 Front .....	16
Figure 2-2. SLB 8 Back — 8 Device Ports, 4 Power Outlets, 8 Switch Ports; 1 AC Power Supply .....	16
Figure 2-3. Device Port Connections .....	20
Figure 2-4. Console Port Connection .....	20
Figure 2-5. Network Connection .....	21
Figure 2-6. PC Card Interface .....	21
Figure 3-1. CAT 5 Cable Connection .....	25
Figure 3-2. Power Outlets .....	26
Figure 3-3. 8-Port Ethernet Switch .....	27
Figure 3-4. SLB Installation Using the Integrated Ethernet Switch .....	28
Figure 3-5. SLB Installation Using a Managed Switch .....	28
Figure 4-1. Front Panel LCD Display and Five Pushbuttons (Enter, Up, Down, Left, Right) ..	30
Figure 4-2. Beginning of Quick Setup Script .....	37
Figure 4-3. Completed Quick Setup .....	39
Figure 5-1. Web Page Layout .....	41
Figure 13-1. SLB Branch Office Manager Configuration .....	206
Figure 13-2. Remote User Connected to a SUN Server via the SLB Device .....	207

## List of Tables

Table 2-1. SLB Models .....	15
Table 3-1. SLB Technical Specifications .....	23
Table 4-1. Methods of Assigning an IP Address .....	29
Table 4-2. Front Panel Setup Options with Associated Parameters .....	31
Table 5-1. Actions and Category Options .....	44
Table 14-1. Actions and Category Options .....	213

# 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 branch office manager 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.

## Chapter Summaries

The remaining chapters in this guide include:

Chapter	Summary
<a href="#">2: Overview</a>	Describes the SLB models, their main features, and the protocols they support.
<a href="#">3: Installation</a>	Provides technical specifications; describes connection formats and power supplies; provides instructions for installing the SLB branch office manager in a rack.
<a href="#">4: Quick Setup</a>	Provides instructions for getting your SLB device up and running and for configuring required settings.
<a href="#">5: Web and Command Line Interfaces</a>	Describes the web and command line interfaces available for configuring the SLB branch office manager. <b>Note:</b> <i>The configuration chapters (6-12) provide detailed instructions for using the web interface and include equivalent command line interface commands.</i>
<a href="#">6: Basic Parameters</a>	Provides instructions for configuring network ports, firewall and routing settings, and the date and time.
<a href="#">7: Services</a>	Provides instructions for enabling and disabling system logging, SSH and Telnet logins, SNMP, SMTP, and the date and time.
<a href="#">8: Device Ports</a>	Provides instructions for configuring global device port settings, individual device port settings, and console port settings.
<a href="#">9: PC Cards</a>	Provides instructions for using the PC Card slot.
<a href="#">10: Connections</a>	Provides instructions for configuring connections and viewing, updating, or disconnecting a connection.
<a href="#">11: User Authentication</a>	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.

Chapter	Summary
<a href="#">12: Maintenance and Operation</a>	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 device.
<a href="#">13: Application Examples</a>	Shows how to set up and use the SLB branch office manager in three different configurations.
<a href="#">14: Command Reference</a>	Lists and describes all of the commands available on the SLB command line interface
<a href="#">A: Bootloader</a>	Lists and describes the commands available for the bootloader command line interface.
<a href="#">B: Security Considerations</a>	Provides tips for enhancing SLB security.
<a href="#">C: Safety Precautions</a>	Lists safety precautions for using the SLB branch office manager.
<a href="#">D: Adapters and Pinouts</a>	Includes adapter pinout diagrams.
<a href="#">E: Protocol Glossary</a>	Lists the protocols supported by the SLB unit with brief descriptions.
<a href="#">F: Compliance Information</a>	Provides information about the SLB device's compliance with industry standards.

## Additional Documentation

Visit the Lantronix Web site at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation) for the latest documentation and the following additional documentation.

<b>SLB Branch Office Manager Quick Start</b>	Describes the steps for getting the SLB branch office manager up and running.
<b>SLB Online Help for the Command Line Interface</b>	Provides online help for configuring the SLB device using commands.
<b>SLB Online Help for the Web Interface</b>	Provides online help for configuring the SLB branch office manager using the web page.

## 2: Overview

The SLB branch office manager enables IT System Administrators to manage remote servers and IT infrastructure equipment securely over the Internet. This innovative device combines the capabilities of the award-winning Lantronix® SLC™ console manager with remote power management and an Ethernet switch into a compact, 1U rack-mountable appliance.

### Features

#### Console Management

- ◆ 8 serial ports for console connectivity
- ◆ Enables system administrators to remotely manage Linux, Unix, and Windows 2003 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

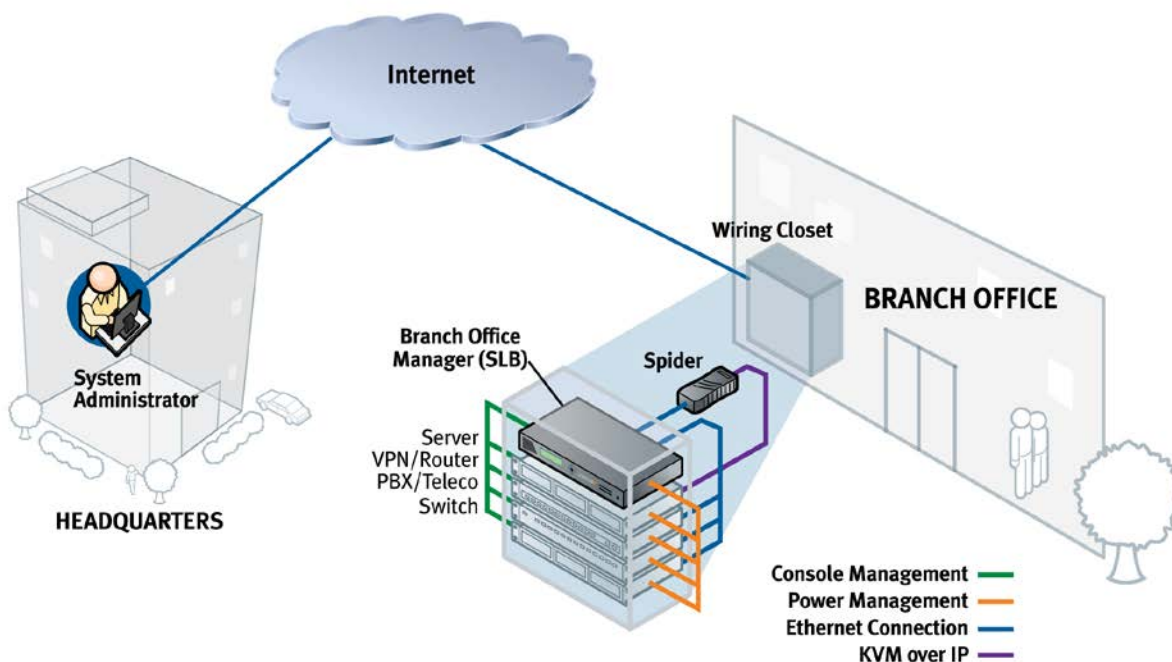
- ◆ 4 outlets for power connectivity
- ◆ Provides ability to control power individually to all attached equipment
- ◆ Provides on/off/reboot control
- ◆ Ensures safe power distribution and reduces in-rush current overload

#### Ethernet Switch

- ◆ 8 ports for network connectivity
- ◆ Provides additional flexibility and scalability
- ◆ Offers convenience
- ◆ Reduces rack space

#### Integration with Other Secure IT Management Products

- ◆ Can be combined with the Lantronix® Spider™ Distributed KVM to provide a complete *all-in-one* “distributed IT” management solution.
- ◆ Can integrate seamlessly with the Lantronix® SLM™ management appliance and brings the “Branch to the Enterprise” for a complete end-to-end OOBI enterprise management solution.



### Meets Needs of Branch Offices

Designed to meet the specific needs of the remote branch office, 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 must be in the same physical location as the equipment. SLB devices give the user a way to access them remotely from anywhere there is a network or modem connection.

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

- ◆ **Servers:** Unix, Linux, Windows 2003, 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 branch office manager is used in many types of business, for example:

- ◆ Banking and finance
- ◆ Insurance companies
- ◆ Healthcare
- ◆ Retail Sales
- ◆ Information Technology
- ◆ Education and campus style facilities
- ◆ Hospitality
- ◆ Manufacturing Facilities

## Benefits

The key benefits of using the SLB branch office manager:

- ◆ **Saves space:** Compact design merges the functionality of three 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 device 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

Two SLB models have the following hardware components:

- ◆ **Two Models:** The SLB branch office manager is available in a 100-120 VAC output model (SLB088411-01) with NEMA 5-15R type outlets and a 208-240 VAC output model (SLB088412-01) with IEC60320/C13 type outlets.
- ◆ **Power Outlets:** Each model has four outlets that 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 [D: Adapters and Pinouts](#) for more information on serial adapters and pin-outs.
- ◆ **Unmanaged Ethernet Switch:** A built-in 8-port unmanaged Ethernet switch provides convenience and helps further reduce required rack space.
- ◆ **Ports and Modem Slots:** The SLB branch office manager has two 10/100 Ethernet ports (referred to in this User Guide as Eth1 and Eth2) and a front panel serial console port (RJ45). The SLB device has two 32-bit CardBus (PC card) slots to support storage cards or a PC Card modem for dial-in access. The list of supported cards is available on the Lantronix website.

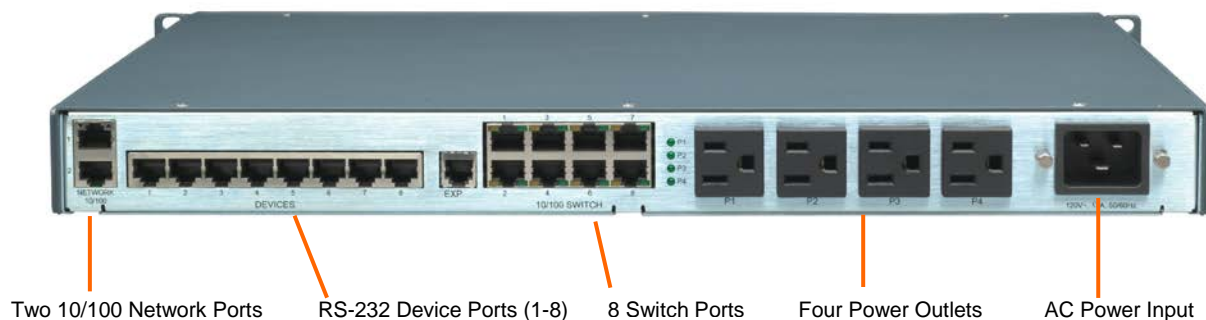
Table 2-1. SLB Models

Part Number	Model and Description
SLB088411-01	SLB branch office manager, 8 device ports, 8 Ethernet switch ports, 4 power outlets (100-120 VAC, NEMA 5-15R type), 1 AC power supply
SLB088412-01	SLB branch office manager, 8 device ports, 8 Ethernet switch ports, 4 power outlets (208-240 VAC, IEC60320/C13 type), 1 AC power supply

Figure 2-1. SLB 8 Front



Figure 2-2. SLB 8 Back — 8 Device Ports, 4 Power Outlets, 8 Switch Ports; 1 AC Power Supply



## 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 four attached devices
- ◆ 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
- ◆ 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
- ◆ Support for an internal PC Card modem or an external modem
- ◆ 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:

- ◆ SSH, Telnet, PPP, NFS, and CIFS for connections in and out of the SLB device
- ◆ SMTP for mail transfer
- ◆ DNS for text-to-IP address name resolution
- ◆ SNMP 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

For brief descriptions of these protocols, see [Appendix 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.

## Power Outlet Control

With the SLB branch office manager'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 device 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.

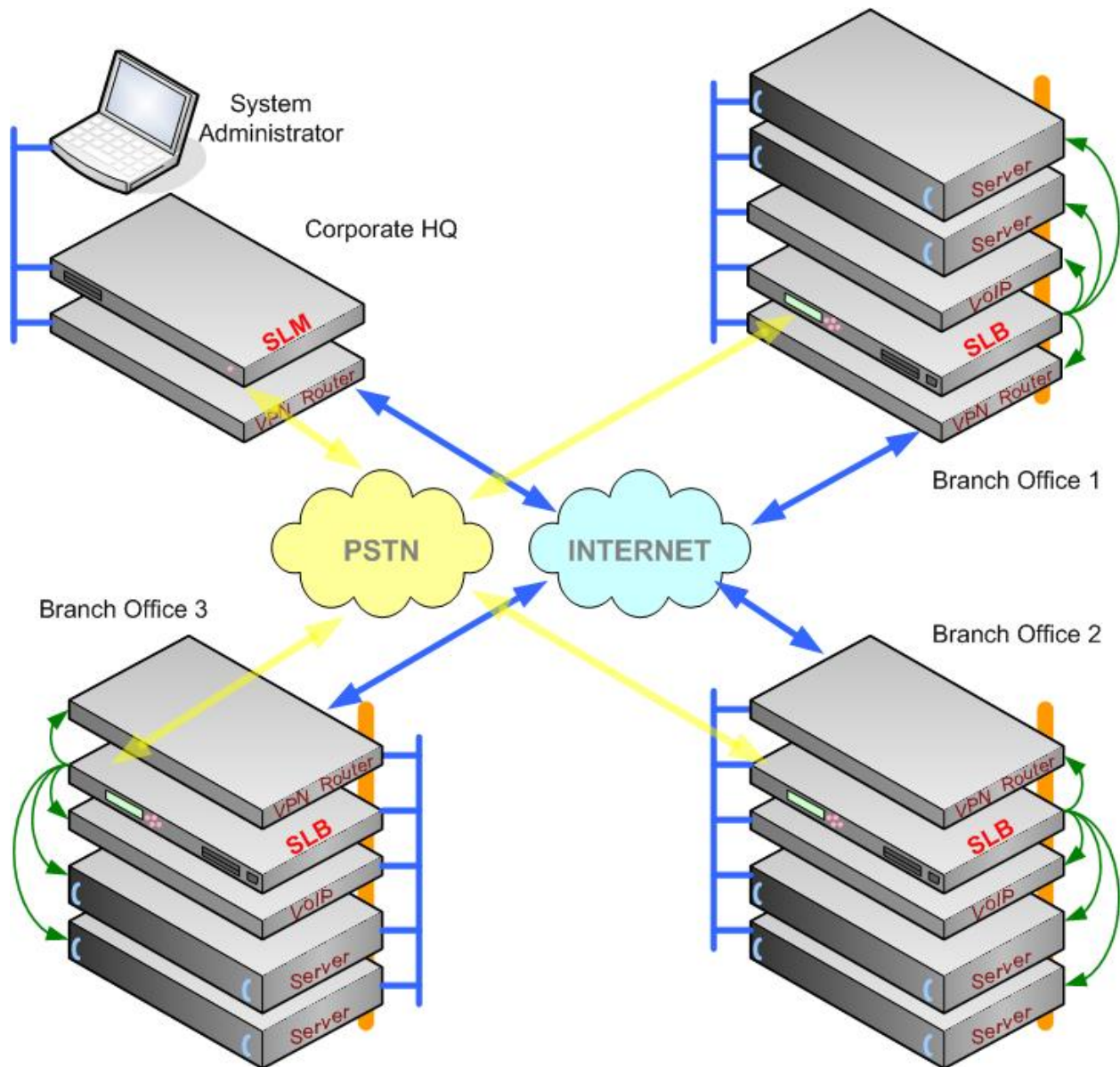
Both a web interface viewed through a standard browser and a command line interface (CLI) are available for configuring the SLB settings and monitoring performance.

## Application Example

The figure below is an example deployment. An SLB branch office manager is deployed in each branch office and an (optional) SLM 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.

**Note:** The SLB branch office manager can also be the authentication gateway to a network architecture that is not VPN-based.

The SLB device provides Ethernet switch service (blue), 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:

- ◆ Views the server's Ethernet interface state information provided by the SLB branch office manager.
- ◆ 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 SLM management appliance) and checks the server's system parameters.
- ◆ If the server is not responsive on the console port, commands the SLB branch office manager to reboot the server's power.
- ◆ If the entire branch office loses IP connectivity, dial in to the SLB device to perform the diagnostic functions

## Hardware Features

The SLB hardware includes the following:

- ◆ 1U-tall (1.75 inch) rack-mountable appliance
- ◆ 2 10Base-T/100Base-TX network ports
- ◆ 1 front panel serial console port for VT100 terminal or PC with emulation
- ◆ 2 PC Card slots
- ◆ Front panel LCD display and keypad
- ◆ 256 KB-per-port buffer memory for serial device ports
- ◆ 8-port unmanaged Ethernet switch with auto MDI/MDIX function
- ◆ 8 RS-232 serial device ports connected via Category 5 (RJ45) wiring
- ◆ AC Power Input:
  - SLB088411-01 model:
    - (1) IEC-60320/C20 inlet, 100-120 VAC, 50/60Hz
    - (20A Branch Circuit) 16A max input current<sup>2</sup>
    - (15A Branch Circuit) 12A max input current<sup>1</sup>
  - SLB088412-01 model:
    - (1) IEC-60320/C20 inlet, 100-240 VAC, 50/60Hz
    - (20A Branch Circuit) 15A max input current
- ◆ Power Outlets (Total Switched Power):
  - SLB088411-01 model:
    - (4) NEMA 5-15R outlets, 100-120 VAC, 50/60Hz
    - (20A Branch Circuit) 15A max per outlet, 16A total<sup>2</sup>
    - (15A Branch Circuit) 12A max per outlet, 12A total<sup>1</sup>
  - SLB088412-01 model:
    - (4) IEC-60320/C13 outlets, 208-240 VAC, 50/60Hz
    - (20A Branch Circuit) 10A max per outlet, 15A total

*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 23](#).

<sup>1</sup> The max input/output current is de-rated to 12A when using the supplied NEMA 5-15P (15A) cable (p/n SLPP012310-01).

<sup>2</sup> The max input/output current is de-rated to 16A when using the optional NEMA 5-20P (20A) cable (p/n SLPP012410-01, SLPP012510-01, SLPP012610-01).

## 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 [D: Adapters and Pinouts](#).)

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

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

Figure 2-3. Device Port Connections



Figure 2-4. Console Port Connection



## 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.

Figure 2-5. Network Connection



## PC Card Interface

The SLB has two PC Card slots. Lantronix qualifies cards continuously and publishes a list of qualified cards on the Lantronix web site.

Figure 2-6. PC Card 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.

**Caution:** To avoid physical and electrical hazards, please be sure to read [C: Safety Information](#) before installing the SLB device.

### What's in the Box

In addition to the SLB branch office manager, the box contains the following items:

Part #	Component Description
<b>Adapters:</b>	
200.2066A	Adapter: DB25M (DCE), Sun w/DB25 female
200.2067A	Adapter: DB25F (DCE) to RJ45, Sun w/DB25 male and some HP9000's
200.2069A	Adapter: DB9M (DCE) to RJ45, SGI Onyx
200.2070A	Adapter: DB9F (DCE) to RJ45, HP9000, SGI Origin, IBM RS6000, and PC-based Linux servers
ADP010104-01	Adapter: RJ45 rolled serial, Cisco, and Sun Netra
<b>Note:</b> An optional adapter for external modems is also available from Lantronix: 200.2073 Adapter: DB25M (DCE) to RJ45, external modems.	
<b>Cables:</b>	
500-184-R	Cable: RJ45 to RJ45, Cat-5, 1 Ft (.3m)
200.0063	Cable: RJ45 to RJ45, Cat-5, 6.6 ft (2 m)
500-153	Cable: RJ45 Loopback
<b>Power Cords:</b>	
SLPP12310-01*	Inlet cord: IEC60320/C19 to NEMA 5-15P (15A), 8 FT.
SLPP12810-01**	Inlet cord: IEC60320/C19 to Schuko (EU), 8 Ft.
SLPP12910-01**	Inlet cord: IEC60320/C19 to BS1363 (UK), 8 Ft.
SLPP12A08-01**	Inlet cord: IEC60320/C19 to AS3112 (AUS/NZ), 8 Ft.
<b>Notes:</b> * Included with SLB088411E-01, ** Included with SLB088412E-01	

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 device:

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

## Technical Specifications

**Table 3-1. SLB Technical Specifications**

<b>Serial Interface (Device)</b>	(8) RJ45-type 8-conductor connector (DTE) Speed software selectable (300 to 115,200 baud)
<b>Serial Interface (Console)</b>	(1) RJ45-type 8-pin connector (DTE) Speed software selectable (300 to 115,200 baud)
<b>Power Input</b>	Model SLB088411-01: <ul style="list-style-type: none"> <li>- (1) IEC-60320/C20 inlet, 100-120 VAC, 50/60Hz</li> <li>- (20A Branch Circuit) 16A max input current <sup>2</sup></li> <li>- (15A Branch Circuit) 12A max input current <sup>1</sup></li> </ul> Model SLB088412-01: <ul style="list-style-type: none"> <li>- (1) IEC-60320/C20 inlet, 100-240 VAC, 50/60Hz</li> <li>- (20A Branch Circuit) 15A max input current</li> </ul>
<b>Power Outlets</b>	Model SLB088411-01: <ul style="list-style-type: none"> <li>- (4) NEMA5-15R outlets, 100-120 VAC, 50/60Hz</li> <li>- (20A Branch Circuit) 15A max per outlet, 16A total<sup>2</sup></li> <li>- (15A Branch Circuit) 12A max per outlet, 12A total<sup>1</sup></li> </ul> Model SLB088412-01: <ul style="list-style-type: none"> <li>- (4) IEC60320/C13 outlets, 208-240 VAC, 50/60Hz</li> <li>- (20A Branch Circuit) 10A max per outlet, 15A total</li> </ul>
<b>Ethernet Switch</b>	(8) Ethernet switch ports (unmanaged) with auto MDI/MDIX
<b>Network Interface</b>	10Base-T/100Base-TX RJ45 Ethernet
<b>Power Supply</b>	(1) Universal AC power input: 100-240 VAC, 50 or 60 Hz IEC-type regional cord set included
<b>Power Consumption</b>	Less than 20 watts
<b>Dimensions</b>	1U, 1.75 in x 17.25 in x 12 in
<b>Weight</b>	10 lb.
<b>Temperature</b>	Operating: 0 to 50 °C (32 to 122 °F) Storage: -20 to 70 °C (-4 to 158 °F)

<b>Relative Humidity</b>	Operating: 10% to 90% non-condensing Storage: 10% to 90% non-condensing
<b>Heat Flow Rate</b>	68 BTU per hour
<b>Current measurement accuracy</b>	± 12%

<sup>1</sup> The max input/output current is de-rated to 12A when using the supplied NEMA 5-15P (15A) cable (p/n SLPP012310-01).

<sup>2</sup> The max input/output current is de-rated to 16A when using the optional NEMA 5-20P (20A) cable (p/n SLPP012410-01, SLPP012510-01, SLPP012610-01).

## Physical Installation

To install the SLB branch office manager in a rack:

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

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

2. Connect the serial device(s) to the SLB device ports. See on page [25](#).
3. Install any PC Cards you intend to use. If you install a modem card, connect to the phone line. See [9: PC Cards](#).
4. You have the following options:
  - a) 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 a Network Port](#) on page [25](#).
  - b) 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 a Terminal](#) on page [25](#).
5. Connect the power cord, and apply power. See [Connecting to a Power Source](#) on page [26](#).
6. Wait approximately a minute and a half for the boot process to complete.

When the boot process ends, the SLB host name and the clock appear on the LCD display.

Now you are ready to configure the network settings as described in [4: Quick Setup](#).



## Connecting to a Device Port

You can connect any device that has a serial console port to a device port on the SLB branch office manager 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.

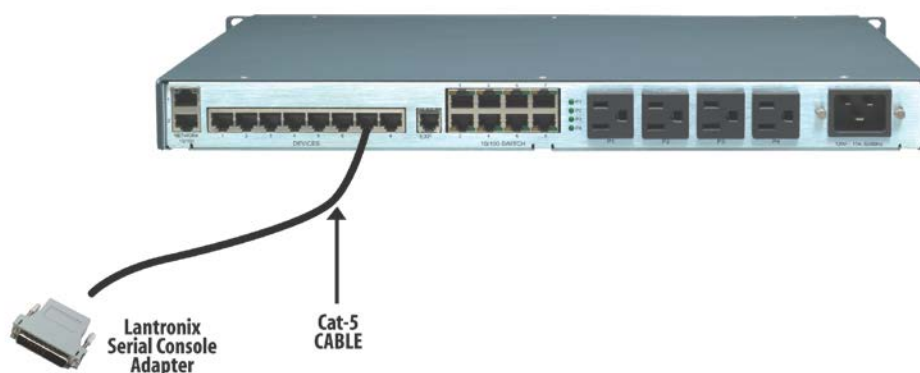
### To connect to a device port:

1. Connect one end of the Cat 5 cable to the device port.
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™ management appliance, use the rolled serial cable provided with the SLB branch office manager, a 200.2225 adapter and Cat 5 cabling, or the ADP010104 adapter that eliminates the need for an additional Cat5 patch cable between the adapter and the connected equipment. See [D: Adapters and Pinouts](#) for more information about Lantronix adapters.

3. Connect the adapter to the serial console of the serial device.

Figure 3-1. CAT 5 Cable Connection



## Connecting to a Network Port

The SLB device'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.

## Connecting a Terminal

The console port is for local access to the SLB branch office manager 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 [D: Adapters and Pinouts](#) and our web site at [www.lantronix.com/support](http://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).
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.

## Connecting to a Power Source

The SLB branch office manager consumes less than 20W of electrical power.

The SLB device has a universal auto-switching AC power supply. The power supply accepts AC input voltage between 100 and 240 VAC with a frequency of 50 or 60 Hz. Rear-mounted IEC-type AC power connector(s) are provided for universal AC power input (see page 22 for included power cords).

Figure 4-2. AC Power Input



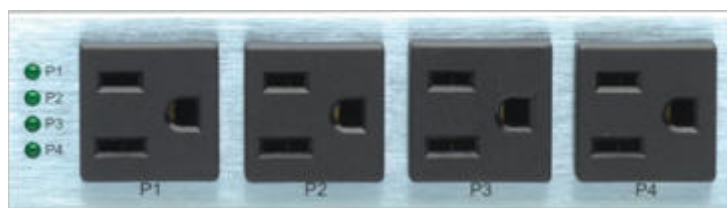
## Connecting Devices to Power Outlets

#### 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 unit and turn the outlets off before connecting the devices.
2. Connect devices to the outlets.

There are four power outlet status LEDs next to outlet number 1. The status LED for outlet 1 is at the top. If the LED for an outlet is dark the outlet is turned off; if it is lit the outlet is turned on.

Figure 3-2. Power Outlets



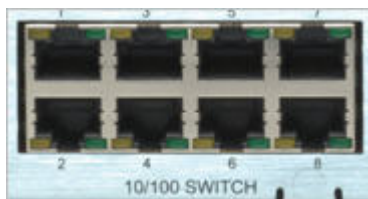
The status of the power outlets displays on the front panel LCD display as the default display.

## Connecting Devices to the 8-Port Ethernet Switch

To connect devices to the unmanaged Ethernet switch:

1. Use the included 1Ft Ethernet patch cable to connect Ethernet port 1 on the SLB branch office manager to one of the switch ports.

Figure 3-3. 8-Port Ethernet Switch



**Note:** The eight unmanaged Ethernet ports are not internally connected to the other two Ethernet ports.

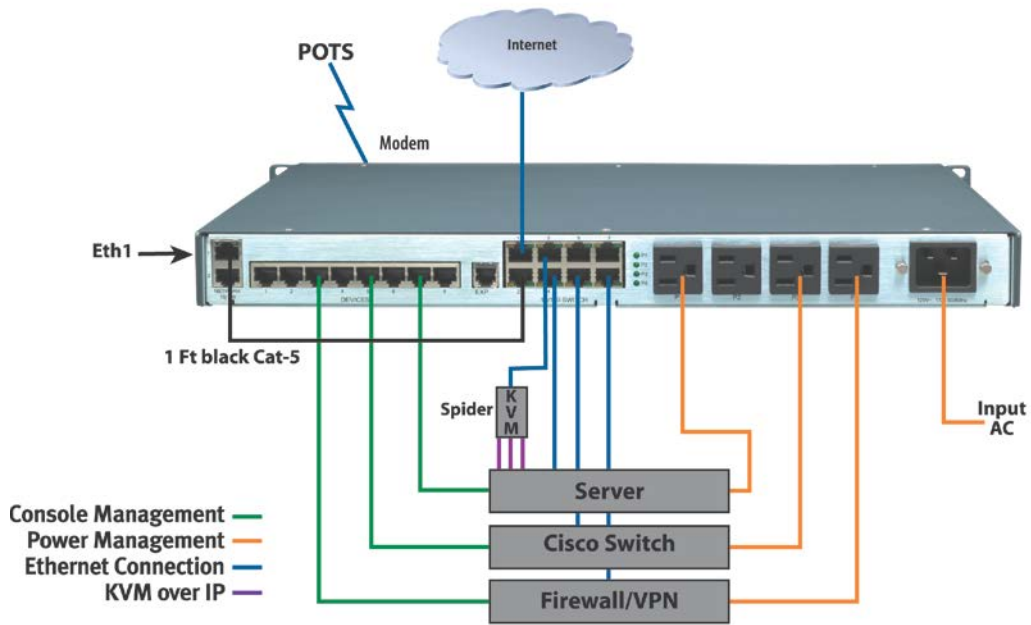
2. Use a standard Ethernet patch cable to connect another switch port to your network.
3. Up to 6 more Ethernet devices may be connected to your network. Use standard Ethernet patch cables from the Ethernet devices to the SLB device's switch ports.

An example of a standard Ethernet patch cable is the Lantronix 200.0062 RJ45 TO RJ45 CAT5 CABLE (LAN PINNING) 6.6 Ft.

## Typical Installations

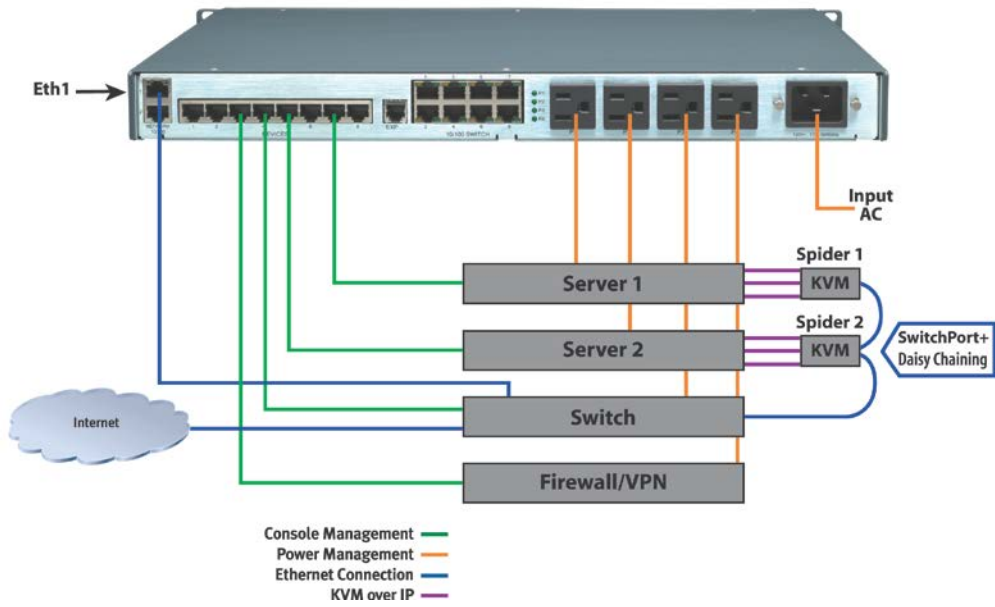
Following are illustrations showing some typical ways to install the SLB branch office manager. In [Figure 3-4](#), three serial devices (a server, a Cisco switch, and a firewall) connect to the SLB device's serial ports, unmanaged switch ports, and power outlets. This setup enables the SLB branch office manager to manage the devices, connect the devices to the network, and provide power to the devices. An SLB switch port connects the Lantronix Spider (optional), a "Distributed KVM" product that provides remote and secure access to the attached server over the network. In addition, the SLB branch office manager connects to a modem for out-of-band dial-up access.

Figure 3-4. SLB Installation Using the Integrated Ethernet Switch



In [Figure 3-5](#), the SLB branch office manager controls four serial devices and provides power to them. The devices use a managed switch to connect to the network. The figure also shows how Lantronix Spiders can be daisy chained.

Figure 3-5. SLB Installation Using a Managed Switch



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

- ◆ Use the front panel LCD display and pushbuttons.
- ◆ Complete the Quick Setup web page 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 Lantronix® Detector™ (downloadable at <http://www.lantronix.com/support/downloads/>). If Eth1 cannot acquire an IP address, you cannot use Telnet, SSH, or the web interface to run Quick Setup.

### IP Address

Your SLB branch office manager 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, and in the same subnet as your PC.

You have the following options for assigning an IP address to your SLB device.

**Table 4-1. Methods of Assigning an IP Address**

Method	Description
DHCP	<p>A DHCP server automatically assigns the IP address and network settings. The SLB branch office manager is DHCP-enabled by default.</p> <p>With the Eth1 network port connected to the network, and the SLB device powered up, Eth1 acquires an IP address, viewable on the LCD.</p> <p>At this point, you can Telnet into the SLB branch office manager, or use the web interface.</p>
BOOTP	Similar to DHCP but for smaller networks.
Detector	<p>A Windows-based application downloadable at <a href="http://www.lantronix.com/support/downloads/">http://www.lantronix.com/support/downloads/</a> for viewing a DHCP-provided IP address or for assigning a static IP address to the SLB branch office manager. You can use Detector only if you have not already assigned a static IP address by another method. For more information, see Detector's online help.</p>

Method	Description
<b>Front panel LCD display and pushbuttons</b>	You manually assign the IP address and other basic network, console, and date/time settings. If desired, you can restore the factory defaults.
<b>Serial port login to command line interface</b>	You assign an IP address and configure the SLB branch office manager using a terminal or a PC running a terminal emulation program to the SLB device's serial console port connection.

## Method #1 Using the Front Panel Display

### Before You Begin

Make sure you know:

- ◆ An IP address that will be unique and 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 in to power and turned on.

### Front Panel LCD Display and Pushbuttons

With the SLB device powered up, you can use the front panel display and pushbuttons to set up the basic parameters.

**Figure 4-1.** Front Panel LCD Display and Five Pushbuttons (Enter, Up, Down, Left, Right)



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

When you click the **right-arrow** pushbutton, the SLB device's network settings display. Using the five pushbuttons, 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 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 a numerical entry of the selected option. Use the **Enter** button to select an option to change or to save your settings.

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

Table 4-2. Front Panel Setup Options with Associated Parameters

Normal	Network Settings	Console Settings	Date / Time Settings	Release
	Eth1 IP Address	Baud Rate Data Bits Stop Bits Parity Flow Control	Time Zone	Firmware version and date code (display only)
	Eth1 Subnet Mask		Date/Time	
	Gateway			Restore Factory Defaults
	DNS1			
	DNS2			
	DNS3			

## Entering the Settings

To enter setup information:

1. From the normal display (host name, date and time), 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 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.
  - a) 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.
  - b) 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 Telnet or 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 last option, **Release**.
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 `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 reboots.

## Method #2 Quick Setup on the Web Page

After the unit has an IP address, you can use the Quick Setup web page to configure the remaining network settings. This page displays the first time you log into the SLB only. Otherwise, the SLB Home Page displays. (For information about the web interface, see [Web Interface](#) on page 40.)

To complete the Quick Setup page:

1. Open a standard web browser. Lantronix supports the latest versions of Internet Explorer, Mozilla Firefox, Safari, Opera or Chrome web browsers.
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 **PASS** as the password. The first time you log in to the SLB, the Quick Setup page automatically displays. Otherwise, the Home page displays.

**Note:** To open the Quick Setup page at another time, click the **Quick Setup** tab.

**LANTRONIX® SLB884**

Logout User: sysadmin Select port for  configuration or  WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance **Quick Setup**

Quick Setup [Help ?](#)

**Quick Setup**

**Welcome to the SecureLinux Branch Office Manager**

Below are basic settings that it is recommended you configure before using the SecureLinux Branch Office Manager. If these settings are OK, click the checkbox below and select the Apply button.

Accept default Quick Setup settings

**Network Settings**

The SLB has two Ethernet ports, Eth1 and Eth2. By default, both Eth1 and Eth2 are configured for DHCP.

Eth1 Settings:  Obtain from DHCP  Obtain from BOOTP  Specify:

IP Address:  Subnet Mask:

Default Gateway:  Hostname:  Domain:

Note: The hostname will be used as the prompt in the Command Line Interface.

**Date & Time Settings**

Change Date/Time:

Date:

Time:  :

Time Zone:

**Administrator Settings**

The **sysadmin** user has complete privileges for SLB administration. The default password is 'PASS'.

Sysadmin Password:

Retype Password:

- 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.

- Enter the following:

### Network Settings

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

<b>Eth 1 Settings</b>	<p><b>Disabled:</b> If selected, disables the network port. Default is Eth1 enabled.</p> <p><b>Obtain from DHCP:</b> 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 <b>Gateway</b>.</p> <p><b>Obtain from BOOTP:</b> Lets a network node request configuration information from a BOOTP "server" node. If you select this option, skip to <b>Gateway</b>.</p> <p><b>Specify:</b> Lets you manually assign a static IP address, generally provided by the system administrator.</p>
<b>IP Address</b> (if specifying)	<p>Enter an IP address that will be unique and valid on your network. There is no default.</p> <p>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.</p> <p><i>Note:</i> Currently, the SLB branch office manager does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).</p>
<b>Subnet Mask</b>	If specifying an IP address, enter the network segment on which the SLB device resides. There is no default.
<b>Default Gateway</b>	The IP address of the router for this network. There is no default.
<b>Hostname</b>	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.
<b>Domain</b>	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLB branch office manager. For example, if <b>abcd</b> is specified for the SMTP server, and <b>mydomain.com</b> is specified for the domain, if <b>abcd</b> cannot be resolved, the SLB device attempts to resolve <b>abcd.mydomain.com</b> for the SMTP server.

### Date & Time Settings

<b>Change Date/Time</b>	Select the checkbox to manually enter the date and time at the SLB branch office manager's location.
<b>Date</b>	From the drop-down lists, select the current month, day, and year.
<b>Time</b>	From the drop-down lists, select the current hour and minute.
<b>Time Zone</b>	From the drop-down list, select the appropriate time zone.

## Administrator Settings

<b>Sysadmin Password/ Retype Password</b>	To change the password (e.g., from the default) enter a password of up to 64 characters.
---	--

6. To save your entries, click the **Apply** button.

## 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 a Terminal](#) on page 25.) If the unit has an IP address, you can use SSH or Telnet to connect to the SLB device.

**Note:** By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the Services web page (see [7: Services](#)), 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 **PASS** as the password and press **Enter**. The first time you log in, the Quick Setup script runs automatically. Normally, the command prompt displays.

**Figure 4-2. 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**.

<b>Configure Eth1</b>	<p>Select one of the following:</p> <p><b>&lt;1&gt; obtain IP Address from DHCP:</b> 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.</p> <p><b>&lt;2&gt; obtain IP Address from BOOTP:</b> Permits a network node to request configuration information from a BOOTP "server" node.</p> <p><b>&lt;3&gt; static IP Address:</b> Allows you to assign a static IP address manually. The IP address is generally provided by the system administrator.</p>
-----------------------	---

<b>IP Address (if specifying)</b>	<p>An IP address that will be unique and valid on your network and in the same subnet as your PC. There is no default.</p> <p>If you selected <b>DHCP</b> or <b>BOOTP</b>, this prompt does not display.</p> <p>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.</p> <p><b>Note:</b> Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.</p>
<b>Subnet Mask</b>	<p>The subnet mask specifies the network segment on which the branch office manager resides. There is no default. If you selected <b>DHCP</b> or <b>BOOTP</b>, this prompt does not display.</p>
<b>Default Gateway</b>	<p>IP address of the router for this network. There is no default.</p>
<b>Hostname</b>	<p>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).</p> <p><b>Note:</b> The host name becomes the prompt in the command line interface.</p>
<b>Domain</b>	<p>If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLB branch office manager. For example, if <b>abcd</b> is specified for the SMTP server, and <b>mydomain.com</b> is specified for the domain, if <b>abcd</b> cannot be resolved, the SLB device attempts to resolve <b>abcd.mydomain.com</b> for the SMTP server.</p>
<b>Time Zone</b>	<p>If the time zone displayed is incorrect, enter the correct time zone and press <b>Enter</b>. 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.</p>
<b>Date/Time</b>	<p>If the date and time displayed are correct, type <b>n</b> and continue. If the date and time are incorrect, type <b>y</b> and enter the correct date and time in the formats shown at the prompts.</p>
<b>Sysadmin password</b>	<p>Enter a new sysadmin password.</p>

After you complete the Quick Setup script, the changes take effect immediately.

Figure 4-3. Completed Quick Setup

```

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 SLB0884 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 (172.19.219.178)
Enter 1-3: [3]
Enter IP Address: [172.19.219.178]
Enter Subnet Mask: [255.255.0.0]

The SLB0884 can be configured to use a default gateway.  

Enter gateway IP Address: [172.19.0.1]

_____  

Hostname
_____  

The current hostname is 'SLB', and the current domain is 'lantronix.com'.  

The hostname will be shown in the CLI prompt.  

Specify a hostname: [SLB]
Specify a domain: [lantronix.com]

_____  

Time Zone
_____  

The current time zone is 'America/Los_Angeles'.  

Enter time zone: [America/Los_Angeles]

_____  

Date/Time
_____  

The current time is Wed Jun 20 10:51:34 2007  

Change the current time? [n]

_____  

Sysadmin Password
_____  

Enter new password: [<current password>]

Reconfiguring the SLB0884...
Ethernet settings successfully updated.

Quick Setup is now complete.

```

5. To logout, type **logout** at the prompt and press **Enter**.

## Next Step

After quick starting the SLB branch office manager, 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 [5: Web and Command Line Interfaces](#).
- ◆ To continue configuring the SLB device, go to [6: Basic Parameters](#).

## 5: Web and Command Line Interfaces

The SLB branch office manager offers three interfaces for configuring the SLB device: a command line interface (CLI), a web interface, and an LCD with pushbuttons on the front panel. This chapter discusses the web and command line interfaces. ([4: Quick Setup](#) 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 branch office manager using most web browsers (Netscape Navigator 6.x and later or Internet Explorer 5.5. and later, with JavaScript enabled). The Web Telnet and Web SSH features require Java 1.1 (or later) support in the browser. The SLB device 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

The screenshot shows the LANTRONIX SLB884 web interface. At the top right, there is a 'Port Number Bar' with buttons for E1, E2, ports 1-8, S1-S8, P1-P4, and A, B. Below this is a 'Logout Button' and a 'User: sysadmin' indicator. A row of 'Tabs' includes Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. Below the tabs are 'Options' for Device Status, Device Ports, Console Port, PC Card, Power Outlets, Connections, and Host Lists. The main content area is titled 'Device Ports - Logging' and shows configuration for 'Port: 3'. It includes sections for Local Logging, Email/Traps, NFS File Logging, PC Card Logging, and Syslog Logging. Each section has various checkboxes, radio buttons, and input fields. At the bottom, there is an 'Apply Button' and a 'Back to Device Port Settings' link. On the right side, there is a 'Help Button'.

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, Switch, and Power Outlet Bar:**

- ◆ The **E1** and **E2** buttons display the Network – Settings page.
- ◆ The left-most 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 two options for use with the port buttons. Selecting a port and the **Configuration** option takes you to the Device Port 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.

- ◆ **S** (switch) buttons refer to the unmanaged Ethernet switch ports on the back of the unit. The firmware does not currently configure or control them.
- ◆ Buttons **P1 - P4** enable you to select a power outlet and display the Power Outlets page with the selected outlet's information highlighted.
- ◆ The **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 6 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 (in order, from left to right) :

- ◆ Home page.
- ◆ Information about the SLB device and Lantronix contact information.
- ◆ Configuration site map.
- ◆ Status of the SLB branch office manager.

**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 (Netscape Navigator 6.x and later or Internet Explorer 5.5 and later).
2. In the URL field, type **https://** followed by the IP address of your SLB branch office manager.
3. To configure the SLB device, use **sysadmin** as the user name and **PASS** as the password. (These are the default values.)

**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 off

### To log off the SLB web interface:

From the main menu, select **Logoff**. The “SLB logoff complete” message displays.

## Web Page Help

### To view detailed information about an SLB web page:

Click the **Help** button to the right of the web page title.

## Command Line Interface

A command line interface (CLI) is available for entering all the commands you can use with the SLB branch office manager. 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 web page, a serial terminal connection, or an SSH connection. (See 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:
  - a) Enter **sysadmin** as the user name and press **Enter**.
  - b) Enter **PASS** 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.
3. To log in as any other user:
  - a) Enter your SLB branch office manager user name and press **Enter**.
  - b) Enter your SLB branch office manager password and press **Enter**.

## Logging out

### To log out of the SLB command line interface:

1. Type **logout** and press **Enter**.

## Command Syntax

Commands have the following format:

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

where

<action> is set, show, connect, admin, diag, pccard, 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 5-1. Actions and Category Options**

Action	Category
set	network   ipfilter   routing   datetime   ntp   services   nfs   cifs   menu   hostlist   auth   localusers   remoteusers   ldap   radius   kerberos   tacacs+   consoleport   deviceport   nis   slcnetwork   command   sshkey   password   history   cli   locallog   power
show	network   ipfilter   routing   datetime   ntp   services   nfs   cifs   menu   hostlist   auth   localusers   nis   ldap   radius   kerberos   tacacs+   consoleport   deviceport   locallog   sysstatus   syslog   auditlog   portstatus   sysconfig   portcounters   connections   slcnetwork   sshkey   history   cli   user   remoteusers   power
connect	direct   listen   bidirection   unidirection   terminate
diag	ping   loopback   traceroute   arp   lookup   netstat   perfstat   sendpacket   nettrace   internals
pccard	storage   modem
admin	reboot   shutdown   ftp   config   firmware   version   banner   keypad   quicksetup   web   events   lcd
logout	Terminates CLI session.

## 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.

SCS Commands	SLB Commands
info	'show sysstatus'
version	'admin version'
reboot	'admin reboot'
poweroff	'admin shutdown'
listdev	'show deviceport names'
direct	'connect direct deviceport'
listen	'connect listen deviceport'
clear	'set locallog clear'
telnet	'connect direct telnet'
ssh	'connect direct ssh'

### 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 [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 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. The following page displays:

**LANTRONIX® SLB884**

Logout User: sysadmin Select port for configuration or WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance Quick Setup

Network Settings IP Filter Routing

### Network Settings

**Ethernet Interfaces**

Eth1 Settings:  Disabled  Obtain from DHCP  Obtain from BOOTP  Specify:

Eth2 Settings:  Disabled  Obtain from DHCP  Obtain from BOOTP  Specify:

IP Address: 172.18.21.64 IP Address:

Subnet Mask: 255.255.0.0 Subnet Mask:

IP v6 Address: fe80::280:a3ff:fe89:423d/ IP v6 Address: fe80::280:a3ff:fe89:423e/

Eth1 Mode: Auto Eth2 Mode: Auto

Eth1 Multicast: 239.255.255.251 224.0.0.1 Eth2 Multicast: 224.0.0.1

	Rx				Tx		
	Bytes	Packets	Errors	Multicast	Bytes	Packets	Errors
Eth1	192405028	2471651	2400	2458892	6194210	28798	0
Eth2	0	0	0	0	1440	12	12

**Gateway** The alternate gateway is used if an IP address usually accessible through the default gateway fails to return one or more pings.

Default: 172.18.0.1 Alternate:

DHCP-Acquired: None IP Address to Ping:

GPRS-Acquired: None Ethernet Port for Ping:  Eth1  Eth2

Precedence:  DHCP-Acquired  Default  GPRS-Acquired Delay between Pings: 3 seconds

Number of Failed Pings: 10

Enable IP Forwarding:

**TCP Keepalive Parameters**

Start Probes: 600 secs

Number of Probes: 5

Interval: 60 secs

Apply

**Hostname & Name Servers**

Hostname: tsslb8

Note: The hostname will be used as the prompt in the Command Line Interface.

Domain: support.int.lantronix

**DNS Servers**

#1: 172.18.0.11

#2: 172.16.1.4

#3: 4.2.2.1

**DHCP-Acquired DNS Servers**

#1: None

#2: None

#3: None

**GPRS-Acquired DNS Servers**

#1: None

#2: None

#3: None

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.



<b>Eth 1 and/or Eth 2 Settings</b>	<p><b>Disabled:</b> If selected, disables the network port. Defaults are Eth1 and Eth2 enabled.</p> <p><b>Obtain from DHCP:</b> 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 <b>Gateway</b>.</p> <p><b>Obtain from BOOTP:</b> Lets a network node request configuration information from a BOOTP "server" node. If you select this option, skip to <b>Gateway</b>.</p> <p><b>Specify:</b> Lets you manually assign a static IP address, generally provided by the system administrator.</p>
<b>IP Address</b> (if specifying)	<p>Enter an IP address that will be unique and valid on your network. There is no default.</p> <p>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.</p> <p><i>Note:</i> Currently, the SLB branch office manager does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).</p>
<b>Subnet Mask</b>	<p>If specifying an IP address, enter the network segment on which the SLB device resides. There is no default.</p>
<b>Eth 1 and/or Eth2 IPv6 Address</b>	<p>Address of the port in IPv6 format.</p> <p><i>Note:</i> The SLB branch office manager supports IPv6 connections for a limited set of services: the web, SSH, and Telnet.</p> <p>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, 1234:0BCD:1D67:0000:0000:8375:BADD:0057 may be shortened to 1234:BCD:1D67::8375:BADD:57.</p>
<b>Eth 1 and/or Eth2 Mode</b>	<p>Select the direction (full duplex or half-duplex) and speed (10 or 100Mbit) of data transmission. The default is <b>Auto</b>, which allows the Ethernet port to auto-negotiate the speed and duplex with the hardware endpoint to which it is connected.</p>
<b>Eth 1 and/or Eth2 Multicast</b>	<p>Displays the multicast address of the Ethernet port.</p>

## Gateway

<b>Default</b>	<p>IP address of the router for this network.</p> <p>If this has not been set manually, any gateway acquired by DHCP for Eth1 or Eth2 displays.</p> <p>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 Eth 2.</p> <p>If you set a default gateway, any network traffic that does not match Eth1 or Eth2 is sent to the default gateway for routing.</p>
<b>DHCP-Acquired</b> (view only)	Gateway acquired by DHCP for Eth1 or Eth2.
<b>GPRS-Acquired</b> (view only)	Displays the IP address of the router if it has been automatically assigned by General Packet Radio Service (GPRS).
<b>Precedence</b>	Indicates whether the gateway acquired by DHCP 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 branch office manager gives precedence to the Eth1 gateway.
<b>Alternate</b>	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.
<b>IP Address to Ping</b>	IP address to ping to determine whether to use the alternate gateway.
<b>Ethernet Port to Ping</b>	Ethernet port to use for the ping.
<b>Delay between Pings</b>	Number of seconds between pings
<b>Number of Failed Pings</b>	Number of pings that fail before the SLB device uses the alternate gateway.
<b>Enable IP Forwarding</b>	<p>IP forwarding enables network traffic received on one interface (Eth1, Eth2, or an external/PC Card 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.</p> <p>Enabling IP forwarding is required if you enable Network Address Translation (NAT) for any device port modem or PC Card/ISDN modem. IP forwarding allows a user accessing the SLB branch office manager over a modem to access the network connected to Eth1 or Eth2.</p>

## Hostname & Name Servers

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

### DNS Servers

<b>DNS Servers #1 - #3</b>	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

<b>#1 - #3</b>	Displays the IP address of the name servers if automatically assigned by DHCP.
----------------	--

### GPRS-Acquired DNS Servers

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

### TCP Keepalive Parameters

<b>Start Probes</b>	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 <b>600</b> seconds (10 minutes).
<b>Number of Probes</b>	Number of probes the SLB device sends before closing a session. The default is <b>5</b> .
<b>Interval</b>	The number of seconds the SLB branch office manager waits between probes. The default is <b>60</b> seconds.

- 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-Settings page displays statistics for each of the SLB 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

The following CLI commands correspond to the web page entries described above.

---

### To configure Ethernet port 1 or 2:

```
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>]
```

---

### To configure up to three DNS servers:

```
set network dns <1|2|3> ipaddr <IP Address>
```

---

### To set the default and alternate network gateways:

```
set network gateway <parameters>
```

*Parameters:*

```
default <IP Address>  
precedence <dhcp|gprs|default>  
alternate <IP Address>  
pingip <IP Address>  
ethport <1 or 2>  
pingdelay <1-250 seconds>  
failedpings <1-25>
```

The alternate gateway is used if an IP address usually accessible through the default gateway fails to return one or more pings.

---

### To set the SLB host name and domain name:

```
set network host <Hostname> [domain <Domain Name>]
```

---

### To set TCP Keepalive and IP Forwarding network parameters:

```
set network <parameters>
```

*Parameters:*

```
interval <1-99999 Seconds>  
ipforwarding <enable|disable>  
probes <Number of Probes>  
startprobes <1-99999 Seconds>
```

---

**To view all network settings:**

```
show network all
```

---

**To view Ethernet port settings and counters:**

```
show network port <1|2>
```

---

**To view DNS settings:**

```
show network dns
```

---

**To view gateway settings:**

```
show network gateway
```

---

**To view the host name of the SLB device:**

```
show network host
```

---

## 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.

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 branch office manager.*

### 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 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:

<b>Enable IP Filter</b>	Select the <b>Enable IP Filter</b> checkbox to enable all filters, or clear the checkbox to disable all filters. Disabled by default.
<b>Packets Dropped</b> (view only)	Displays the number of data packets that the filter ignored (did not respond to).
<b>Packets Rejected</b> (view only)	Displays the number of data packets that the filter sent a “rejected” response to.
<b>Test Timer</b>	Timer for testing IP Filter rulesets. Select <b>No</b> to disable the timer. <b>Select Yes, minutes (1-120)</b> 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.
<b>Time Remaining</b> (view only)	Indicates how many minutes are left on the timer before it expires and IP Filters are disabled.

## 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 Rule Set](#) on page 56.

**To add an IP filter:**

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

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a status bar with various indicators (E1, E2, 1-8, S, P1-P4, A, B) and a 'Logout' button for user 'sysadmin'. The main navigation menu includes 'Network', 'Services', 'User Authentication', 'Devices', 'Maintenance', and 'Quick Setup'. The current page is 'Network - IP Filter Ruleset'. It features a 'Ruleset Name' input field, 'Rule Parameters' (IP Address, Subnet Mask, Protocol: All, Port Range, Action: Drop), and a list of services to generate rules for (e.g., BOOTP/DHCP, Telnet, HTTP, FTP, etc.). There are also 'Clear', 'Add Rule', and 'Apply' buttons.

2. Enter the following

<b>Ruleset Name</b>	Name that identifies a filter; may be composed of letters, numbers, and hyphens only. (The name cannot start with a hyphen.) <b>Example:</b> FILTER-2
---------------------	--

**Rule Parameters**

IP Address	Specify a single IP address to act as a filter. Example: 172.19.220.64 – this specific IP address only
Subnet Mask	Specify a subnet mask to act as a filter. Example: 255.255.0.0
Protocol	From the drop-down list, select the type of protocol through which the filter will operate. The default setting is All.

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. Examples: 22 – filter on port 22 only 23,64,80 – filter on ports 23, 64 and 80 23:64,80,143:150 – filter on ports 23 through 64, port 80 and ports 143 through 150
Action	Select whether to drop, reject, or allow 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.

3. Click the **right arrow** button to add the new rule to the bottom of the **Rules** list box on the right.
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 IP Filter page.

## Updating an IP Filter

The administrator can update an IP filter rule set.

1. On the IP Filter page, select the IP filter ruleset to be edited and click the **Edit Ruleset** button. The IP Filter Ruleset page displays.
2. Edit the information as desired and click the **Apply** button.

## Deleting an IP Filter

The administrator can delete an IP filter rule set.

1. On the IP Filter page, select the IP filter ruleset to be deleted and click the **Delete** button.

## Mapping a Rule Set

The administrator can assign an IP Filter Rule Set to a network interface (Ethernet interface), a modem connected to a Device Port, or a PC Card modem.



**To map a rule set to a network interface:**

1. On the IP Filter page, select the IP filter rule set 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 IP Filter page, select the mapping from the list and click the **Delete Mappings** button. The mapping no longer displays.
2. Click the **Apply** button.

## IP Filter Commands

The following CLI commands correspond to the web page entries described above.

---

**To enable or disable IP filtering for incoming network traffic:**

```
set ipfilter state
```

---

**To set IP filter mapping:**

```
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>
pccardslot <upper|lower> state <disable>
pccardslot <upper|lower> state <enable> ruleset
<Ruleset Name>
```

---

**To set IP filter rules:**

```
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>
```

---

## 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:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'Network' tab is selected, and the 'Routing' sub-tab is active. The main content area is titled 'Routing' and contains several configuration options:

- Enable RIP:** A checkbox that is currently unchecked.
- RIP Version:** Radio buttons for version 1, 2 (selected), and 1 and 2.
- Enable Static Routing:** A checkbox that is currently unchecked.
- IP Address, Subnet Mask, Gateway:** Three input fields for configuring static routes.
- Buttons:** 'Add/Edit Route', 'Delete Route', and 'Apply' buttons.
- Static Routes Table:** A table with columns for 'No', 'IP Address', 'Subnet Mask', and 'Gateway'.

2. Enter the following:

### Dynamic Routing

<b>Enable RIP</b>	Select to enable Dynamic Routing Information Protocol (RIP) to assign routes automatically. Disabled by default.
<b>RIP Version</b>	Select the RIP version. The default is 2.

### Static Routing

<b>Enable Static Routing</b>	<p>Select to assign the routes manually. The system administrator usually provides the routes. Disabled by default.</p> <ul style="list-style-type: none"> <li>◆ To add a static route, enter the <b>IP Address</b>, <b>Subnet Mask</b>, and <b>Gateway</b> for the route and click the <b>Add/Edit Route</b> button. The route displays in the Static Routes table. You can add up to 64 static routes.</li> <li>◆ To edit a static route, select the radio button to the right of the route, change the <b>IP Address</b>, <b>Subnet Mask</b>, and <b>Gateway</b> fields as desired, and click the <b>Add/Edit Route</b> button.</li> <li>◆ To delete a static route, select the radio button to the right of the route and click the <b>Delete Route</b> button.</li> </ul>
------------------------------	--

3. Click the **Apply** button.

**Note:** To display the routing table, click the **IP Routes Report** link. The **Status/Reports** page displays. To view the report, select the **IP Routes** checkbox and click **Generate Report**.

## Equivalent Routing Commands

The following CLI commands correspond to the web page entries described above.

---

### To configure static or dynamic routing:

```
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>
```

**Note:** To delete a static route, set the IP address, mask, and gateway parameters to **0.0.0.0**.

---

### To set the routing table to display IP addresses (disable) or the corresponding host names (enable):

```
show routing [resolveip <enable|disable>] [email <Email Address>]
```

**Note:** You can optionally email the displayed information.

---

## 7: Services

### System Logging and Other Services

Use the Services 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. MIB definition files for the private enterprise MIB are downloadable at <http://www.lantronix.com/support/downloads/>. The private enterprise MIB provides read-only access to all statistics and configurable items provided by the SLB. It provides read-write access to a select set of functions for controlling the SLB 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 branch office managers 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.

LANTRONIX® SLB884

User: sysadmin

Logout

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS SecureLinux Network Date & Time

### SSH/Telnet/Logging

**System Logging**

Network Level: Info

Services: Info

Authentication: Info

Device Ports: Info

Diagnostics: Info

General: Info

Remote Server #1: 172.18.100.29

#2:

**SSH**

Enable Logins:  Web SSH:

Timeout:  No  Yes: 0 minutes

SSH Port: 22

SSH V1 Logins:

**Telnet**

Enable Logins:  Web Telnet:

Timeout:  No  Yes: 0 minutes

**SMTP**

Server:

**Phone Home**

Enable:

IP Address:

Last Attempt: N/A Results: N/A

Apply

2. Enter the following settings:

### System Logging

In the System Logging section, select one of the following alert levels from the drop-down list for each message category:

- ◆ **Off:** Disables this type of logging.
- ◆ **Info:** Saves informative message, in addition to warning and error messages.
- ◆ **Warning:** 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.
- ◆ **Error:** Saves messages that are output because of an error.
- ◆ **Debug:** Saves extraneous detail that may be helpful in tracking down a problem, in addition to information, warning, and error messages.

<b>Network Level</b>	Messages concerning the network activity, for example about Ethernet and routing.
<b>Services</b>	Messages concerning services such as SNMP and SMTP.
<b>Authentication</b>	Messages concerning user authentication.
<b>Device Ports</b>	Messages concerning device ports and connections.
<b>Diagnostics</b>	Messages concerning system status and problems.
<b>General</b>	Any message not in the categories above.

<b>Remote Servers (#1 and #2)</b>	<p>IP address of the remote server(s) where system logs are stored.</p> <p>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.</p>
-----------------------------------	---

## SSH

<b>Enable Logins</b>	<p>Enables or disables SSH logins to the SLB branch office manager to allow users to access the CLI using SSH. Enabled by default.</p> <p>This setting does not control SSH access to individual device ports. (See <a href="#">Device Ports – Settings</a> on page 84 for information on enabling SSH access to individual ports.)</p> <p>Most system administrators enable SSH logins, which is the preferred method of accessing the system.</p>
<b>Web SSH</b>	<p>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.</p>
<b>Timeout</b>	<p>If you enable SSH logins, you can cause an idle connection to disconnect after a specified number of minutes. Select <b>Yes</b> and enter a value of from 1 to 30 minutes.</p> <p><b>Note:</b> You must reboot the unit before a change will take effect.</p>
<b>SSH Port</b>	<p>Allows you to change the SSH login port to a different value in the range of 1 - 65535. The default is 22.</p> <p><b>Note:</b> You must reboot the unit before a change will take effect.</p>
<b>SSH V1 Logins</b>	<p>Enables or disables SSH version 1 connections to the SLB branch office manager. Enabled by default.</p> <p><b>Note:</b> Disabling SSH V1 blocks Web SSH CLI and Web SSH to device port connections on the SLB Network page. Also, you must reboot the SLB device before a change will take effect.</p>

## Telnet

<b>Enable Logins</b>	<p>Enables or disables Telnet logins to the SLB branch office manager to allow users to access the CLI using Telnet. Disabled by default.</p> <p>This setting does not control Telnet access to individual device ports. (See <a href="#">Device Ports – Settings</a> on page 84 for information on enabling Telnet access to individual ports.)</p> <p>You may want to keep this option disabled for security reasons.</p>
----------------------	---

<b>Web Telnet</b>	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.
<b>Timeout</b>	If you enable Telnet logins, you can cause an idle connection to disconnect after a specified number of minutes. Select <b>Yes</b> and enter a value of from 1 to 30 minutes.  <i>Note: You must reboot the unit before a change will take effect.</i>

### Audit Log

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

### SMTP

<b>Server</b>	IP address of your network's Simple Mail Transfer Protocol (SMTP) relay server.
---------------	---

### Phone Home

<b>Enable</b>	If enabled, the SLB branch office manager will attempt to phone home every hour until it has contacted an SLM management appliance and provided it with its configuration.
<b>IP Address</b>	IP address of the SLM management appliance.
<b>Last Attempt</b> (view only)	Date and time of last connection attempt.
<b>Results</b> (view only)	Indicates whether the attempt was successful.

- 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:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The Services tab is selected, and the SNMP option is highlighted. The main content area is titled 'SNMP' and contains the following configuration options:

- Enable Agent:**
- Enable Traps:**
- NMS:** 172.18.100.29
- Communities:**
  - Read-Only: public
  - Read-Write: private
  - Trap: public
  - Location: location
  - Contact: contact
  - Alarm Delay: 60 seconds
- Version 3:**
  - Security:  No Auth/No Encrypt,  Auth/No Encrypt,  Auth/Encrypt
  - Auth with:  MD5,  SHA
  - Encrypt with:  DES,  AES
  - V3 Read-Only User:**
    - User Name: snmpuser
    - Password: [masked]
    - Retype Password: [masked]
    - Passphrase: [empty]
    - Retype Passphrase: [empty]
  - V3 Read-Write User:**
    - User Name: snmprwuser
    - Password: [masked]
    - Retype Password: [masked]
    - Passphrase: [empty]
    - Retype Passphrase: [empty]

An 'Apply' button is located at the bottom of the configuration area.

2. Enter the following:

<b>Enable Agent</b>	Enables or disables SNMP agent, which allows read-only access to the system. Disabled by default.
<b>Enable Traps</b>	<p>Traps are notifications of certain critical events. Disabled by default. This feature is applicable when SNMP is enabled. Examples of traps that the SLB branch office manager sends include:</p> <ul style="list-style-type: none"> <li>◆ Ethernet Port Link Up</li> <li>◆ Ethernet Port Link Down</li> <li>◆ Authentication Failure</li> <li>◆ SLB Booted</li> <li>◆ SLB Shutdown</li> <li>◆ Device Port Logging</li> <li>◆ Power Supply Status</li> <li>◆ Sysadmin user password changed</li> </ul> <p>The SLB branch office manager sends the traps to the host identified in the <b>NMS</b> field.</p>



<b>NMS</b>	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 branch office manager and receive traps from the SLB device. Enter the IP address of the NMS server. Required if you selected <b>Enable Traps</b> .
<b>Location</b>	Physical location of the SLB branch office manager (optional). Useful for managing the SLB device using SNMP. Up to 20 characters.
<b>Contact</b>	Description of the person responsible for maintaining the SLB branch office manager, for example, a name (optional). Up to 20 characters.
<b>Alarm Delay</b>	Number of seconds delay between outgoing SNMP traps.

### Communities

<b>Trap</b>	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 <b>public</b> .
<b>Read-Only</b>	A string that acts like a password for an SNMP manager to access the read-only data the SLB SNMP agent provides. The default is <b>public</b> .
<b>Read-Write</b>	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 default is <b>private</b> .

### Version 3

<b>Security</b>	Levels of security available with SNMP v. 3. <b>No Auth/No Encrypt:</b> No authentication or encryption. <b>Auth/No Encrypt:</b> Authentication but no encryption. (default) <b>Auth/Encrypt:</b> Authentication and encryption.
<b>Auth with</b>	For <b>Auth/No Encryp</b> or <b>Auth/Encrypt</b> , the authentication method: <b>MD5:</b> Message-Digest algorithm 5 (default) <b>SHA:</b> Secure Hash Algorithm
<b>Encrypt with</b>	Encryption standard to use: <b>DES:</b> Data Encryption Standard (default) <b>AES:</b> Advanced Encryption Standard

### V3 Read-Only User

<b>User Name</b>	SNMP v3 is secure and requires user-based authorization to access SLB MIB objects. Enter a user ID. The default is <b>snmpuser</b> . Up to 20 characters.
<b>V3 Password/Retype Password</b>	Password for a user with read-only authority to use to access SNMP v3. The default is <b>SNMPPASS</b> . Up to 20 characters.
<b>Passphrase/Retype Passphrase</b>	Passphrase associated with the password for a user with read-only authority. Up to 20 characters.

### V3 Read-Write User

<b>User Name</b>	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 <b>snmprwuser</b> . Up to 20 characters.
<b>V3 Password/Retype Password</b>	Password for the user with read-write authority to use to access SNMP v3. The default is <b>SNMPRWPASS</b> . Up to 20 characters.
<b>Passphrase/Retype Passphrase</b>	Passphrase associated with the password for a user with read-write authority. Up to 20 characters.

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

## SNMP, SSH, Telnet, and Logging Commands

The following CLI commands correspond to the web page entries described above.

**To configure services (system logging, SSH and Telnet access, SSH and Telnet timeout, SNMP agent, email (SMTP) server, and audit log):**

```
set services <one or more services parameters>
```

*Parameters:*

```
alarmdelay <1-6000 Seconds>
auditlog <enable|disable>
auditsize <Size in Kbytes>
Range is 1-500 Kbytes.
authlog <off|error|warning|info|debug>
clicommands <enable|disable>
contact <Admin contact info>
devlog <off|error|warning|info|debug>
diaglog <off|error|warning|info|debug>
genlog <off|error|warning|info|debug>
includesyslog <enable|disable>
```

---

```
location <Physical Location>
netlog <off|error|warning|info|debug>
nms <IP Address or Name>
phonehome <enable|disable>
phoneip <IP Address>
portssh <TCP Port>
rocommunity <Read-Only Community Name>
rwcommunity <Read-Write Community Name>
servlog <off|error|warning|info|debug>
smtpserver <IP Address or Hostname>
snmp <enable|disable>
ssh <enable|disable>
syslogserver1 <IP Address or Name>
syslogserver2 <IP Address or Name>
telnet <enable|disable>
timeoutssh <disable or 1-30>
timeouttelnet <disable or 1-30>
traps <enable|disable>
trapcommunity <Trap Community>
v1ssh <enable|disable>
v3user <V3 RO User>
v3password <V3 RO User Password>
v3phrase <V3 RO User Passphrase>
v3rwuser <V3 RW User>
v3rwpassword <V3 RW User Password>
v3rwphrase <V3 RW User Passphrase>
v3security <noauth|auth|authencrypt>
v3auth <md5|sha>
v3encrypt <des|aes>
v3password <Password for v3 auth>
v3user <User for v3 auth>
webssh <enable|disable>
webtelnet <enable|disable>
```

---

---

**To view current services:**

show services

---

## NFS and SMB/CIFS

Use the NFS & SMB/CIFS page if you want to save configuration and logging data onto a remote NFS server, or export configuration and logging data 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 device 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 device exports a single read-write CIFS share called "public," with two subdirectories:

- ◆ The `logs` directory, which contains the system logs and the device port local buffers (see [System Logs](#) on page 190) and is read-only.
- ◆ 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. Users can also access the device port local buffers from the CIFS share (see [Device Ports – Logging](#) on page 98).

### To configure NFS and SMB/CIFS:

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

**LANTRONIX® SLB884**

User: sysadmin

Select port for  configuration or  WebSSH (Device Port only)

**NFS & SMB/CIFS**

**NFS Mounts**

	Remote Directory	Local Directory	Read-Write	Mount
#1:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
#2:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
#3:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

**SMB/CIFS Share**

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](#).

Share SMB/CIFS directory:

Network Interfaces:  Eth1 (172.18.21.64)  Eth2

CIFS User Password:

Retype Password:

Workgroup:

The SMB/CIFS share can be accessed by the 'cifsuser' login.

- Enter the following for up to three directories:

### NFS Mounts

<b>Remote Directory</b>	The remote NFS share directory in the format: <b>nfs_server_hostname</b> or <b>ipaddr:/exported/path</b>
<b>Local Directory</b>	The local directory on the SLB branch office manager on which to mount the remote directory. The SLB device creates the local directory automatically.
<b>Read-Write</b>	If enabled, indicates that the SLB branch office manager 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.
<b>Mount</b>	Select the checkbox to enable the SLB device to mount the file to the NFS server. Disabled by default.

- Enter the following:

### SMB/CIFS Share

<b>Share SMB/CIFS directory</b>	Select the checkbox to enable the SLB branch office manager to export an SMB/CIFS share called "public." Disabled by default.
---------------------------------	---

<b>Network Interfaces</b>	Select the network ports from which the share can be seen. The default is for the share to be visible on both network ports.
<b>CIFS User Password/Retype Password</b>	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 <b>CIFSPASS</b> .  More than one user can access the share with the <b>cifsuser</b> user name and password at the same time.
<b>Workgroup</b>	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.

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

## NFS and SMB/CIFS Commands

The following CLI commands correspond to the web page entries described above.

### To mount a remote NFS share:

```
set nfs mount <one or more parameters>
```

*Parameters:*

```
locdir <Directory>
mount <enable|disable>
remdir <Remote NFS Directory>
rw <enable|disable>
Enables read/write access to remote directory.
```

**Note:** The *remdir* and *locdir* parameters are required, but if you specified them previously, you do not need to provide them again.

### To unmount a remote NFS share:

```
set nfs unmount <1|2|3>
```

### To view NFS share settings:

```
show nfs
```

**To configure the SMB/CIFS share, which contains the system and device port logs:**

```
set cifs <one or more parameters>
```

*Parameters:*

```
eth1 <enable|disable>
```

```
eth2 <enable|disable>
```

```
state <enable|disable>
```

```
workgroup <Windows workgroup>
```

**Note:** The `admin config` command saves SLB configurations on the SMB/CIFS share.

---

**To change the password for the SMB/CIFS share login (default is cifsuser):**

```
set cifs password
```

---

**To view SMB/CIFS settings:**

```
show cifs
```

---

## Secure Lantronix Network

Use the Secure Lantronix Network option to view and manage SLC console manager and Spiders 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.

**To view and manage SLB branch office managers and Lantronix® Spiders™ on the local network:**

1. Click the **Services** tab and select the **Secure Lantronix Network** option. The following page displays.



LANTRONIX<sup>®</sup> SLB884

Logout User: sysadmin Select port for  configuration or  WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance Quick Setup

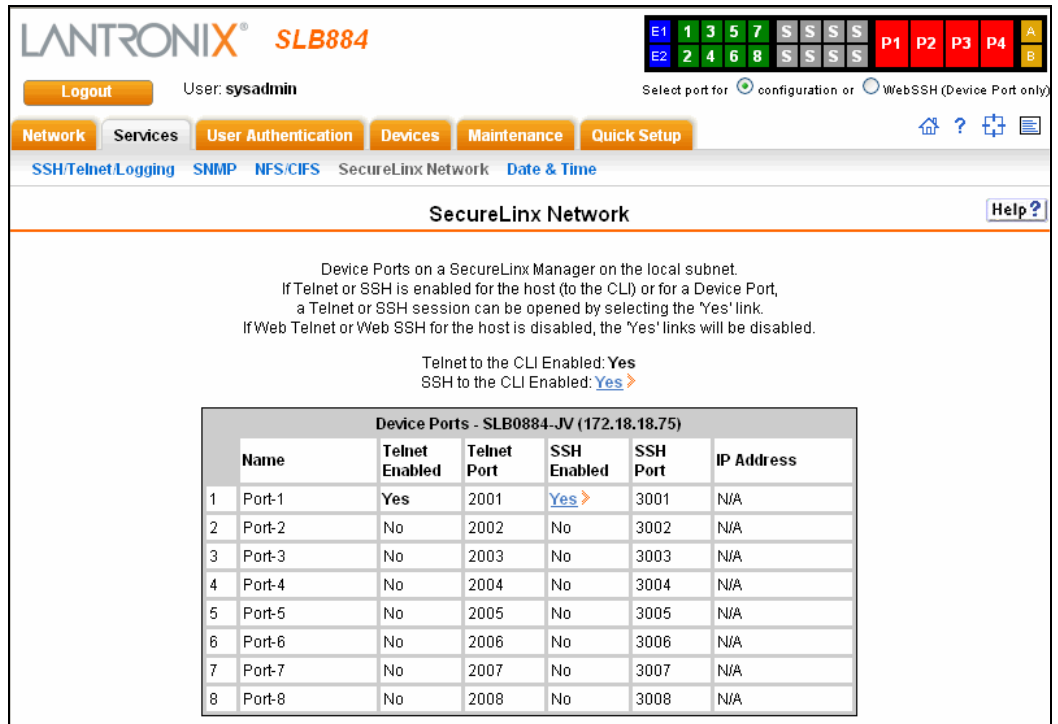
SSH/Telnet/Logging SNMP NFS/CIFS SecureLinX Network Date & Time

### SecureLinX Network Help ?

SecureLinX Managers and Spiders on the local subnet.  
Each host can be managed by selecting its IP address. [Search Options >](#)

Model	IP Address/ Web Interface	Telnet/SSH to Device Ports or CLI	HW Address	Firmware Version	Serial Number
SLB884	<a href="#">172.18.18.75 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:8d:00:c0	5.2	0080A38D00C0
SLC48	<a href="#">172.18.12.200 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:0b:6d	5.3	0080A3890B6D
SLC16	<a href="#">172.18.11.210 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:01:a7	5.2	0080A38901A7
SLC48	<a href="#">172.18.18.55 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:00:fb	5.2	0080A38900FB
SLC48	<a href="#">172.18.21.61 &gt;</a>	<a href="#">View &gt;</a>	00:30:31:ff:ff:42	5.3	003031FFFF42
SLC48	<a href="#">172.18.18.56 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:0e:f9	5.3	0080A3890EF9
SLC32	<a href="#">172.18.0.107 &gt;</a>	<a href="#">View &gt;</a>	00:30:31:ff:ff:54	5.2	003031FFFF54
SLC48	<a href="#">172.18.26.100 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:12:7d	5.2	0080A389127D
SLC8	<a href="#">172.18.21.63 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:1e:29	5.3	0080A3891E29
SLC16	<a href="#">172.18.23.110 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:25:37	5.2	0080A3892537
SLC8	<a href="#">172.18.19.50 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:2d:a1	5.2	0080A3892DA1
SLB884	<a href="#">172.18.21.64 &gt;</a>	<a href="#">View &gt;</a>	00:80:a3:89:42:3d	5.3	0080A389423D
Spider	<a href="#">172.18.18.45 &gt;</a>	N/A	00:80:a3:8c:1c:f9	2.1	008014007417
Spider	<a href="#">172.18.37.4 &gt;</a>	N/A	00:80:a3:8c:1c:94	2.1	008014007316
Spider	<a href="#">172.18.21.77 &gt;</a>	N/A	00:80:a3:de:fa:ce	2.1	0080EF44E10D
Spider	<a href="#">172.18.21.75 &gt;</a>	N/A	00:20:4a:80:8c:0a	2.1	002048447B1B
Spider	<a href="#">172.18.18.44 &gt;</a>	N/A	00:80:a3:8c:0d:dd	2.0	008033353439
Spider	<a href="#">172.18.11.18 &gt;</a>	N/A	00:80:a3:8c:0f:b2	2.1	008014004018

2. To manage a secure IT management device, click its **IP Address**. A separate browser page takes the user to the web interface for the selected Secure IT management device (login required).
3. For SLM management appliances, if SSH or Telnet is enabled for the device (to the CLI) or for a device port and you want to access the device or device port:
  - a) Click the **View** link in the **Telnet/SSH to Device Ports or CLI** column. The following page displays:



LANTRONIX<sup>®</sup> SLB884

Logout User: sysadmin Select port for  configuration or  WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS SecureLinux Network Date & Time

### SecureLinux Network

Device Ports on a SecureLinux Manager on the local subnet.  
If Telnet or SSH is enabled for the host (to the CLI) or for a Device Port, a Telnet or SSH session can be opened by selecting the 'Yes' link.  
If Web Telnet or Web SSH for the host is disabled, the 'Yes' links will be disabled.

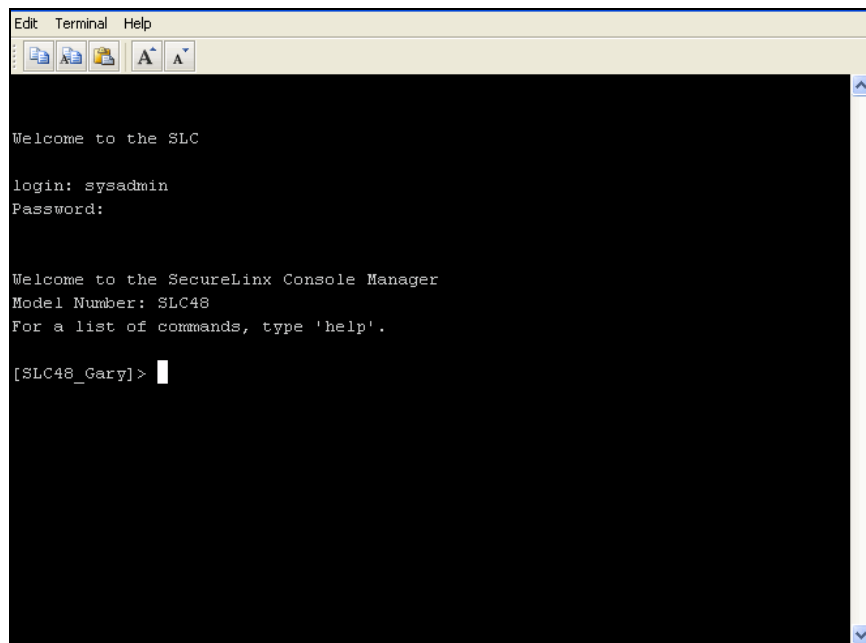
Telnet to the CLI Enabled: [Yes](#)  
SSH to the CLI Enabled: [Yes](#) >

Device Ports - SLB0884-JV (172.18.18.75)						
Name	Telnet Enabled	Telnet Port	SSH Enabled	SSH Port	IP Address	
1 Port-1	Yes	2001	<a href="#">Yes</a> >	3001	N/A	
2 Port-2	No	2002	No	3002	N/A	
3 Port-3	No	2003	No	3003	N/A	
4 Port-4	No	2004	No	3004	N/A	
5 Port-5	No	2005	No	3005	N/A	
6 Port-6	No	2006	No	3006	N/A	
7 Port-7	No	2007	No	3007	N/A	
8 Port-8	No	2008	No	3008	N/A	

Above the table, the **Telnet to the CLI Enabled** and **SSH to the CLI Enabled** fields indicate whether the unit has been set for Telnet or SSH access to the CLI. The table page lists all of the unit's device ports (if applicable), indicates whether they are Telnet enabled or SSH enabled, and lists their Telnet and SSH port numbers.

**Note:** For the links to work, you must enable **Web Telnet** or **Web SSH** for the secure IT management unit.

- b) To open a Telnet session to the CLI, click **Yes** in the **Telnet to the CLI Enabled** field above the table.



```

Edit Terminal Help
Welcome to the SLC
login: sysadmin
Password:

Welcome to the SecureLinux Console Manager
Model Number: SLC48
For a list of commands, type 'help'.

[SLC48_Gary]>

```

- c) To open a Telnet session to a specific device port, click the **Yes** link in the **Telnet Enabled** column.
- d) To open an SSH session to the CLI, click **Yes** in the **SSH to the CLI Enabled** field above the table.
- e) To open an SSH session to a specific device port, click the **Yes** link in the **SSH Enabled** column.

**To configure how secure IT management devices are searched for on the network:**

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

2. Enter the following:

<p><b>Secure Lantronix Network Search</b></p>	<p>Select the type of search you want to conduct.</p> <p><b>Local Subnet</b> performs a broadcast to detect secure IT management devices on the local subnet.</p> <p><b>Manually Entered IP Address List</b> provides a list of IP addresses that may not respond to a broadcast because of how the network is configured.</p> <p>The default is <b>Both</b>.</p>
<p><b>IP Address</b></p>	<p>If you selected <b>Manually Entered IP Address List</b> or <b>Both</b>, enter the IP address of the secure IT management device you want to find and manage.</p>

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 Secure Lantronix Network page displays the secure IT management devices resulting from the search. You can now manage these devices.

## Secure Lantronix Network Commands

The following commands for the command line interface correspond to the web page entries described above.

---

### To detect and view all SLB branch office manager or user-defined IP addresses on the local network:

```
set slcnetwork <one or more parameters>
```

*Parameters:*

```
add <IP Address>
```

```
delete <IP Address>
```

```
search <localsubnet|ipaddrlist|both>
```

---

### To detect and display all secure IT managers and Spiders on the local network:

```
show slcnetwork [ipaddrlist <all|Address Mask>]
```

**Note:** Without the `ipaddrlist` parameter, the command searches the network according to the search setting. 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`).

---

## Date and Time

You can specify the current date, time, and time zone at the SLB branch office manager's location (default), or the SLB device 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:

LANTRONIX<sup>®</sup> SLB884

Logout User: sysadmin Select port for  configuration or  WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS SecureLinux Network Date & Time

### Date & Time Help?

Change Date/Time:

Date: April 24 2008

Time: 02 : 37 : 59 pm

Time Zone: PST8PDT

---

Enable NTP:  The SLB can synchronize its clock with a remote time server using NTP.

Synchronize via:  Broadcast from NTP Server  Poll NTP Server(s):

Local:  #1:   
 #2:   
 #3:

Public:  US/San Jose: clock.sjc.he.net (216.218.254.202)

Apply

2. Enter the following:

<b>Change Date/Time</b>	Select the checkbox to manually enter the date and time at the SLB branch office manager's location.
<b>Date</b>	From the drop-down lists, select the current month, day, and year.
<b>Time</b>	From the drop-down lists, select the current hour and minute.
<b>Time Zone</b>	From the drop-down list, select the appropriate time zone.

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

### To synchronize the SLB branch office manager with a remote timeserver using NTP:

1. Enter the following:

<b>Enable NTP</b>	Select the checkbox to enable NTP synchronization. NTP is disabled by default.
-------------------	--

<b>Synchronize via</b>	<p>Select one of the following:</p> <p><b>Broadcast from NTP Server:</b> Enables the SLB branch office manager to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP.</p> <p><b>Poll NTP Server:</b> Enables the SLB device to query the NTP Server for the correct time. If you select this option, complete one of the following:</p> <p><b>Local:</b> 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.</p> <p><b>Public:</b> 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.)</p> <p>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.</p>
------------------------	---

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

## Date and Time Commands

The following CLI commands correspond to the web page entries described above.

### To set the local date, time, and local time zone (one parameter at a time):

```
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.

### To view the local date, time, and time zone:

```
show datetime
```

**To synchronize the SLB branch office manager with a remote time server using NTP:**

```
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>
```

---

**To view NTP settings:**

```
show ntp
```

---

## 8: Device Ports

This chapter describes how to configure and use an SLB branch office manager device port connected to an external device, such as a server or a modem. The next chapter, [10: Connections](#), describes how to use the Connections web page to connect external devices and outbound network connections (such as Telnet or SSH) in various configurations. The 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 the IP address. For Telnet and SSH, use the default TCP port number (23 and 22, respectively) to connect to the device port. For raw TCP, use the TCP port number defined for **TCP In** to the device port on the [Device Ports – Settings](#) page.
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:

- ◆ **Direct (or data) mode:** The user can interact with and monitor the device port (`connect direct` command).
- ◆ **Listen mode:** The user can only monitor the device port (`connect listen` command).
- ◆ **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 Device Status page displays the status of the SLB branch office manager's ports, PC card slots and power outlets.

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

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there is a status bar with port indicators (E1-E2, 1-8, S, P1-P4, A, B) and a user login section for 'User: sysadmin'. Below the navigation tabs, the 'Device Status' page is displayed, featuring three data tables:

Device Port Status and Counters					
No	Name	DSR	Bytes Input/Output	Errors	Connection Status
1	Port-1	No	0/0	0	Idle
2	Port-2	No	0/0	0	Idle
3	Port-3	No	0/0	0	Idle
4	Port-4	No	0/0	0	Idle
5	Port-5	No	0/0	0	Idle
6	Port-6	No	0/0	0	Idle
7	Port-7	No	0/0	0	Idle
8	Port-8	No	0/0	0	Idle

PC Card Slots			
Slot	Device	Type	State
Upper	none	N/A	N/A
Lower	none	N/A	N/A

Power Outlets		
Outlet	Name	State
P1	PowerOutlet-1	On
P2	PowerOutlet-2	On
P3	PowerOutlet-3	On
P4	PowerOutlet-4	On

## Global Port Settings

On the 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 Status** option. The following page displays:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a user login section for 'sysadmin' and a 'Logout' button. Below that are navigation tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'Device Ports' tab is active, showing a 'Device Status' section and a 'Device Ports' configuration area. The configuration area has two main sections: 'Telnet/SSH/TCP In Port Numbers' and 'Device Port Limits'. The first section has input fields for 'Starting Telnet Port' (2001), 'Starting SSH Port' (3001), and 'Starting TCP Port' (4001). The second section has an input field for 'Direct Connects' (1) with '(maximum)' next to it. To the right is a table titled 'Ports:' with columns 'No', 'Name', 'Mode', and 'Select'. The table lists ports 1 through 8, all currently in 'Idle' mode. A 'Configure' button is at the top right of the table.

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.



The port is in data/text mode.

**Note:** You may set up ports to allow Telnet access using the IP Settings on the Device Ports – Settings page.



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



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

Starting Telnet Port	Description
	Each port is assigned a number for connecting via Telnet. Enter a number (1025-65535) 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.

<b>Starting SSH Port</b>	Each port is assigned a number for connecting via SSH. Enter a number (1025-65535) 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.
<b>Starting TCP Port</b>	<p>Each port is assigned a number for connecting through a raw TCP connection. Enter a number (1025-65535) that represents the first port. The default is 4000 plus the port number. For example, if you enter 4001, subsequent ports are automatically numbered 4002, 4003, and so on.</p> <p>You can use a raw TCP connection in situations where a TCP/IP connection is to communicate with a serial device. For example, you can connect a serial printer to a device port and use a raw TCP connection to spool print jobs to the printer over the network.</p> <p><b>Note:</b> When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, set the <b>Break Sequence</b> of the respective device port to null (clear it).</p>

**Caution:** Ports 1-1024 are RFC-assigned and may conflict with services running on the SLB branch office manager. 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 [Device Ports – Settings](#) on page 84.

## Global Commands

The following CLI commands correspond to the web page entries described above.

**To configure settings for all or a group of device ports:**

```
set deviceport global <one or more parameters>
```

*Parameters:*

```
maxdirect <1-10>
```

*Sets the maximum number of direct connections for each device port.*

```
sshport <TCP Port>
```

```
tcpport <TCP Port>
```

```
telnetport <TCP Port>
```

*Port is a port number between 1025 and 65535.*

---

**To view global settings for device ports:**

```
show deviceport global
```

---

## Global Commands

The following CLI commands correspond to the web page entries described above.

---

**To configure settings for all or a group of device ports:**

```
set deviceport global <one or more parameters>
```

*Parameters:*

```
maxdirect <1-10>
```

*Sets the maximum number of direct connections for each device port.*

```
sshport <TCP Port>
```

```
tcpport <TCP Port>
```

```
telnetport <TCP Port>
```

*Port is a port number between 1025 and 65535.*

---

**To view global settings for device ports:**

```
show deviceport global
```

---

## 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 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 (shown below) at the top of any page:



The following page displays:

LANTRONIX® SLB884

Logout    User: **sysadmin**    Select port for  configuration or  WebSSH (Device Port only)

Network
Services
User Authentication
Devices
Maintenance
Quick Setup

Device Status
Device Ports
Console Port
PC Card
Power Outlets
Connections
Host Lists

### Device Ports - Settings Help?

Port: 3  
Mode: **Idle**  
Name:   
Banner:   
Break Sequence:   
Note: remove Break Sequence for Device Ports connected to raw binary connections.  
Logging: [Settings >](#)  
Zero Port Counters:

Connected to:  [Device Commands >](#)

**IP Settings**

Enable Telnet In:  Port:  Authenticate:

Enable SSH In:  Port:  Authenticate:

Enable TCP In:  Port:  Authenticate:

IP Address:

Web SSH/Telnet Columns:  Rows:

**Data Settings**

Baud:

Data Bits:

Stop Bits:

Parity:

Flow Control:

Enable Logins:

Show Lines On Connecting:

**Modem Settings**

State:  Mode:  Text  PPP

Initialization Script:

Modem Timeout:  No  Yes, seconds (1-9999):

Caller ID Logging:  Modem Command:

**Text Mode**

Timeout Logins:  No  Yes, minutes (1-30):

Dial-back Number:  Local User Number  Fixed Number:

Dial-in Host List:  [Host Lists >](#)

**PPP Mode**

Negotiate IP Address:  Yes  No    Local IP:  Remote IP:

Authentication:  PAP  CHAP

CHAP Handshake: Host/User Name:   
Secret/User Password:

Same authentication for Dial-in & Dial-on-Demand (DOD):

DOD Authentication:  PAP  CHAP

DOD CHAP Handshake: Host/User Name:   
Secret/User Password:

Enable NAT:  Note: Enabling NAT requires [IP Forwarding](#) to be enabled.

Dial-out Number:

Dial-out Login:

Dial-out Password:  Retype:

Restart Delay:  seconds

Port Status and Counters	
DSR/CD	No
DTR	Yes
CTS	No
RTS	Yes
Bytes input	0
Bytes output	0
Framing errors	0
Parity errors	0
Overrun errors	0
Flow Control errors	0
Seconds since zeroed	524955

[Back to Device Ports](#)
Apply
Apply Settings:  to Device Ports:

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

**To enter device port settings:**

1. Enter the following:

<b>Mode</b>	The status of the port; displays automatically.
<b>Name</b>	The name of the port. Valid characters are letters, numbers, dashes (-), periods, and underscores ( _ ).
<b>Banner</b>	Text to display when a user connects to a device port by means of Telnet, SSH, or TCP. If authentication is enabled for the device port, the banner displays once the user successfully logs in. Blank is the default.
<b>Break Sequence</b>	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 <b>Esc+B</b> (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as <b>\x1bB</b> , which is hexadecimal ( <b>\x</b> ) character 27 ( <b>1B</b> ) followed by a <b>B</b> .
<b>Logging</b>	Click the <b>Settings</b> link to configure file logging, email logging, local logging, and PC Card logging. (See <a href="#">Device Ports – Logging</a> on page 98.)
<b>Zero Port Counters</b>	Resets all of the numerical values in the Port Counters table at the bottom of the page to zero (0).
<b>Connected to</b>	The type of device connected to the device port. Presently, the SLB branch office manager supports SLP power manager (SLP8 and SLP16) and Sensorsoft devices. If the type of device is not listed, select <b>undefined</b> .  If you select anything other than <b>undefined</b> , click <b>Device Commands</b> . The appropriate web page displays.

**IP Settings**

<b>Enable Telnet In</b>	Enables access to this port through Telnet. Disabled by default.
<b>Enable SSH In</b>	Enables access to this port through SSH. Disabled by default.
<b>Enable TCP in</b>	Enables access to this port through a raw TCP connection. Disabled by default.  <i>Note: When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, set the <b>Break Sequence</b> of the respective device port to null (clear it).</i>
<b>Port</b>	Automatically assigned Telnet, SSH, and TCP port numbers. (See <a href="#">8: Device Ports</a> for information on setting up the numbering scheme.) You may override this value, if desired.
<b>Authenticate</b>	If selected, the SLB branch office manager requires user authentication before granting access to the port. <b>Authenticate</b> is selected by default for <b>Telnet in</b> and <b>SSH in</b> , but not for <b>TCP in</b> .

<b>IP Address</b>	<p>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.</p> <p>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 <b>TCP In</b> to the device port is used.</p>
<b>Web SSH/Telnet Columns</b>	Number of columns in the Web SSH/Telnet applet when this device port is accessed via the applet.
<b>Web SSH/Telnet Rows</b>	Number of rows in the Web SSH/Telnet applet when this device port is accessed via the applet.

### 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.

<b>Baud</b>	<p>The speed with which the device port exchanges data with the attached serial device.</p> <p>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.</p>
<b>Data Bits</b>	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is <b>8</b> data bits.
<b>Stop Bits</b>	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 <b>1</b> .
<b>Parity</b>	Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is <b>none</b> .
<b>Flow Control</b>	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 <b>none</b> .
<b>Enable Logins</b>	<p>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.</p> <p>Disabled is the default and is the correct setting if the device port is the endpoint for a connection.</p>

<b>Show Lines on Connecting</b>	<p>If enabled, when the user either does a <code>connect direct</code> 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.</p> <p>For example, an SLB branch office manager issues a <code>connect direct device 1</code> command to connect port 1 to a Linux server.</p> <p>Then the SLB device user gets a directory with the <code>ls</code> command exits the connection. When the SLB user issues another <code>direct connect device 1</code>", the output of the <code>ls</code> command (or some portion of it) is output again, so the user can know what state the server was left in.</p>
---------------------------------	---

### Hardware Signal Triggers

<b>Check DSR on Connect</b>	<p>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.</p>
<b>Disconnect on DSR</b>	<p>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.</p>

### Modem Settings

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

<b>State</b>	<p>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.</p>
<b>Mode</b>	<p>The format in which the data flows back and forth:</p> <p><b>Text:</b> 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. <b>Text</b> is the default.</p> <p><b>PPP:</b> This mode establishes an IP-based link over the modem. PPP connections can be used in dial-out mode (e.g., the SLB device 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), or dial-on-demand.</p>



<b>Initialization Script</b>	<p>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 device uses a default initialization string of <b>AT S7=45 SO=0 L1 V1 X4 &amp;D2 &amp;c1 E1 Q0</b>.</p> <p><b>Note:</b> We recommend that the modem initialization script always be preceded with <b>AT</b> and include <b>E1 V1 x4 Q0</b> so that the SLB branch office manager may properly control the modem.</p>
<b>Modem Timeout</b>	<p>Timeout for all modem connections. Select Yes (default) for the SLB device 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.</p>
<b>Caller ID Logging</b>	<p>Select to enable the SLB branch office manager to log caller IDs on incoming calls. Disabled by default.</p> <p><b>Note:</b> For the Caller ID <b>AT</b> command, refer to the modem user guide.</p>
<b>Modem Command</b>	<p>Modem <b>AT</b> command used to initiate caller ID logging by the modem.</p> <p><b>Note:</b> For the <b>AT</b> command, refer to the modem user guide.</p>

### Modem Settings: Text Mode

<b>Timeout Logins</b>	<p>If you selected <b>Text</b> mode, you can enable logins to time out after the connection is inactive for a specified number of minutes. The default is <b>No</b>. This setting is only applicable for text mode connections. <b>PPP</b> mode connections stay connected until either side drops the connection. Disabled by default.</p>
<b>Dial Back Number</b>	<p>Users with dial-back access can dial into the SLB branch office manager and enter their login and password. Once the SLB device authenticates them, the modem hangs up and dials them back.</p> <p>Select the phone number the modem dials back on a fixed number or a number associated with their login. If you select <b>Fixed Number</b>, enter the number (in the format 2123456789).</p>
<b>Dial-in Host List</b>	<p>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 <b>connect direct</b> at the CLI. The hosts in the list are cycled through until the SLB branch office manager successfully connects to one.</p> <p>To establish and configure host lists, click the <b>Host Lists</b> link.</p>

## Modem Settings: PPP Mode

<b>Negotiate IP Address</b>	<p>If the SLB branch office manager and/or the serial device have dynamic IP addresses (e.g., IP addresses assigned by a DHCP server), select <b>Yes</b>. <b>Yes</b> is the default.</p> <p>If the SLB branch office manager or the modem have fixed IP addresses, select <b>No</b>, and enter the local IP (IP address of the port) and remote IP (IP address of the modem).</p>
<b>Authentication</b>	<p>Enables <b>PAP</b> or <b>CHAP</b> authentication for modem logins. <b>PAP</b> 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.</p>
<b>CHAP Handshake</b>	<p>The host/username (for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.</p>
<b>Same authentication for Dial-in &amp; Dial-on-Demand (DOD)</b>	<p>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.</p>
<b>DOD Authentication</b>	<p>Enables <b>PAP</b> or <b>CHAP</b> authentication for dial-in &amp; dial-on-demand. <b>PAP</b> 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 DOD CHAP Handshake fields authenticate the user.</p>
<b>DOD CHAP Handshake</b>	<p>For <b>DOD Authentication</b>, enter the host/username for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.</p>
<b>Enable NAT</b>	<p>Select to enable Network Address Translation (NAT) for dial-in and dial-out PPP connections on a per modem (device port or PC Card) basis. Users dialing into the SLB branch office manager access the network connected to Eth1 and/or Eth2.</p> <p><b>Note:</b> IP forwarding must be enabled on the <i>Network - Settings</i> page for NAT to work. See <a href="#">6: Basic Parameters</a>.</p>
<b>Dial-out Number</b>	<p>Phone number for dialing out to a remote system or serial device. May have up to 20 characters. Any format is acceptable.</p>
<b>Dial-out Login</b>	<p>User ID for dialing out to a remote system. May have up to 32 characters.</p>
<b>Dial-out Password and Retype</b>	<p>Password for dialing out to a remote system. May have up to 64 characters.</p>

<b>Restart Delay</b>	The number of seconds after the timeout and before the SLB branch office manager attempts another connection. The default is <b>30</b> seconds.
----------------------	---

2. To save settings for just this port, click the **Apply** button.
3. To save selected settings to ports other than the one you are configuring:
  - a) From the **Apply Settings** drop-down box, select **none**, a group of settings, or **All**.
  - b) 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.

Port Status and Counters	
DSR/CD	No
DTR	Yes
CTS	No
RTS	Yes
Bytes input	0
Bytes output	0
Framing errors	0
Parity errors	0
Overrun errors	0
Flow Control errors	0
Seconds since zeroed	84127

## Device Ports – SLP Power Manager

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 Ports – Settings page, select an SLP or SLPEXP.
2. Click the **Device Commands** link. The following page displays:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'Devices' tab is selected, and the 'Device Ports' sub-tab is active. The main content area is titled 'Device Ports - SLP'. It displays the following information:

- Port: 3
- Name: Port-3
- Device: SLP8
- SLP Login: [Text Input Field]
- SLP Password: [Text Input Field]
- Retype Password: [Text Input Field]
- SLP Status Info**
  - Outlet Status:  Tower A  Tower B
  - All Outlets
  - Single Outlet: [Text Input Field]
- Environmental Status** (Link)
- Infeed Status** (Link)
- System Info** (Link)
- SLP Commands**
  - Restart SLP:
  - Control Outlet: [Dropdown Menu: No Action]
  - Tower A  Tower B
  - All Outlets
  - Single Outlet: [Text Input Field]

At the bottom, there is a 'Back to Device Port Settings' link and an 'Apply' button.

**To enter SLP commands:**

1. Enter the following:

<b>SLP Login</b>	User ID for logging into the SLP power manager.
<b>SLP Password/Retype Password</b>	Password for logging into the SLP power manager.

**SLP Status/Info**

<b>Outlet Status</b>	<p><b>Note:</b> If there is an SLP power manager and an SLP Expansion chassis, the SLP power manager is Tower A and the Expansion chassis is Tower B.</p> <p>For Tower A or Tower B, select <b>All Outlets</b> or <b>Single Outlet</b> to view the status of all outlets or a single outlet of the SLP power manager. If you select <b>Single Outlet</b>, enter a value of 1-8 for the SLP8 power manager or 1-16 for the SLP16 power manager.</p> <p>Click the <b>Outlet Status</b> link to see the status of the selected outlet(s).</p>
<b>Environmental Status</b>	Click the link to view the environmental status (e.g., temperature and humidity) of the SLP power manager.

<b>Infeed Status</b>	Click the link to view the status of the data the SLP power manager is receiving.
<b>System Info</b>	Click the link to see system information pertaining to the SLP device.

### SLP Commands

<b>Restart SLP</b>	To restart the SLP power manager, select the checkbox.
<b>Control Outlet</b>	For Tower A or Tower B, select <b>All Outlets</b> or <b>Single Outlet</b> and the number of the outlet to be controlled (1-8 for the SLP8 power manager or 1-16 for the SLP16 power manager) and select the command for the outlet (No Action, Power On, Power Off, Cycle Power). <b>No Action</b> is the default.

- Click the **Apply** button.

### Device Port – Sensorsoft Device

Devices made by Sensorsoft are used to monitor environmental conditions.

- In the **Connected to** field above the IP Settings section of the Device Ports – Settings page, select **Sensorsoft**.
- Click the **Device Commands** link. The following page displays:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there is a status bar with indicators for E1, E2, S1-S8, P1-P4, and A, B. Below this is a navigation menu with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The main content area is titled "Device Ports - Sensorsoft" and contains a table of Sensorsoft Devices. The table has columns for Device Port, Device Port Name, Temp (°C), Low Temp, High Temp, Humidity (%), Low Humidity, High Humidity, and Traps. The table shows one device with Device Port 3, Device Port Name Port-3, Temp (°C) 0.0, Low Temp 0, High Temp 25, Humidity (%) 0.0, Low Humidity 0, High Humidity 100, and Traps checked. There is an "Apply" button at the bottom right of the table.

- Select a port and enter or view the following information:

<b>Device Port</b> (view only)	Number of the SLB port.
<b>Device Name</b> (view only)	Name of the SLB port.
<b>Temp (°C)</b>	Current temperature (degrees Celsius) on the device the sensor is monitoring.
<b>Low Temp</b>	Enter the temperature (degrees Celsius) permitted on the monitored device below which the SLB branch office manager sends a trap.
<b>High Temp</b>	Enter the temperature (degrees Celsius) permitted on the monitored device above which the SLB device sends a trap.

<b>Humidity (%)</b>	Current relative humidity on the device the sensor is monitoring.
<b>Low Humidity</b>	Enter the relative humidity permitted on the device the sensor is monitoring below which the sensor sends a trap to the SLB branch office manager.
<b>High Humidity</b>	Enter the highest relative acceptable humidity permitted on the device above which the sensor sends a trap to the SLB device.
<b>Traps</b>	Select to indicate the SLB branch office manager should send a trap or configured Event Alert when the sensor detects an out-of-range configured threshold.

- Click the **Apply** button.
- To view the status detected by the Sensorsoft, click the **Sensorsoft Status** link to the right of the table.

## Device Port Commands

The following CLI commands correspond to the web page entries described above.

### To configure a single port or a group of ports:

**Example:** `set deviceport port 2-5,6,12,15-16 baud 2400`

```
set deviceport port <Device Port List or Name> <one or more
device port parameters>
```

#### Parameters:

```
auth <pap|chap>
banner <Banner Text>
baud <300-115200>
breakseq <1-10 Chars>
calleridcmd <Modem Command String>
calleridlogging <enable|disable>
chaphost <CHAP Host or User Name>
chapsecret <CHAP Secret or User Password>
The user defines the secret.
checkdsr <enable|disable>
closedsr <enable|disable>
databits <7|8>
device <none|slp8|slp16>
dialinlist <Host List for Dial-in>
dialoutnumber <Phone Number>
dialoutlogin <User Login>
```

---

```

dialoutpassword <Password>
dialbacknumber <username|Phone Number>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
dodchapsecret <CHAP Secret or User Password>
flowcontrol <none|xon/xoff|rts/cts>
idletimeout <disable|1-9999 seconds>
ipaddr <IP Address>
initscript <Initialization Script>
A script that initializes a modem.
localipaddr <negotiate|IP Address>
logins <enable|disable>
modemmode <text|ppp>
modemstate
<disable|dialout|dialin|dialback|dialondemand|
dialin+dialondemand|dialinhostlist>
modemtimeout <disable|1-9999 seconds>
name <Device Port Name>
nat <enable|disable>
parity <none|odd|even>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
showlines <enable|disable>
sshauth <enable|disable>
sshin <enable|disable>
sshport <TCP Port>
stopbits <1|2>
tcpauth <enable|disable>
tcpin <enable|disable>
tcpport <TCP Port>
telnetauth <enable|disable>
telnetin <enable|disable>
telnetport <TCP Port>
timeoutlogins <disable or 1-30>
webcolumns <Web SSH/Telnet Cols>
webrows <Web SSH/Telnet Rows>

```

---

**To view the settings for one or more device ports:**

```
show deviceport port <Device Port List or Name>
```

**To view a list of all device port names:**

```
show deviceport names
```

**To view the modes and states of one or more device port(s):**

*You can optionally email the displayed information.*

```
show portstatus [deviceport <Device Port List or Name>] [email
<Email Address>]
```

**To view device port statistics and errors for one or more ports:**

*You can optionally email the displayed information.*

```
show portcounters [deviceport <Device Port List or Name>]
[email <Email Address>]
```

**To zero the port counters for one or more device ports:**

```
show portcounters zerocounters <Device Port List or Name>
```

## Device Commands

The following CLI commands correspond to the web page entries described above.

**To send 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 and Sensorsoft devices.*

```
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 power manager uses to restart itself.*

```
slp outletcontrol state <on|off|cyclepower>
[outlet <Outlet #>][tower <A|B>]
```

*Outlet # is 1-8 for SLP8 power manager and 1-16 for SLP16 power manager.*

*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 power manager.*

`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 lowest 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.*

---

## 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:

`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:**

```
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>
```

---

**Notes:**

- ◆ *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.*
- ◆ 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 PC Card) 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 Device Ports – Logging web 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

### PC Card Logging

Data can be logged to a PC Card Compact Flash that is loaded into one of the PC Card slots on the front of the SLB branch office manager and properly mounted (see [PC Card Logging](#) on page 99). Data logged locally to the SLB device is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a PC Card Compact Flash 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 [7: Services](#)). 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 – Logging page to set logging parameters on individual ports.

## Sylog 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 [7: Services](#).)

### To set logging parameters:

1. In the top section of the Device Ports – Settings page, click the **Settings** link in the **Logging** field. The following page displays:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. Below that, a sub-navigation bar includes Device Status, Device Ports, Console Port, PC Card, Power Outlets, Connections, and Host Lists. The main content area is titled "Device Ports - Logging" and is for "Port 3".

**Local Logging:**  Clear Local Log:  [View Local Log >](#)

**Email Traps:**  Send:  Email  SNMP Trap  Both Trigger on:  Byte Count  Text String Recognition

Byte Threshold:  Email Delay:  seconds Restart Delay:  seconds Text String:  Email To:  Email Subject:

**NFS File Logging:**  Directory to Log to:  Max Number of Files:  Max Size of Files:  bytes

**PC Card Logging:**  Log to:  Upper Slot  Lower Slot Max Number of Files:  Max Size of Files:  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.

[Back to Device Port Settings](#)   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.

2. Enter the following:

### Local Logging

<b>Local Logging</b>	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.
<b>Clear Local Log</b>	Select the checkbox to clear the local log.
<b>View Local Log</b>	Click this link to see the local log in text format.

## Email/SNMP Traps

<b>Email/Traps</b>	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 <a href="#">7: Services</a> ) when alert criteria are met. Disabled by default.
<b>Send</b>	If you enabled email and SNMP logging, select what type of notification log to send: <b>Email</b> , <b>SNMP</b> , or <b>Both</b> . <b>Email</b> is the default.
<b>Trigger on</b>	Select the method of triggering a notification:  <b>Byte Count:</b> A specific number of bytes of data. This is the default.  <b>Text String Recognition:</b> A specific pattern of characters, which you can define by a regular expression.  <i>Note: Text string recognition may negatively impact the SLB device's performance, particularly when regular expressions are used.</i>
<b>Byte Threshold</b>	The number of bytes of data the port receives before the SLB branch office manager captures log data and sends a notification regarding this port. The default is <b>100</b> bytes.  In most cases, the console port of your device does not send any data unless there is an alarm condition. After the SLB device receives a small number of bytes, it perceives that your device needs some attention. The SLB branch office manager 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 device receives 30 bytes of data, it captures log data and sends an email regarding this port.
<b>Email Delay</b>	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 <b>60</b> seconds.
<b>Restart Delay</b>	The number of seconds for the period <i>after</i> 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 <b>60</b> seconds.

<b>Text String</b>	<p>The specific pattern of characters the SLB branch office manager 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.</p> <p>The SLB device supports GNU regular expressions; for more information, see:</p> <p><a href="http://www.codeforge.com/help/GNURegularExpr.html">http://www.codeforge.com/help/GNURegularExpr.html</a></p> <p><a href="http://www.delorie.com/gnu/docs/regex/regex.html">http://www.delorie.com/gnu/docs/regex/regex.html</a></p>
<b>Email to</b>	<p>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 <b>single space</b>. You can enter up to 128 characters.</p>
<b>Email Subject</b>	<p>A subject text appropriate for your site. May have up to 128 characters.</p> <p>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).</p> <p><b>Note:</b> The character sequence <b>%d</b> anywhere in the email subject is replaced with the device port number automatically.</p>

### NFS File Logging

<b>NFS File Logging</b>	<p>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.</p>
<b>Directory to Log to</b>	<p>The path of the directory where the log files will be stored.</p> <p><b>Note:</b> <i>This directory must be a directory exported from an NFS server mounted on the SLB branch office manager. Specify the local directory path for the NFS mount.</i></p>
<b>Max Number of Files</b>	<p>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 <b>10</b>.</p>
<b>Max Size of Files</b>	<p>The maximum allowable file size in bytes. The default is <b>2048</b> bytes. Once the maximum size of a file is reached, the SLB device begins generating a new file.</p>

## PC Card Logging

<b>PC Card Logging</b>	Select to enable PC Card logging. A PC Card Compact Flash must be loaded into one of the PC Card slots on the front of the SLB branch office manager and properly mounted ((see <a href="#">PC Card Logging</a> on page 99). Disabled by default.
<b>Log To</b>	If port logging is to a PC Card, select the slot ( <b>Upper</b> or <b>Lower</b> ) in which the PC Card has been inserted. <b>Upper</b> is the default.
<b>Max Number of Files</b>	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 <b>10</b> .
<b>Max Size of Files</b>	The maximum allowable file size in bytes. The default is 2048 bytes. Once the maximum size of a file is reached, the SLB device begins generating a new file. The default is <b>2048</b> bytes.

## Syslog Logging

<b>Syslog Logging</b>	Select to enable system logging.  <i>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 page.</i>
-----------------------	--

**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)

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

## Logging Commands

The following CLI commands correspond to the web page entries described above.

### To configure logging settings for one or more device ports:

**Example:** `set deviceport port 2-5,6,12,15-16 baud 2400 locallogging enable`

**Note:** 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 [11: User Authentication](#)).

```
set deviceport port <Device Port List or Name> <one or more
deviceport parameters>
```

Parameters:

```
emaildelay <Email Delay>
```

```
emaillogging <disable|bytecnt|charstr>
```

---

```

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>
pccardlogging <enable|disable>
pccardmaxfiles <Max # of Files>
pccardmaxsize <Size in Bytes>
pccardslot <upper|lower>
sysloglogging <enable|disable>

```

---

**To view a specific number of bytes of data for a device port:**

```
show locallog <Device Port # or Name> [bytes <Bytes To Display>]
```

*1 Kbyte is the default.*

---

**To clear the local log for a device port:**

```
set locallog clear <Device Port # or Name>
```

---

**Note:** 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 [11: User Authentication](#)).

---

## Console Port

The console port initially has the same defaults as the device ports. Use the 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:



LANTRONIX<sup>®</sup> SLB884

Logout User: sysadmin

Select port for  configuration or  WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port PC Card Power Outlets Connections Host Lists

### Console Port Help?

Baud: 9600

Data Bits: 8

Stop Bits: 1

Parity: none

Flow Control: none

Timeout:  No  Yes, minutes (1-30):

Show Lines On Connecting:

Apply

2. Change the following as desired:

<b>Baud</b>	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 <b>9600</b> for the administration port, so the console port defaults to this value.
<b>Data Bits</b>	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is <b>8</b> data bits.
<b>Stop Bits</b>	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 <b>1</b> .
<b>Parity</b>	Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is <b>none</b> .
<b>Flow Control</b>	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 <b>none</b> .
<b>Timeout</b>	The number of minutes (1-30) after which an idle session on the console is automatically logged out. Disabled by default.
<b>Show Lines on Connecting</b>	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.

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

## Console Port Commands

The following CLI commands correspond to the web page entries described above.

**To configure console port settings:**

```
set consoleport <one or more parameters>
```

*Parameters:*

```
baud <300-115200>
databits <7|8>
stopbits <1|2>
parity <none|odd|even>
flowcontrol <none|xon/xoff|rts/cts>
showlines <enable|disable>
timeout <disable|1-30>
```

---

**To view console port settings:**

```
show consoleport
```

---

## Power Outlets

The SLB branch office manager has four outlets that can provide power to other units in an IT environment. Each outlet can be configured and controlled through the SLB device. The SLB can issue an SNMP trap if the total current for all four 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:** The four red buttons (P1-P4) at the top of any page display the Device Ports – Power Outlets page.

LANTRONIX® SLB884

User: sysadmin

Select port for  configuration or  WebSSH (Device Port only)

Logout

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port PC Card Power Outlets Connections Host Lists

### Power Outlets

Switching Delay:  msec

Over Current Alarm:  Off  On, Threshold (1-180):  Tenths of Amps

Current Level for all Outlets: 2.8 Amps

Outlet	Status	Name	Description	Power State	Wakeup Mode	Reboot
P1	On	PowerOutlet-1	Power Outlet 1	<input checked="" type="radio"/> On <input type="radio"/> Off	<input type="radio"/> On <input checked="" type="radio"/> Off <input type="radio"/> Last State	<input type="checkbox"/>
P2	On	PowerOutlet-2	Power Outlet 2	<input checked="" type="radio"/> On <input type="radio"/> Off	<input type="radio"/> On <input checked="" type="radio"/> Off <input type="radio"/> Last State	<input type="checkbox"/>
P3	On	PowerOutlet-3	Power Outlet 3	<input checked="" type="radio"/> On <input type="radio"/> Off	<input type="radio"/> On <input checked="" type="radio"/> Off <input type="radio"/> Last State	<input type="checkbox"/>
P4	On	PowerOutlet-4	Power Outlet 4	<input checked="" type="radio"/> On <input type="radio"/> Off	<input type="radio"/> On <input checked="" type="radio"/> Off <input type="radio"/> Last State	<input type="checkbox"/>

Apply

2. Enter the following:

<b>Switching Delay</b>	Number of milliseconds the SLB branch office manager between subsequent switching. The range is 1000-2500 msec. The default is <b>2000 msec</b> (2 sec).
<b>Over Current Alarm</b>	If SNMP traps are enabled (see <a href="#">7:Services</a> ), 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 device sends a trap. The maximum is 180. <b>Note:</b> If the alarm goes off, a warning message displays on the CLI.
<b>Current Level for all Outlets</b>	Displays the total load carried by the outlets.

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

<b>Outlet</b>	Displays the number of the outlet being configured.
<b>Status</b>	Displays the current state of the outlet.
<b>Name</b>	User-configurable name identifying the outlet.
<b>Description (optional)</b>	User-configurable text describing the outlet.
<b>Power State</b>	Select whether the power should be on or off. Default is Off.
<b>Wakeup Mode</b>	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.
<b>Last State</b>	Select whether to return the outlet to the state it was in before the reboot.
<b>Reboot</b>	To power cycle the outlet, select the checkbox. Default is unchecked. <i>Note:</i> You can reboot the SLB branch office manager on the <a href="#">Maintenance</a> page, but after the reboot, the power outlet has the same power state as it did before the reboot.

---

- To save, click **Apply**.

## Power Outlet Commands

The following CLI commands correspond to the web page entries described above.

---

### To configure and control power outlets:

```
set power switchingdelay <Delay in msec>
set power alarmthreshold <disable|Tenths of Amps>
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
```

**Example:** set power outlet 1-2,4 state on

---

### To view power outlet settings:

```
show power [outlet <Outlet # or Name>]
```

*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.

---

## 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 add a host list:

- Click the **Devices** tab and select the **Host Lists** option. The following page displays:

2. Enter the following:

**Note:** To clear fields in the lower part of the page, click the **Clear Host List** button.

<b>Host List Id</b> (view only)	Displays after a host list is saved.
<b>Host List Name</b>	Enter a name for the host list.
<b>Retry Count</b>	Enter the number of times the SLB branch office manager should attempt to retry connecting to the host list.
<b>Authentication</b>	Select to require authentication when the SLB device connects to a host.

3. You have the following options:

- ◆ To save the host list without adding hosts at this time, click the **Add Host List** button.
- ◆ To add hosts, enter the following:

#### Host Parameters

<b>Host</b>	Name or IP address of the host.
<b>Protocol</b>	Protocol for connecting to the host (TCP, SSH, or Telnet).
<b>Port</b>	Port on the host to connect to.

---

<b>Escape Sequence</b>	The escape character used to get the attention of the SSH or Telnet client. It is optional, and if not specified, Telnet and SSH use their default escape character.  For Telnet, the escape character is either a single character or a two-character sequence consisting of '^' followed by one character. If the second character is '?', the DEL character is selected. Otherwise, the second character is converted to a control character and used as the escape character.  For SSH, the escape character is a single character.
------------------------	---

---

4. Click the **right arrow**. The host displays in the **Hosts** box.
5. Repeat steps 2-4 to add more hosts to the host list.  
*Note:* To clear fields before adding the next host, click the **Clear Host Parameters** button.
6. You have the following options:
  - ◆ 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**.
7. Click the **Add Host List** button. After the process completes, a link back to the Device Ports – Settings page displays.

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

1. In the **Host Lists** table, select the host list and click the **View Host List** button. The list of hosts display in the **Hosts** box.

2. View, add, or update the following:

<b>Host List Id</b> (view only)	Displays after a host list is saved.
<b>Host List Name</b>	Enter a name for the host list.
<b>Retry Count</b>	Enter the number of times the SLB branch office manager should attempt to retry connecting to the host list.
<b>Authentication</b>	Select to require authentication when the SLB device connects to a host.

**Host Parameters**

<b>Host</b>	Name or IP address of the host.
<b>Protocol</b>	Protocol for connecting to the host (TCP, SSH, or Telnet).
<b>Port</b>	Port on the host to connect to SLB branch office manager.

<b>Escape Sequence</b>	<p>The escape character used to get the attention of the SSH or Telnet client. It is optional, and if not specified, Telnet and SSH use their default escape character.</p> <p>For Telnet, the escape character is either a single character or a two-character sequence consisting of '^' followed by one character. If the second character is '?', the DEL character is selected. Otherwise, the second character is converted to a control character and used as the escape character.</p> <p>For SSH, the escape character is a single character.</p>
------------------------	--

3. You have the following options:
  - ◆ To add a host to the host list, click the **right arrow**. The host displays in the **Hosts** box.
  - ◆ 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**.
4. Click the **Edit Host List** button. After the process completes, a link back to the Device Ports – Settings page displays.

#### To delete a host list:

1. Select the host list in the **Host Lists** table.
2. Click the **Delete Host List** button. After the process completes, a link back to the Device Ports – Settings page displays.

## Host List Commands

The following CLI commands correspond to the web page entries described above.

#### To configure a prioritized list of hosts to be used for modem dial-in connections:

```
set hostlist add|edit <Host List Name> [<parameters>]
```

##### Parameters:

```
name <Host List Name> (edit only)
```

```
retrycount <1-10>
```

Default is 3.

```
auth <enable|disable>
```



**To add a new host entry to a list or edit an existing entry:**

```
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>
```

**To move a host entry to a new position in the host list:**

```
set hostlist edit <Host List Name> move <Host Number>
position <Host Number>
```

**To delete a host list, or a single host entry from a host list:**

```
set hostlist delete <Host List> [entry <Host Number>]
```

**To display the members of a host list:**

```
show hostlist <all|names|Host List Name>
```

---

## 9: PC Cards

You can use the PC Card page to configure storage (Compact Flash) and modem/ISDN PC cards. A Compact Flash is useful for saving and restoring configurations (see [Configuration Management on page 182](#)) and for Device Port Logging (see [PC Card Logging on page 99](#)). The SLB branch office manager supports a variety of Compact Flash-to-PC Card adapters, as well as modem and Basic Rate Interface (BRI) ISDN cards. (See the Lantronix web site for a complete list.)

### To set up PC Card storage in the SLB device:

1. Insert any of the supported PC Cards into either of the PC Card bays on the front of the SLB branch office manager. (You can do this before or after powering up the SLB device.)

If the card is a compact Flash-to-PC Card adapter, and the first partition on the Compact Flash is formatted with a file system supported by the SLB branch office manager (ext2 and FAT), the card mounts automatically.

2. If the card does not mount automatically, or if you want to update its settings, click the **Devices** tab and select the **PC Card** option. The following page displays.

The screenshot shows the Lantronix SLB884 web interface. At the top, there is a status bar with various indicators (E1, E2, 1-8, S, P1-P4, A, B). Below this is a navigation menu with tabs for Network, Services, User Authentication, Devices (selected), Maintenance, and Quick Setup. Under the Devices tab, there are sub-tabs for Device Status, Device Ports, Console Port, PC Card (selected), Power Outlets, Connections, and Host Lists. The main content area is titled 'PC Card' and contains a table with the following data:

Slot	Device	Type	State	
Upper	modem	"HAYES CORPORATION", "HAYES ACCURA V90 PC CARD"	inserted	<input type="radio"/>
Lower	storage	"SanDisk", "SDP", "5/3 0.6"	ext2, mounted	<input type="radio"/>

To the right of the table, there is a 'Configure' button and a note: 'If a PC Card has been inserted, but is not visible in the table, please refresh the web page. To configure the settings for a PC Card, select the radio button in the right column.'

3. From the PC Card Slots table, select the button (on the right) for the PC Card you want to configure for storage and click the **Configure** button. The following page displays.

The image shows two screenshots of the LANTRONIX web interface for SLB884 and SLC16 devices. Both screenshots display the 'PC Card - Storage' configuration page. The user is logged in as 'sysadmin'. The interface includes a navigation menu with options like Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'PC Card' section shows the following settings:

- Slot: Lower
- Device: Storage
- Type: "SanDisk", "SDP", "5/3 0.6"
- State: ext2, mounted
- Mount:
- Unmount:
- Format:
- Filesystem:  Ext2  FAT

An 'Apply' button is visible at the bottom of each configuration page.

4. Enter the following settings for the selected PC Card:

## Storage Settings

<b>Mount</b>	Select the checkbox to mount the first partition of the Compact Flash on the SLB device (if not currently mounted). Once mounted, a Compact Flash is used for device port logging and saving/restoring configurations.
<b>Unmount</b>	To eject the Compact Flash from the SLB branch office manager, <b>first</b> unmount the Compact Flash. Select the checkbox to unmount it.  <b>Warning:</b> <i>If you eject a Compact Flash from the SLB device without unmounting it, subsequent mounts of a PC Card Compact Flash in either slot may fail, and you will need to reboot the SLB branch office manager to restore PC Card functionality.</i>
<b>Format</b>	Select to unmount the Compact Flash (if it is mounted), remove all existing partitions, create one partition on the Compact Flash, format it with the selected file system (ext2 or FAT), and mount it.

<b>Filesystem</b>	Select ext2 or <b>FAT</b> , the file systems the SLB device supports.
-------------------	---

5. Click the **Apply** button.

**To enter modem settings for a PC Card:**

1. Insert any of the supported modem or ISDN cards (see [www.lantronix.com/slb](http://www.lantronix.com/slb)) into either of the PC Card bays on the front of the SLB branch office manager. (You can do this before or after powering up the SLB device.)
2. Click the **Devices** tab and select the **PC Card** option. The PC Card page displays.
3. Select the PC Card you want to configure from the PC Card Slots table and click the **Configure** button. The PC Card – Modem/ISDN page displays.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. Below this is a sub-navigation bar with links for Device Status, Device Ports, Console Port, PC Card, Power Outlets, Connections, and Host Lists. The main content area is titled "PC Card - Modem/ISDN" and contains several configuration sections:

- General Settings:** Slot: Upper, State: Disabled, Mode: Text, Device: Modem/ISDN, Type: "HAYES CORPORATION", "HAYES ACCURA V90 PC CARD", State: N/A.
- Data Settings:** Baud: 9600, Data Bits: 8, Parity: none, Stop Bits: 1, Flow Control: xon/xoff.
- ISDN Settings:** Channel: 1, Phone #: [Redacted].
- GSM/GPRS Settings:** Dial-out Mode: GPRS, PIN: [Redacted], Retype PIN: [Redacted], GPRS Context: AT+CGDCONT=1,"IP",[Accel], PPP Compression: [unchecked], GSM Bearer Svc: AT+CBST=7,0, Auto-acquire DNS: [checked], Negotiated IP: N/A.
- Text Mode:** Initialization Script: [Redacted], Modem Timeout: No, Caller ID Logging: [unchecked], Modem Command: [Redacted].
- PPP Mode:** Negotiate IP Address: Yes, Authentication: PAP, CHAP Handshake: [Redacted], DOD Authentication: PAP, DOD CHAP Handshake: [Redacted].
- IP Settings:** Service: None, Telnet Port: 2049, SSH Port: 3049, TCP Port: 4049.

An "Apply" button is located at the bottom of the configuration area.

4. Enter or view the following:

<b>State</b>	Select to indicate whether to disable the PC Card or set it for dial-in, dial-out, dial-back, dial-on-demand, or dial-in & dial-on-demand. Disabled by default.
--------------	---

<b>Mode</b>	<p>The format in which the data flows back and forth.</p> <p>With <b>Text</b> selected, the SLB branch office manager assumes that the modem will be used for remotely logging into the command line. Text mode is only for dialing in. This is the default.</p> <p><b>PPP</b> establishes an IP-based link over the modem. PPP connections can be used in dial-out mode (e.g., the SLB device connects to an external network) or dial-in mode (e.g., the external computer connects to the network that the SLB branch office manager is part of) or dial-on-demand. For ISDN cards, only PPP connections are allowed.</p>
<b>Initialization Script</b>	<p>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 device uses a default initialization string of <b>AT S7=45 SO=0 L1 V1 X4 &amp;D2 &amp;c1 E1 Q0</b>.</p> <p><i>Note:</i> We recommend that the modem initialization script always be preceded with <b>AT</b> and include <b>E1 V1 x4 Q0</b> so that the SLB branch office manager may properly control the modem.</p>
<b>Modem Timeout</b>	<p>Timeout for modem connections. Select <b>Yes</b> 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.</p>
<b>Caller ID Logging</b>	<p>Select to enable the SLB device to log caller IDs on incoming calls.</p> <p><i>Note:</i> For the Caller ID <b>AT</b> command, refer to the modem user guide.</p>
<b>Modem Command</b>	<p>Modem <b>AT</b> command used to initiate caller ID logging by the modem.</p> <p><i>Note:</i> For the <b>AT</b> command, refer to the modem user guide.</p>

## Data Settings

<b>Baud</b>	<p>The speed with which the device port exchanges data with the attached serial device.</p> <p>From the drop-down list, select the baud rate. Most devices use <b>9600</b> for the administration port, so this is the default. Check the equipment settings and documentation for the proper baud rate.</p>
<b>Data Bits</b>	<p>Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is <b>8</b> data bits.</p>

<b>Parity</b>	Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is <b>none</b> .
<b>Stop Bits</b>	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 <b>1</b> .
<b>Flow Control</b>	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 <b>none</b> .

## ISDN Settings

**Note:** These fields are disabled if the PC Card inserted is not an ISDN card.

<b>Channel</b>	Select to indicate which B channel on the ISDN card to use. Valid values are 1 and 2. (The B-channel is the channel that carries the main data.) Only one 64K channel can be used at a time.
<b>Phone Number</b>	Phone number associated with the B channel. May have up to 20 characters. Any format is acceptable.

## GSM/GPRS Settings

These settings are only active when a GSM/GPRS PC card modem is in the appropriate slot.

### Notes:

- ◆ Please consult your wireless carrier's configuration requirements for more detailed information.
- ◆ 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 branch office manager. Click the **Static Routes** link (above **Data Settings**) to configure a static route. (See [Routing](#) on page 58.)

<b>Dial-out Mode</b>	Select the type of dial-out connection: <b>GPRS:</b> (General Packet Radio Service) <b>GSM:</b> (Global System for Mobile communication)
<b>PIN and Retype PIN</b>	PIN (personal identification number) for accessing the GSM/GPRS card.
<b>GPRS Context</b>	Command to specify the protocol data packet (PDP) context parameter values.
<b>PPP Compression</b>	Select to enable negotiation of data compression over PPP links. Disabled by default.
<b>GSM Bearer Svc.</b>	Command to select the bearer service, data rate, and connection element to use when data call originate.
<b>Auto-acquire DNS</b>	Select to enable the SLB device to acquire up to three DNS servers by means of GPRS. Enabled by default.

<b>Negotiated IP</b>	IP address associated with the GPRS connection.
----------------------	---

## Text Mode

<b>Timeout Logins</b>	If you selected <b>Text</b> mode, you can enable logins to time out after the connection is inactive for a specified number of minutes. The default is <b>No</b> . This setting only applies to text mode connections. <b>PPP</b> mode connections stay connected until either side drops the connection. Disabled by default.
<b>Dial-back Number</b>	Users with dial-back access can dial into the SLB branch office manager and enter their login and password. Once the SLB device 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 <b>Fixed Number</b> , enter the number (in the format 2123456789).
<b>Dial-in Host List</b>	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. The hosts in the list are cycled through until the modem successfully connects to one.  To establish and configure host lists, click the <b>Host Lists</b> link. (See <a href="#">Host Lists</a> on page 108.)

## PPP Mode

<b>Negotiate IP Address</b>	If the SLB branch office manager and/or the serial device have dynamic IP addresses (e.g., IP addresses assigned by a DHCP server), select <b>Yes</b> . This is the default.  If the SLB device or the modem have fixed IP addresses, select <b>No</b> , and enter the <b>Local IP</b> (IP address of the port) and <b>Remote IP</b> (IP address of the modem).
<b>Authentication</b>	Enables <b>PAP</b> or <b>CHAP</b> authentication for modem logins. <b>PAP</b> 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 <b>CHAP Handshake</b> fields authenticate the user.
<b>CHAP Handshake</b>	The host/username (for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.
<b>Same authentication for Dial-in &amp; Dial-on-Demand (DOD)</b>	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 <b>DOD Authentication</b> is PAP, then the <b>DOD CHAP Handshake</b> field is not used.



<b>DOD Authentication</b>	Enables <b>PAP</b> or <b>CHAP</b> authentication for dial-in & dial-on-demand. <b>PAP</b> 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 <b>DOD CHAP Handshake</b> fields authenticate the user.
<b>DOD CHAP Handshake</b>	For <b>DOD Authentication</b> , enter the host/username for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.
<b>Enable NAT</b>	Select to enable Network Address Translation (NAT) for dial-in and dial-out PPP connections on a per modem (Device Port or PC Card) basis. Users dialing into the SLB branch office manager access the network connected to Eth1 and/or Eth2.  <i>Note: IP forwarding must be enabled on the Network - Settings page for NAT to work. To enable, click the <b>IP Forwarding</b> link to display the Network Settings page. See</i>
<b>Dial-out Number</b>	Phone number for dialing out to a remote system or serial device. May have up to 20 characters. Any format is acceptable.
<b>Dial-out Login</b>	User ID for dialing out to a remote system. May have up to 32 characters.
<b>Dial-out Password and Retype</b>	Password for dialing out to a remote system. May have up to 64 characters.
<b>Restart Delay</b>	The number of seconds after the timeout and before the SLB branch office manager attempts another connection. The default is <b>30</b> seconds.

## IP Settings

<b>Service</b>	The available connection services for this modem port (Telnet, SSH, or TCP). Only one can be active at a time. The default is <b>None</b> .
<b>Telnet Port</b>	Telnet session port number to use if you selected <b>Telnet</b> . Defaults: Upper PC Card Slot: <b>2049</b> Lower PC Card Slot: <b>2050</b> Range: <b>1025-65535</b>
<b>SSH Port</b>	The SSH session port number to use if you selected <b>SSH</b> . Defaults: Upper PC Card Slot: <b>3049</b> Lower PC Card Slot: <b>3050</b> Range: <b>1025-65535</b>

<b>TCP Port</b>	The TCP (raw) session port number to use if you selected <b>TCP</b> . Defaults: Upper PC Card Slot: <b>4049</b> Lower PC Card Slot: <b>4050</b> Range: <b>1025-65535</b>
<b>Authenticate</b>	If selected, the SLB branch office manager requires user authentication before granting access to the port. <b>Authenticate</b> is selected by default for <b>Telnet Port</b> and <b>SSH Port</b> , but not for <b>TCP Port</b> .

5. Click the **Apply** button.

## PC Card Commands

These commands for the command line interface correspond to the web page entries described above.

### PC Card Storage Commands

**To mount a Compact Flash card in the SLB branch office manager for use as a storage device:**

*Note:* The Compact Flash card must be formatted with an ext2 or FAT file system before you mount it.

```
pccard storage mount <upper|lower>
```

**To view a directory listing of a Compact Flash card:**

```
pccard storage dir <upper|lower>
```

**To unmount a Compact Flash card:**

*Note:* Enter this command before ejecting the card.

```
pccard storage unmount <upper|lower>
```

**To format a Compact Flash card:**

```
pccard storage format <upper|lower> [filesystem <ext2|fat>]
```

**To rename a file on a Compact Flash card:**

```
pccard storage rename <upper|lower> file <Filename> newfile <New  
Filename>
```

**To copy a file on a Compact Flash card:**

```
pccard storage copy <upper|lower> file <Filename> newfile <New  
Filename>
```

**Removes a file on a Compact Flash card:**

```
pccard storage delete <upper|lower> file <Current Filename>
```

**PC Card Modem Commands****To configure a currently loaded PC Card modem:**

```
pccard modem <upper|lower> <parameters>
```

*Parameters:*

```
auth <pap|chap>
baud <300-115200> 9600 is the default.
calleridcmd <Modem Command String>
calleridlogging <enable| disable>
chaphost <CHAP Host or User Password>
chapsecret <CHAP Secret or User Password>
databits <7|8>
dialbacknumber <username|Phone Number>
dialinlist <Host List for Dial-in>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
dodchapsecret <CHAP Secret or User Password>
dialoutlogin <User Login>
dialoutnumber <Phone Number>
dialoutpassword <Password>
flowcontrol <none|xon/xoff|rts|cts>
gsmautodns <enable|disable>
gsmbearerservice <GSM Bearer Service>
gsmcompression <enable|disable>
gsmcontext <GPRS Context Id>
gsmdialoutmode <gprs|gsm>
gsmppin <GSM/GPRS PIN Number>
idletimeout <disable|1-9999 seconds>
initscript <Initialization Script>
isdnchannel <1|2>
isdnumber <Phone Number>
localipaddr <negotiate|IP Address>
```

---

```
modemmode <text|ppp>
modemstate
<disable|dialout|dialin|dialback|dialondemand|
dialin+dialondemand|dialinhostlist>
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>
```

---

## 10: Connections

*Chapter 8: Device Ports* described how to configure and interact with an SLB branch office manager device port connected to an external device. This chapter describes how to use the Connections web 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:

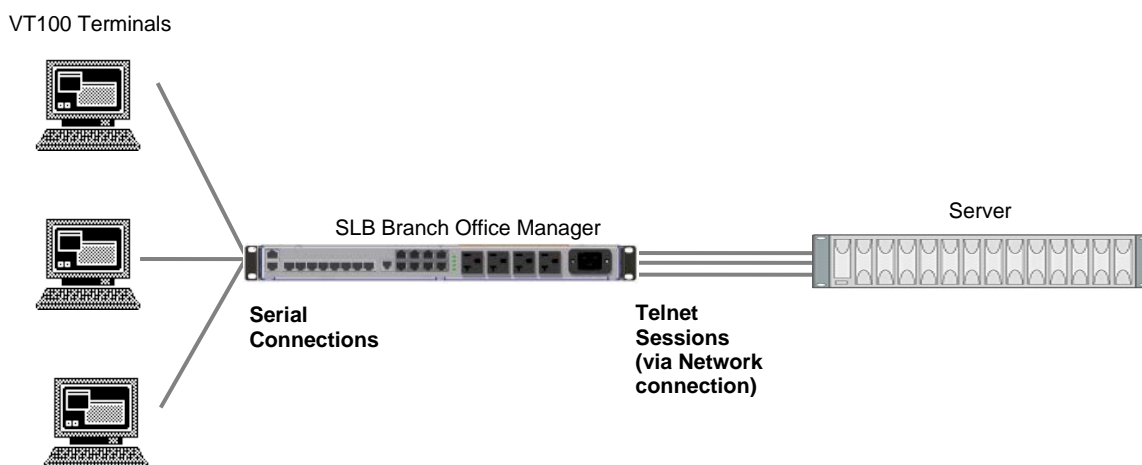
- ◆ Immediately. These connections are always re-established after reboot.
- ◆ At a specified date and time. These connections connect if the date and time have already passed.
- ◆ After a specified amount of data or a specified sequence of data passes through the connection. Following reboot, the connection is not reestablished until the specified data passes through the connection.

## Typical Setup Scenarios for the SLB Device

Following are typical configurations in which SLB connections can be used, with references to settings on the Connections and Device Ports web pages.

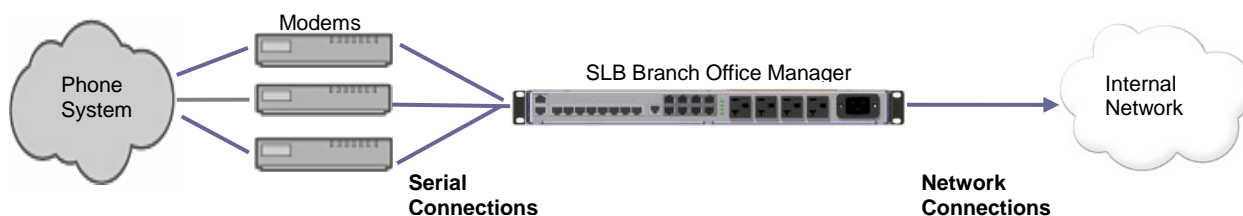
### Terminal Server

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 device and configured as a **Device Port to Telnet out** type connection on the 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.



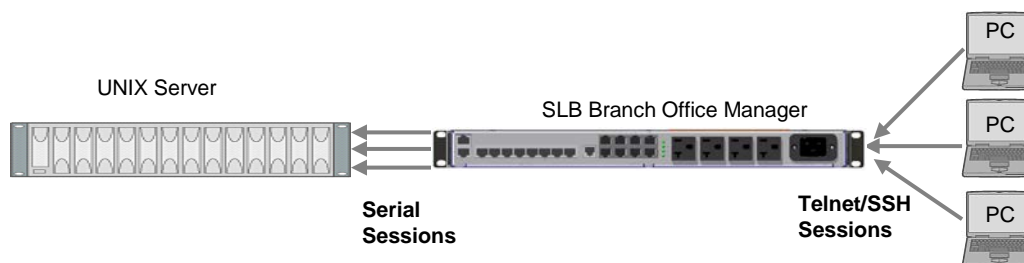
### Remote Access Server

In this setup, the SLB branch office manager 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 device and either Telnet or SSH into the SLB branch office manager. They could also select text mode where, using a terminal emulation program, a user could dial into the SLB device and connect to the command line interface.



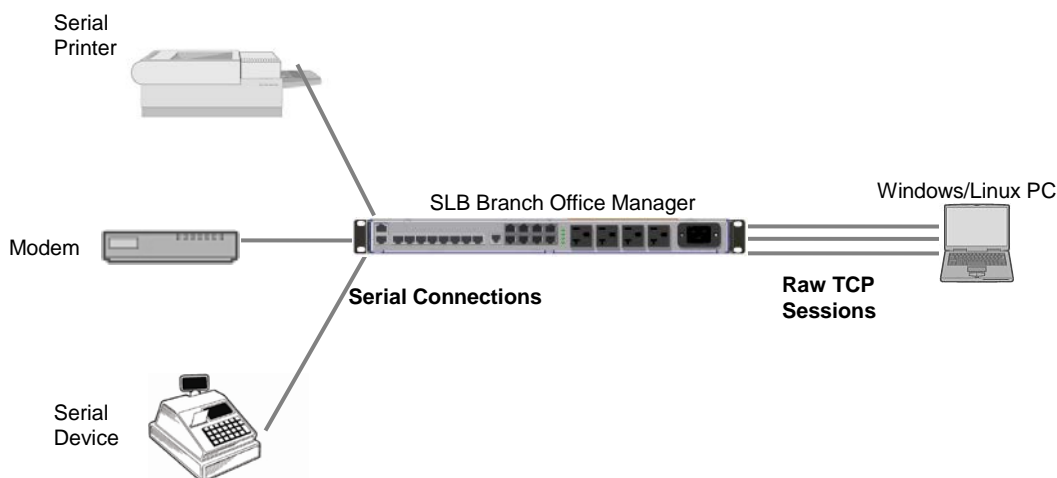
## Reverse Terminal Server

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 device. To configure the SLB branch office manager, select the **Enable Telnet In** or **Enable SSH In** option on the Device Ports – Settings web page.



## Multiport Device Server

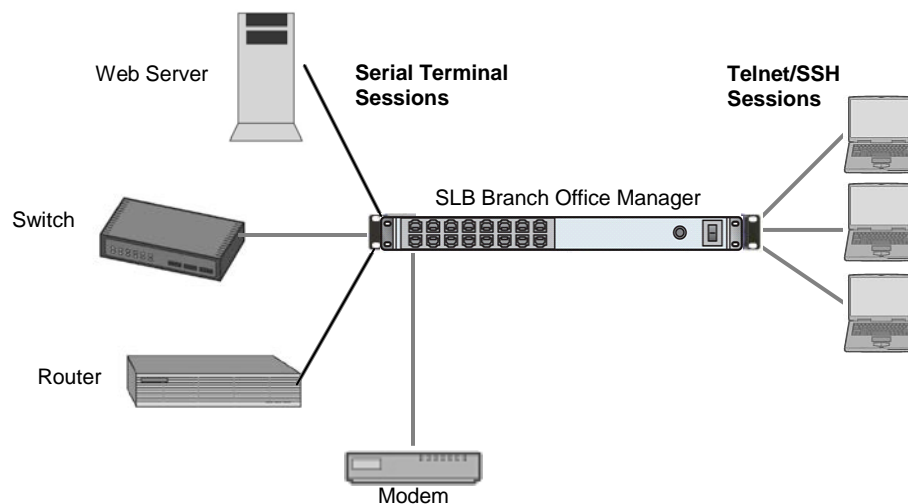
A PC can use the device ports on the SLB device as virtual serial ports, enabling the ports to act as if they are local ports to the PC. To use the SLB branch office manager in this setup, the PC requires special software, for example, Com Port Redirector (available on [www.lantronix.com](http://www.lantronix.com)) or similar software).



## Console Server

For this situation, the SLB branch office manager 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 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 device 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 web 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 web page. A user could then dial into the SLB branch office manager 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:

LANTRONIX<sup>®</sup> SLB884

Logout User: sysadmin Select port for  configuration or  WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port PC Card Power Outlets Connections Host Lists

### Connections Help ?

Outgoing Connection Timeout:  No  Yes:  seconds

Connect: Device Port Port:  [Settings >](#)

Data Flow:

to:  Hostname:  Port:  [Settings >](#)

SSH Out Options User:  Version:  None  1  2 Command:

Trigger:  Connect now  Connect at date/time: April 24, 2008 04:48 pm  Auto-connect on characters transferring:  at least  characters  character sequence:

To view details for a connection, hold the mouse over the arrow icon in the Flow column. To terminate a connection, select the radio button in the right column below and select 'Terminate'. Web connections can be viewed [here >](#)

Port/Service	Flow	Port/Service	User	Time	
Console Port		Command Line	N/A	146:51:03	<input type="radio"/>

2. For a device port, enter the following:

<b>Port</b>	<p>The number of the device port you are connecting.</p> <p>This device port must be connected to an external serial device and must <i>not</i> have command line interface logins enabled, be connected to a modem, or be running a loopback test.</p> <p><b>Note:</b> To see the current settings for this device port, click the <b>Settings</b> link.</p>
<b>Data Flow</b>	Select the arrow showing the direction (bidirectional or unidirectional) the data will flow in relationship to the device port you are connecting.

<b>to</b>	<p>From the drop-down list, select a destination for the connection: a device port connected to a serial device, a device port connected to a modem, or an outbound network connection (Telnet, SSH, TCP Port, or UDP Port).</p> <p><b>Note:</b> To see the current settings for a selected device port, click the <b>Settings</b> link.</p>
<b>Hostname</b>	<p>The host name or IP Address of the destination. This entry is required if the <b>to</b> field is set to Telnet out, SSH out, TCP port, or UDP port.</p>
<b>Port</b>	<p>If the <b>to</b> field is set to <b>Device Port</b> or <b>Modem on Device Port</b>, enter the number of the device port. For all other options, this is the TCP/UDP port number, which is optional for Telnet out and SSH out, but required for TCP Port and UDP Port.</p> <p><b>Notes:</b></p> <p><i>If you select <b>Device Port</b>, it must not have command line interface logins enabled or be running a loopback test.</i></p> <p><i>To view the device port's settings, click the <b>Settings</b> link to the right of the port number.</i></p>
<b>SSH Out Options</b>	<p>Select one of the following optional flags to use for the SSH connection.</p> <p><b>User:</b> Login ID to use for authenticating on the remote host.</p> <p><b>Version:</b> Version of SSH. Select <b>1</b> or <b>2</b>.</p> <p><b>Command:</b> Enter a specific command on the remote host (for example, <code>reboot</code>).</p>
<b>Trigger</b>	<p>Select the condition that will trigger a connection. Options include:</p> <p><b>Connect now:</b> Connects immediately, or if you reboot the SLB branch office manager, immediately on reboot.</p> <p><b>Connect at date/time:</b> Connects at a specified date and time. Use the drop-down lists to complete the date and time. Upon rebooting, the SLB device reestablishes the connection if the date/time has passed.</p> <p><b>Auto-connect on characters transferring:</b> Select the arrow indicating the direction of the data transfer and either the minimum number of characters or a specific character sequence that will trigger the connection.</p> <p>You can select the direction of the data transfer only if <b>Data Flow</b> is bidirectional. Upon rebooting, the SLB branch office manager does not reestablish the connection until the specified data has passed through one of the endpoints of the connection.</p>

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

**To view, update, or disconnect a current connection:**

The bottom of the Connections web page displays current connections.

To view details for a connection, hold the mouse over the arrow icon in the Flow column.  
To terminate a connection, select the radio button in the right column below and select 'Terminate'.  
Web connections can be viewed [here](#).

Current Connections					Terminate
Port/Service	Flow	Port/Service	User	Time	
Console Port	↔	Command Line	N/A	0:12:19	<input type="radio"/>
SSH In 172.18.100.26	↔	Command Line	sysadmin	0:04:21	<input type="radio"/>

- To view details about a connection, hold the mouse over the arrow in the **Flow** column.
- To disconnect (delete) a connection, select the connection in the **Select** column and click the **Terminate** button.
- To reestablish the connection, create the connection again in the top part of the page.
- To view information about Web connections, click the **here** link in the text above the table. The Firmware & Configurations - Web Sessions page displays.

**Connection Commands**

These commands for configuring connections correspond to the web page entries described above.

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

```
connect direct <endpoint>
```

*Endpoint is one of:*

```
deviceport <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>]
hostlist <Host List>
```

**To configure initial timeout for outgoing connections:**

**Note:** This is not a TCP timeout.

```
connect global outgoingtimeout <disable|1-9999 seconds>
```

**To monitor a device port:**

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

**To connect a device port to another device port or an outbound network connection (data flows in both directions):**

```
connect bidirection <Port # or Name> <endpoint>
```

*Endpoint is one of:*

```
charcount <# of Chars>
charseq <Char Sequence>
charxfer <toendpoint|fromendpoint>
deviceport <Device Port # or Name>
date <MMDDYYhhmm[ss]>
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>
udp <IP Address> [port <UDP Port>]
```

**Note:** 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.

**To connect a device port to another device port or an outbound network connection (data flows in one direction):**

```
connect unidirection <Device Port # or Name> dataflow
<toendpoint|fromendpoint> <endpoint>
```

*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>
```

```
udp <IP Address> [port <UDP Port>]
```

**Note:** 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.

---

#### To terminate a bidirectional or unidirectional connection:

```
connect terminate <Connection ID>
```

---

#### To view connections and their IDs:

**Note:** 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 [email <Email Address>].
```

You can optionally email the displayed information.

---

#### To display details for a single connection:

You can optionally email the displayed information.

```
show connections connid <Connection ID> [email <Email Address>
```

---

#### To display global connections:

```
connect global show
```

---

## 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 device will use the methods. By default, local user authentication is enabled and is the first method the SLB branch office manager 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.*

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:**

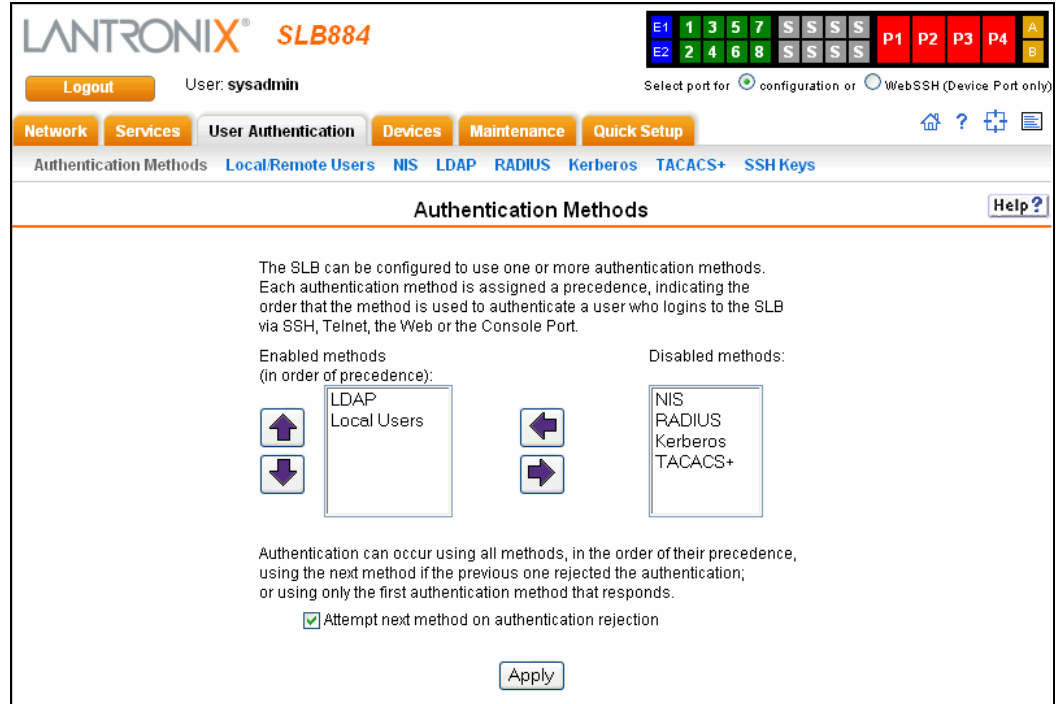
There is an LDAP user "joe" and an NIS user "joe" and the order of authentication methods is:

- 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 device 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:



- 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:

<b>NIS (Network Information System)</b>	<p>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.</p> <p>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).</p>
<b>LDAP (Lightweight Directory Access Protocol)</b>	<p>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.</p>
<b>RADIUS (Remote Authentication Dial-In User Service)</b>	<p>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.</p> <p>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.</p>
<b>Kerberos</b>	<p>Kerberos is a network authentication protocol that enables two parties to exchange private information across an unprotected network.</p> <p>It works by assigning a unique electronic credential, called a <i>ticket</i>, to each user who logs on to the network. The ticket is embedded in messages to identify the sender.</p>

<b>TACACS+ (Terminal Access Controller Access Control System)</b>	TACACS+ allows a remote access server to communicate with an authentication server to determine whether the user has access to the network. TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS. The SLB branch office manager supports TACACS+ only.
<b>Local Users</b>	Local accounts authenticate users who attempt to log in via SSH, Telnet, the Web, or the console port.

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 device 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 branch office manager 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

The following command for the command line interface corresponds to the web page entries described above.

### To set ordering of authentication methods:

**Note:** Local Users authentication is always the first method used. Any methods omitted from the command will be disabled.

```
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>
```

### To view authentication methods and their order of precedence:

```
show auth
```



## Local and Remote Users

The system administrator can configure the SLB device 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.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a navigation bar with tabs for Network, Services, User Authentication (selected), Devices, Maintenance, and Quick Setup. Under User Authentication, there's a sub-menu with options: Authentication Methods, Local/Remote Users (selected), NIS, LDAP, RADIUS, Kerberos, TACACS+, and SSH Keys. The main content area is titled "Local/Remote Users" and includes a "Help" link.

Configuration options include:

- Enable Local Users:
- Authenticate only remote users who are in the remote users list:
- Local User Passwords:
  - Complex Passwords:
  - Allow Reuse:
  - Reuse History:
  - Password Lifetime:  days
  - Warning Period:  No  Yes:  days
  - Max Login Attempts:  No  Yes:
  - Lockout Period:  No  Yes:  minutes
- Buttons: Add/Edit User, Delete User

At the bottom, there's a table titled "Local/Remote Users" with the following data:

Login	Auth	UID	Group	Permissions	Esc Seq	Brk Seq	Custom Menu	DB	Listen	Data	Clear	Outlet
michaell	Remote	N/A	Adm	fa,nt,sv,lu,ra,dt,sk,um,dp,pc,rs,fc,dr,sn,wb,po	\x1bA	\x1bB		N	1-8,U,L	1-8,U,L	1-8,U,L	1-4
sysadmin	Local	0	Adm	fa,nt,sv,lu,ra,dt,sk,um,dp,pc,rs,fc,dr,sn,wb,po	\x1bA	\x1bB		N	1-8,U,L	1-8,U,L	1-8,U,L	1-4

An "Apply" button is located at the bottom center of the page.

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:

1. Enter the following:

<b>Enable Local Users</b>	Select to enable all local users except sysadmin. The sysadmin is always available regardless of how you set the check box. Enabled by default.
<b>Authenticate only users who are in the remote users list</b>	Select the check box to authenticate users listed in the <b>Remote Users</b> list in the lower part of the page. Disabled by default.

2. Click the **Apply** button.

### To set password requirements for local users:

## Local User Passwords

<b>Complex Passwords</b>	Select to enable the SLB branch office manager to enforce rules concerning the password structure (e.g., alphanumeric requirements, number of characters, punctuation marks). Disabled by default. <b>Complexity rules:</b> 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 (()\~!@#\$\$%%^&*~+=\{}[];:'"<>.,?/_).
<b>Allow Reuse</b>	Select to enable users to continue to reuse old passwords. If you disable the check box, they cannot use any of the <b>Reuse History</b> number of passwords. Enabled by default.
<b>Reuse History</b>	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.
<b>Password Lifetime (days)</b>	The number of days until the password expires. The default setting is <b>90</b> .
<b>Warning Period (days)</b>	The number of days ahead that the system warns that the user's password will expire. The default setting is <b>7</b> .
<b>Max Login Attempts</b>	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 <b>0</b> (disabled).
<b>Lockout Period (minutes)</b>	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 <b>0</b> (disabled).

- Click the **Apply** button.

### To add, edit, or delete a user:

You can delete a user listed in the table on this page or open the page for adding or editing a user.

You have the following options:

- ◆ To add a user, click the **Add/Edit User** button. The Local/Remote User Settings page displays. (See [Local/Remote User Settings](#) below)
- ◆ To edit a user, select the user in the table and click the **Add/Edit User** button. The Local/Remote User Settings page displays.
- ◆ To delete a user, select the user in the table, click the **Delete** button, and then click the **Apply** button.

## Local/Remote User Settings

On this page, you can add, edit, or delete a local or remote user.

### To add a user:

- On the Local/Remote Users page (described above), click the **Add/Edit User** button. The Local/Remote User Settings page displays.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a status bar with E1-E2, 1-8, S, P1-P4, and A/B indicators. Below that, a navigation menu includes Network, Services, User Authentication (selected), Devices, Maintenance, and Quick Setup. The main content area is titled 'Local/Remote User Settings' and contains several input fields and checkboxes for configuring a user. The 'Authentication' section is set to 'Local'. A note on the right states: 'Each user is a member of a group which has predefined user rights associated with it. User rights that are associated with a group cannot be modified for individual users.'

2. Enter the following information for the user:

<b>Login</b>	User ID of selected user.
<b>Authentication</b>	Select the type of authenticated user: <b>Local:</b> User listed in the SLB database. <b>Remote:</b> User not listed in the SLB database.
<b>UID</b>	A unique numeric identifier the system administrator assigns to each user. Valid UIDs are 101-4294967295. <b>Note:</b> The UID must be unique. If it is not, SLB branch office manager automatically increments it. Starting at 101, the SLB finds the next unused UID.
<b>Listen Ports</b>	The device ports that the user may access to view data using the <code>connect listen</code> command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15). <b>U</b> and <b>L</b> denote the PC Card upper and lower slots.
<b>Data Ports</b>	The device ports with which the user may interact using the <code>connect direct</code> command. Enter the port numbers or the range of port numbers.
<b>Clear Port Buffers</b>	The device port buffers the users may clear using the <code>set locallog clear</code> command. Enter the port numbers or the range of port numbers.

<b>Access Outlets</b>	The outlets the user may monitor and configure.
<b>Enable for Dial-back</b>	Select to grant a local user dial-back access (see page 84). Users with dial-back access can dial into the SLB branch office manager and enter their login and password. Once the SLB device authenticates them, the modem hangs up and dials them back. Disabled by default.
<b>Dial-back Number</b>	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).
<b>Escape Sequence</b>	<p>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.)</p> <p>A suggested value is <b>Esc+A</b> (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as <b>\x1bA</b>, which is hexadecimal (<b>\x</b>) character 27 (<b>1B</b>) followed by an <b>A</b>.</p> <p>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 <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p>
<b>Break Sequence</b>	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 <b>Esc+B</b> (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as <b>\x1bB</b> , which is hexadecimal ( <b>\x</b> ) character 27 ( <b>1B</b> ) followed by a <b>B</b> .
<b>Custom Menu</b>	<p>If custom menus have been created, you can assign a default custom menu to the user. The custom menu will display at login.</p> <p><i>Note: In the Local Users table, if the menu assigned to a local user no longer exists, it is marked with an asterisk (*).</i></p>
<b>Display Menu at Login</b>	If custom menus have been created, select to enable the menu to display when the user logs into the CLI.
<b>Password/ Retype Password</b>	When a user logs into the SLB branch office manager, the SLB device prompts for a password (up to 64 characters). The sysadmin establishes that password here.
<b>Password Expires</b>	If not selected, allows the user to keep a password indefinitely. If selected the user keeps the password for a set period. (See <a href="#">Local and Remote Users</a> on page 137 for information on specifying the length of time before the password expires.)
<b>Allow Password Change</b>	Select to allow the user to change password.
<b>Change Password on Next Login</b>	Indicate whether the user must change the password at the next login.
<b>Lock Account</b>	Select to lock the account indefinitely.

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.

<b>Group</b>	Select the group to which the user will belong: <b>Default Users:</b> This group has only the most basic rights. You can specify additional rights for the individual user . <b>Power Users:</b> This group has the same rights as Default Users plus <b>Networking, Date/Time, Reboot &amp; Shutdown,</b> and <b>Diagnostics &amp; Reports.</b> You can specify additional rights for the individual user. <b>Administrators:</b> This group has all possible rights.
<b>Full Administrative</b>	Right to perform any function on the SLB branch office manager.
<b>Networking</b>	Right to enter network and routing settings.
<b>Services</b>	Right to enable and disable system and audit logging, SSH and Telnet logins, SNMP, and SMTP. Includes NFS and CIFS.
<b>Secure Lantronix Network</b>	Right to view and manage secure IT management units (e.g., SLP power managers, Spiders, SLB branch office managers) on the local subnet.
<b>Date/Time</b>	Right to set the date and time.
<b>Local Users</b>	Right to add or delete local users on the system.
<b>Remote Authentication</b>	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
<b>SSH Keys</b>	Right to set SSH keys for authenticating users.
<b>User Menus</b>	Right to create or edit a custom user menu for the CLI.
<b>Web Access</b>	Right to access Web Manager.
<b>Reboot &amp; Shutdown</b>	Right to shutdown or reboot the SLB branch office manager.
<b>Firmware &amp; Configuration</b>	Right to upgrade the firmware on the unit and save or restore a configuration (all settings).
<b>Diagnostics &amp; Reports</b>	Right to obtain diagnostic information and reports about the unit.
<b>Device Ports</b>	Right to enter device port settings. Includes creating bidirectional and unidirection connections
<b>PC Card</b>	Right to enter modem settings for PC cards. Includes managing storage PC Cards.
<b>Power Outlets</b>	Right to view and enter settings for power outlets.

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.
3. Click the **Apply** button.

**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 and click the **Add/Edit User** button. The Local/Remote User Settings page displays.
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.

**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.

3. Click the **Apply** button.

## Local Users Commands

The following CLI commands correspond to the web page entries described above.

---

### To configure local accounts (including sysadmin) who log in to the SLB branch office manager by means of SSH, Telnet, the Web, or the console port:

```
set localusers add|edit <User Login> <parameters>
```

#### Parameters:

```
accessoutlets <Outlet List>
allowdialback <enable|disable>
breakseq <1-10 Chars>
changenextlogin <enable|disable>
changepassword <enable|disable>
clearports <Port List>
custommenu <Menu Name>
dataports <Port List>
dialbacknumber <Phone Number>
displaymenu <enable|disable>
escapeseq <1-10 Chars>
group <default|power|admin|>
listenports <Port List>
passwordexpires <enable|disable>
permissions <Permission List>
uid <User Identifier>
```

---

### To set whether a complex login password is required:

```
set localusers complexpasswords <enable|disable>
```

---

### To enable or disable authentication of local users:

```
set localusers state <enable|disable>
```

---

### To set a login password for the local user:

```
set localusers password <User Login>
```

---

### To delete a local user:

```
set localusers delete <User Login>
```

---

**To view settings for all users or a local user:**

```
show localusers [user <User Login>]
```

---

**To block (lock out) a user's ability to log in:**

```
set localusers lock <User Login>
```

**Note:** This capability is not available on the web page.

---

**To allow (unlock) a user's ability to log in:**

```
set localusers unlock <User Login>
```

**Note:** This capability is not available on the web page.

---

## Local User Rights Commands

The following CLI commands correspond to the web page entries described above.

---

**To add a local user to a user group or to change the group the user belongs to:**

```
set localusers add|edit <user> group <default|power|admin>
```

---

**To set a local user's permissions (not defined by the user group):**

```
set localusers add|edit <user> permissions <Permission List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

---

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

```
show user
```

---

## Remote User Commands

The following CLI commands correspond to the web page entries described above.

---

**To configure whether remote users who are not part of the remote user list will be authenticated:**

```
set remoteusers listonlyauth <enable|disable>
```

---



**To configure attributes for users who log in by a remote authentication method:**

```
set remoteusers add|edit <User Login> [<parameters>]
```

**Parameters**

```
accessoutlets <Outlet List>
```

```
breakseq <1-10 Chars>
```

```
clearports <Port List>
```

```
dataports <Port List>
```

```
escapeseq <1-10 Chars>
```

```
group <default|power|admin>
```

```
listenports <Port List>
```

```
permissions <Permissions List>
```

**where**

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

---

**To remove a remote user:**

```
set remoteusers delete <User Login>
```

---

**To view settings for all remote users:**

```
show remoteusers
```

---

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

```
show user
```

---

## NIS

The system administrator can configure the SLB branch office manager to use NIS to authenticate users attempting to log in to the SLB device 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 branch office manager to use NIS to authenticate users:**

1. Click the **User Authentication** tab and select the **NIS** option.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a status bar with various indicators (E1-E2, S, P1-P4, A, B). Below that, a navigation menu includes 'Network', 'Services', 'User Authentication', 'Devices', 'Maintenance', and 'Quick Setup'. The 'User Authentication' section is active, showing 'Authentication Methods' with options like 'Local/Remote Users', 'NIS', 'LDAP', 'RADIUS', 'Kerberos', 'TACACS+', and 'SSH Keys'. The 'NIS' configuration page is displayed, featuring a 'Help?' button. The NIS configuration includes:
 

- Enable NIS:
- NIS Domain:
- Note: The NIS Domain must match the NIS domain name on the NIS Server.
- Broadcast for NIS Server:
- NIS Master Server:
- NIS Slave Server #1:
- NIS Slave Server #2:
- NIS Slave Server #3:
- NIS Slave Server #4:
- NIS Slave Server #5:
- Custom Menu:
- Escape Sequence:
- Break Sequence:
- Data Ports:
- Listen Ports:
- Clear Port Buffers:
- Access Outlets:

 Below the NIS configuration is the 'User Rights' section. It includes a 'Group' selection with radio buttons for 'Default Users' (selected), 'Power Users', and 'Administrators'. There are also checkboxes for various rights: Full Administrative, Networking, Services, SecureLinux Network, Date/Time, Local Users, Remote Authentication, SSH Keys, User Menu, Web Access, Reboot & Shutdown, Firmware & Configuration, Diagnostics & Reports, Device Ports, PC Card, and Power Outlets. An 'Apply' button is located at the bottom of the form.

2. Enter the following:

<b>Enable NIS</b>	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.  <i>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.</i>
<b>NIS Domain</b>	The NIS domain of the SLB branch office manager must be the same as the NIS domain of the NIS server.
<b>Broadcast for NIS Server</b>	If selected, the SLB device sends a broadcast datagram to find the NIS Server on the local network.
<b>NIS Master Server (required)</b>	The IP address or host name of the master server.
<b>NIS Slave Servers #1 -5</b>	The IP addresses or host names of up to five slave servers.

<b>Custom Menu</b>	If custom menus have been created you can assign a default custom menu to NIS users.
<b>Escape Sequence</b>	<p>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.)</p> <p>A suggested value is <b>Esc+A</b> (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as <code>\x1bA</code>, which is hexadecimal (<b>x</b>) character 27 (<b>1B</b>) followed by an <b>A</b>.</p> <p>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 <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p>
<b>Break Sequence</b>	<p>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 <b>Esc+B</b> (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as <code>\x1bB</code>, which is hexadecimal (<b>x</b>) character 27 (<b>1B</b>) followed by a <b>B</b>.</p>
<b>Data Ports</b>	The ports users are able to monitor and interact with using the <code>connect direct</code> command. <b>U</b> and <b>L</b> denote the PC Card upper and lower slots.
<b>Listen Ports</b>	The ports users are able to monitor using the <code>connect listen</code> command.
<b>Clear Port Buffers</b>	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.
<b>Access Outlets</b>	The outlets the user may monitor and configure.

3. In the **User Rights** section, select the user group to which NIS users will belong:

<b>Group</b>	<p>Select the group to which the NIS users will belong:</p> <p><b>Default Users:</b> This group has only the most basic rights. You can specify additional rights for the individual user .</p> <p><b>Power Users:</b> This group has the same rights as Default Users plus <b>Networking</b>, <b>Date/Time</b>, <b>Reboot &amp; Shutdown</b>, and <b>Diagnostics &amp; Reports</b>.</p> <p><b>Administrators:</b> This group has all possible rights.</p>
--------------	--

4. Select or clear the checkboxes for the following rights:

<b>Full Administrative</b>	Right to add, update, and delete all editable fields.
<b>Networking</b>	Right to enter Network settings.
<b>Services</b>	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
<b>Date/Time</b>	Right to set the date and time.

<b>Secure Lantronix Network</b>	Right to view and manage secure IT management units (e.g., SLP power managers, Spiders, SLC console managers, SLB branch office managers) on the local subnet.
<b>Local Users</b>	Right to add or delete local users on the system.
<b>Remote Authentication</b>	Right to assign a remote user to a user group and assign a set of rights to the user.
<b>SSH Keys</b>	Right to set SSH keys for authenticating users.
<b>User Menus</b>	Right to create a custom user menu for the CLI for NIS users.
<b>Reboot &amp; Shutdown</b>	Right to use the CLI or shut down the SLB branch office manager and then reboot it.
<b>Firmware &amp; Configuration</b>	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects <b>Reboot &amp; Shutdown</b> .
<b>Diagnostics &amp; Reports</b>	Right to obtain diagnostic information and reports about the unit.
<b>Web Access</b>	Right to access Web Manager.
<b>Device Ports</b>	Right to enter device port settings.
<b>PC Card</b>	Right to enter modem settings for PC cards.
<b>Power Outlets</b>	Right to configure power outlets.

- Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

## NIS Commands

These commands for the command line interface correspond to the web page entries described above.

**To configure the SLB branch office manager to use NIS to authenticate users who log in via the Web, SSH, Telnet, or the console port:**

```
set nis <one or more parameters>
```

*Parameters:*

```
accessoutlets <Outlet List>
breakseq <1-10 Chars>
broadcast <enable|disable>
clearports <Port List>
dataports <Port List>
domain <NIS Domain Name>
escapeseq <1-10 Chars>
listenports <Port List>
master <IP Address or Hostname>
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>
```

---

**To set group and permissions for NIS users:**

```
set nis group <default|power|admin>
```

---

**To set permissions for NIS users not already defined by the user rights group:**

```
set nis permissions <Permission List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

---

**To set a default custom menu for NIS users:**

```
set nis custommenu <Menu Name>
```

---

**To view NIS settings:**

```
show nis
```

---

## 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 branch office manager to use LDAP to authenticate users:**

1. Click the **User Authentication** tab and select **LDAP**. The following page displays.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a navigation bar with tabs for Network, Services, User Authentication (selected), Devices, Maintenance, and Quick Setup. Below this is a sub-menu for Authentication Methods, with LDAP selected. The main content area is titled 'LDAP' and contains several configuration sections:

- Enable LDAP:** A checked checkbox.
- Server:** Text input field containing '172.18.21.15'.
- Port:** Text input field containing '389'.
- Base:** Text input field containing 'dc=thetmatrix,dc=lantron'. A note below says '(example: dc=domain,dc=com)'.
- Bind Name:** Text input field containing 'cn=admin, cn=Users'.
- Bind Password:** Password input field with masked characters.
- Retype Password:** Password input field with masked characters.
- Active Directory Support:** A checked checkbox.
- Encrypt Messages:** An unchecked checkbox.
- Custom Menu:** A dropdown menu set to '<none>'.
- Escape Sequence:** Text input field containing '\x1bA'.
- Break Sequence:** Text input field containing '\x1bB'.
- Data Ports:** Text input field containing '1-8,U,L'.
- Listen Ports:** Text input field containing '1-8,U,L'.
- Clear Port Buffers:** Text input field containing '1-8,U,L'.
- Access Outlets:** Text input field containing '1-4'.

Below the LDAP configuration is a section titled 'User Rights'. It includes a 'Group' selection with radio buttons for 'Default Users' (selected), 'Power Users', and 'Administrators'. To the right, a note states: 'All LDAP users are members of a group which has predefined user rights associated with it. Additional rights which are not defined by the group can be added.' Below this are various checkboxes for permissions:

- Full Administrative:
- Networking:
- Services:
- SecureLink Network:
- Date/Time:
- Local Users:
- Remote Authentication:
- SSH Keys:
- User Menus:
- Web Access:
- Reboot & Shutdown:
- Firmware & Configuration:
- Diagnostics & Reports:
- Device Ports:
- PC Card:
- Power Outlets:

An 'Apply' button is located at the bottom of the configuration area.

2. Enter the following:

<b>Enable LDAP</b>	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.
<b>Server</b>	The IP address or host name of the LDAP server.
<b>Port</b>	Number of the TCP port on the LDAP server to which the SLB branch office manager talks. The default is <b>389</b> .

<b>Base</b>	The name of the LDAP search base (e.g., dc=company, dc=com). May have up to 80 characters.
<b>Bind Name</b>	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
<b>Bind Password and Retype Password</b>	Password for a non-anonymous bind. This entry is optional. Acceptable characters are <b>a-z</b> , <b>A-Z</b> , and <b>0-9</b> . The maximum length is 127 characters.
<b>Active Directory Support</b>	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. Disabled by default.
<b>Encrypt Messages</b>	Select to encrypt messages between the SLB branch office manager and the LDAP server. Disabled by default.
<b>Custom Menu</b>	If custom menus have been created (see <a href="#">Custom User Menus</a> on page 174), you can assign a default custom menu to LDAP users.
<b>Escape Sequence</b>	<p>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.)</p> <p>A suggested value is <b>Esc+A</b> (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as <b>\x1bA</b>, which is hexadecimal (<b>\x</b>) character 27 (<b>1B</b>) followed by an <b>A</b>.</p> <p>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 <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p>
<b>Break Sequence</b>	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 <b>Esc+B</b> (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as <b>\x1bB</b> , which is hexadecimal ( <b>\x</b> ) character 27 ( <b>1B</b> ) followed by a <b>B</b> .
<b>Data Ports</b>	The ports users are able to monitor and interact with using the <code>connect direct</code> command. <b>U</b> and <b>L</b> denote the PC Card upper and lower slots.
<b>Listen Port</b>	The ports users are able to monitor using the <code>connect listen</code> command.
<b>Clear Port Buffers</b>	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.
<b>Access Outlets</b>	The outlets the user may monitor and configure.

3. In the User Rights section, select the user group to which LDAP users will belong:

<b>Group</b>	<p>Select the group to which the LDAP users will belong:</p> <p><b>Default Users:</b> This group has only the most basic rights. You can specify additional rights for the individual user.</p> <p><b>Power Users:</b> This group has the same rights as Default Users plus <b>Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</b></p> <p><b>Administrators:</b> This group has all possible rights.</p>
--------------	---

4. Select or clear the checkboxes for the following rights:

<b>Full Administrative</b>	Right to add, update, and delete all editable fields.
<b>Networking</b>	Right to enter Network settings.
<b>Services</b>	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
<b>Secure Lantronix Network</b>	Right to view and manage secure IT management units (e.g., SLP power managers, Spiders, SLB branch office managers) on the local subnet.
<b>Date/Time</b>	Right to set the date and time.
<b>Local Users</b>	Right to add or delete local users on the system.
<b>Remote Authentication</b>	Right to assign a remote user to a user group and assign a set of rights to the user.
<b>SSH Keys</b>	Right to set SSH keys for authenticating users.
<b>User Menus</b>	Right to create a custom user menu for the CLI for LDAP users.
<b>Reboot &amp; Shutdown</b>	Right to use the CLI or shut down the SLB branch office manager and then reboot it.
<b>Firmware &amp; Configuration</b>	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects <b>Reboot &amp; Shutdown.</b>
<b>Diagnostics &amp; Reports</b>	Right to obtain diagnostic information and reports about the unit.
<b>Web Access</b>	Right to access Web Manager.
<b>Device Ports</b>	Right to enter device port settings.
<b>PC Card</b>	Right to enter modem settings for PC cards.
<b>Power Outlets</b>	Right to configure power outlets.

5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.



## LDAP Commands

These commands for the command line interface correspond to the web page entries described above.

---

### To configure the SLB branch office manager to use LDAP to authenticate users who log in via the Web, SSH, Telnet, or the console port:

```
set ldap <one or more parameters>
```

#### Parameters:

```
accessoutlets <Outlet List>
adsupport <enable|disable>
Enables or disables active directory.
base <LDAP Base>
bindname <Bind Name>
breakseq <1-10 Chars>
dataports <Ports List>
listenports <Port List>
clearports <Port List>
escapeseq <1-10 Chars>
bindpassword <Bind Password>
encrypt <enable|disable>
port <TCP Port>
Default is 389.
server <IP Address or Hostname>
state <enable|disable>
```

---

### To set user group and permissions for LDAP users:

```
group <default|power|admin>
```

---

### To set permissions for LDAP users not already defined by the user rights group:

```
permissions <Permission List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

---

### To set a default custom menu for LDAP users:

```
custommenu <Menu Name>
```

---

### To view LDAP settings:

```
show ldap
```

---

## RADIUS

The system administrator can configure the SLB branch office manager 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.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The User Authentication tab is selected, and the RADIUS configuration page is displayed. The page includes a 'Logout' button and the user name 'sysadmin'. The RADIUS configuration section has the following fields and options:

- Enable RADIUS:**
- RADIUS Server #1:**
- Server #1 Port:**
- Server #1 Secret:**
- RADIUS Server #2:**
- Server #2 Port:**
- Server #2 Secret:**
- Timeout:**  seconds
- Custom Menu:**
- Escape Sequence:**
- Break Sequence:**
- Data Ports:**
- Listen Ports:**
- Clear Port Buffers:**
- Access Outlets:**

The **User Rights** section includes a group selection (Default Users, Power Users, Administrators) and a grid of checkboxes for various permissions:

- Full Administrative:
- Networking:
- Services:
- SecureLinux Network:
- Date/Time:
- Local Users:
- Remote Authentication:
- SSH Keys:
- User Menus:
- Web Access:
- Reboot & Shutdown:
- Firmware & Configuration:
- Diagnostics & Reports:
- Device Ports:
- PC Card:
- Power Outlets:

An **Apply** button is located at the bottom of the form.

2. Enter the following:

<b>Enable RADIUS</b>	<p>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.</p> <p><b>Note:</b> 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.</p>
<b>RADIUS Server #1</b>	<p>IP address or hostname of the primary RADIUS server. This RADIUS server may be a proxy for SecurID.</p> <p>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).</p>
<b>Server #1 Port</b>	<p>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 (<b>1812</b>).</p>
<b>Server #1 Secret</b>	<p>Text that serves as a shared secret between a RADIUS client and the server (SLB device). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.</p>
<b>RADIUS Server #2</b>	<p>IP address or host name of the secondary RADIUS server. This server can be used as a SecurID proxy.</p>
<b>Server #2 Port</b>	<p>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 (<b>1812</b>).</p>
<b>Server #2 Secret</b>	<p>Text that serves as a shared secret between a RADIUS client and the server (SLB device). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.</p>
<b>Timeout</b>	<p>The number of seconds (1-30) after which the connection attempt times out. The default is <b>30</b> seconds.</p>
<b>Custom Menu</b>	<p>If custom menus have been created, you can assign a default custom menu to RADIUS users.</p>
<b>Escape Sequence</b>	<p>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.)</p> <p>A suggested value is <b>Esc+A</b> (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as <b>\x1bA</b>, which is hexadecimal (<b>\x</b>) character 27 (<b>1B</b>) followed by an <b>A</b>.</p> <p>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 <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p>

<b>Break Sequence</b>	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 <b>Esc+B</b> (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as <code>\x1bB</code> , which is hexadecimal ( <b>x</b> ) character 27 ( <b>1B</b> ) followed by a <b>B</b> .
<b>Data Ports</b>	The ports users are able to monitor and interact with using the <code>connect direct</code> command. <b>U</b> and <b>L</b> denote the PC Card upper and lower slots.
<b>Listen Port</b>	The ports users are able to monitor using the <code>connect listen</code> command.
<b>Clear Port Buffers</b>	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.
<b>Access Outlets</b>	The power outlets users may monitor and configure.

**Note:** Older RADIUS servers may use **1645** as the default port. Check your RADIUS server configuration.

- In the **User Rights** section, select the user group to which RADIUS users will belong.

<b>Group</b>	Select the group to which the RADIUS users will belong: <b>Default Users:</b> This group has only the most basic rights. You can specify additional rights for the individual user. <b>Power Users:</b> This group has the same rights as Default Users plus <b>Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</b> <b>Administrators:</b> This group has all possible rights.
--------------	--

- Select or clear the checkboxes for the following rights:

<b>Full Administrative</b>	Right to add, update, and delete all editable fields.
<b>Networking</b>	Right to enter Network settings.
<b>Services</b>	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
<b>Secure Lantronix Network</b>	Right to view and manage secure IT management units (e.g., SLP power managers, Spiders, SLB branch office managers) on the local subnet.
<b>Date/Time</b>	Right to set the date and time.
<b>Local Users</b>	Right to add or delete local users on the system.
<b>Remote Authentication</b>	Right to assign a remote user to a user group and assign a set of rights to the user.
<b>SSH Keys</b>	Right to set SSH keys for authenticating users.
<b>User Menus</b>	Right to create a custom user menu for the CLI for NIS users.

<b>Reboot &amp; Shutdown</b>	Right to use the CLI or shut down the SLB branch office manager and then reboot it.
<b>Firmware &amp; Configuration</b>	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects <b>Reboot &amp; Shutdown</b> .
<b>Diagnostics &amp; Reports</b>	Right to obtain diagnostic information and reports about the unit.
<b>Web Access</b>	Right to access Web Manager.
<b>Device Ports</b>	Right to enter device port settings.
<b>PC Card</b>	Right to enter modem settings for PC cards.
<b>Power Outlets</b>	Right to configure power outlets.

- Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

## RADIUS Commands

These commands for the command line interface correspond to the web page entries described above.

**To configure 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 <one or more parameters>
```

*Parameters:*

```
accessoutlets <Outlet List>
breakseq <1-10 Chars>
clearports <Port List>
dataports <Port List>
escapeseq <1-10 Chars>
listenports <Port List>
state <enable|disable>
```

**To identify the RADIUS server(s), the text secret, and the number of the TCP port on the RADIUS server:**

```
set radius server <1|2> host <IP Address or Hostname> secret
<Secret> [port <TCP Port>]
```

*The default port is 1812.*

**To set the number of seconds after which the connection attempt times out:**

```
set radius timeout <disable|1-30>
```

*May be 1-30 seconds.*

**To set user group and permissions for RADIUS users:**

```
set radius group <default|power|admin>
```

---

**To set permissions for RADIUS users not already defined by the user rights group:**

```
set radius permissions <Permission List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

---

**To set a default custom menu for RADIUS users:**

```
set radius custommenu <Menu Name>
```

---

**To view RADIUS settings:**

```
show radius
```

---

## 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 branch office manager to use Kerberos to authenticate users:**

1. Click the **User Authentication** tab and select the **Kerberos** option. The following page displays.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a navigation bar with tabs for Network, Services, User Authentication (selected), Devices, Maintenance, and Quick Setup. Below this is a sub-menu with Authentication Methods, Local/Remote Users, NIS, LDAP, RADIUS, Kerberos (selected), TACACS+, and SSH Keys. The main content area is titled 'Kerberos' and contains several configuration sections:

- Enable Kerberos:** A checkbox that is currently unchecked.
- Realm:** An empty text input field.
- KDC:** An empty text input field.
- KDC IP Address:** An empty text input field.
- KDC Port:** A text input field containing '88'.
- Use LDAP:** An unchecked checkbox.
- Custom Menu:** A dropdown menu set to '<none>'.
- Escape Sequence:** A text input field containing '\x1bA'.
- Break Sequence:** A text input field containing '\x1bB'.
- Data Ports:** A text input field containing '1-8,U,L'.
- Listen Ports:** A text input field containing '1-8,U,L'.
- Clear Port Buffers:** A text input field containing '1-8,U,L'.
- Access Outlets:** A text input field containing '1-4'.

Below the Kerberos section is the **User Rights** section, which includes a radio button for 'Default Users' (selected) and two other options: 'Power Users' and 'Administrators'. There are also several checkboxes for permissions:

- Full Administrative:
- Networking:
- Services:
- SecureLinux Network:
- Date/Time:
- Local Users:
- Remote Authentication:
- SSH Keys:
- User Menus:
- Web Access:
- Reboot & Shutdown:
- Firmware & Configuration:
- Diagnostics & Reports:
- Device Ports:
- PC Card:
- Power Outlets:

An 'Apply' button is located at the bottom center of the configuration area.

2. Enter the following:

<p><b>Enable Kerberos</b></p>	<p>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.</p> <p><b>Note:</b> 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.</p>
<p><b>Realm</b></p>	<p>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.</p>
<p><b>KDC</b></p>	<p>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.</p> <p>Enter the <b>KDC</b> in the fully qualified domain format (FQDN). An example is SLB.local.</p>

<b>KDC IP Address</b>	Enter the IP address of the Key Distribution Center (KDC).
<b>KDC Port</b>	Port on the KDC listening for requests. Enter an integer with a maximum value of 65535. The default is <b>88</b> .
<b>Custom Menu</b>	If custom menus have been created, you can assign a default custom menu to RADIUS users.
<b>Escape Sequence</b>	<p>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.)</p> <p>A suggested value is <b>Esc+A</b> (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as <b>\x1bA</b>, which is hexadecimal (<b>x</b>) character 27 (<b>1B</b>) followed by an <b>A</b>.</p> <p>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 <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p>
<b>Break Sequence</b>	<p>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 <b>Esc+B</b> (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as <b>\x1bB</b>, which is hexadecimal (<b>x</b>) character 27 (<b>1B</b>) followed by a <b>B</b>.</p>
<b>Use LDAP</b>	<p>Indicate whether Kerberos should rely on LDAP to look up user IDs and Group IDs. This setting is disabled by default.</p> <p><b>Note:</b> Make sure to configure LDAP if you select this option.</p>
<b>Data Ports</b>	The ports users are able to monitor and interact with using the <code>connect direct</code> command. <b>U</b> and <b>L</b> denote the PC Card upper and lower slots.
<b>Listen Port</b>	The ports users are able to monitor using the <code>connect listen</code> command.
<b>Clear Port Buffers</b>	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.
<b>Access Outlets</b>	The power outlets users may monitor and configure.

3. In the **User Rights** section, select the user group to which Kerberos users will belong.

<b>Group</b>	<p>Select the group to which the Kerberos users will belong:</p> <p><b>Default Users:</b> This group has only the most basic rights. You can specify additional rights for the individual user.</p> <p><b>Power Users:</b> This group has the same rights as Default Users plus <b>Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports</b>.</p> <p><b>Administrators:</b> This group has all possible rights.</p>
--------------	---

4. Select or clear the checkboxes for the following rights:



<b>Full Administrative</b>	Right to add, update, and delete all editable fields.
<b>Networking</b>	Right to enter Network settings.
<b>Services</b>	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
<b>Secure Lantronix Network</b>	Right to view and manage secure IT management units (e.g., SLP power managers, Spiders, SLB branch office managers) on the local subnet.
<b>Date/Time</b>	Right to set the date and time.
<b>Local Users</b>	Right to add or delete local users on the system.
<b>Remote Authentication</b>	Right to assign a remote user to a user group and assign a set of rights to the user.
<b>SSH Keys</b>	Right to set SSH keys for authenticating users.
<b>User Menus</b>	Right to create a custom user menu for the CLI for Kerberos users.
<b>Reboot &amp; Shutdown</b>	Right to use the CLI or shut down the SLB branch office manager and then reboot it.
<b>Firmware &amp; Configuration</b>	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects <b>Reboot &amp; Shutdown</b> .
<b>Diagnostics &amp; Reports</b>	Right to obtain diagnostic information and reports about the unit.
<b>Web Access</b>	Right to access Web Manager.
<b>Device Ports</b>	Right to enter device port settings.

<b>PC Card</b>	Right to enter modem settings for PC cards.
<b>Power Outlets</b>	Right to configure power outlets.

- Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

## Kerberos Commands

These commands for the command line interface correspond to the web page entries described above.

**To configure the SLB branch office manager to use Kerberos to authenticate users who log in via the Web, SSH, Telnet, or the console port:**

```
set kerberos <one or more parameters>
```

*Parameters:*

```
accessoutlets <Outlet List>
breakseq <1-10 Chars>
clearports <Port List>
dataports <Port List>
escapeseq <1-10 Chars>
ipaddr <Key Distribution Center IP Address>
kdc <Key Distribution Center>
listenports <Port List>
port <Key Distribution Center TCP Port>
realm <Kerberos Realm>
state <enable|disable>
useldapforlookup <enable|disable>
```

**To set user group and permissions for Kerberos users:**

```
set kerberos group <default|power|admin>
```

**To set permissions for Kerberos users not already defined by the user rights group:**

```
set kerberos permissions <Permission List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

**To set a default custom menu for Kerberos users:**

```
set kerberos custommenu <Menu Name>
```

**To view Kerberos settings:**

```
show kerberos
```

## 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 device 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 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 branch office manager to use TACACS+ to authenticate users:**

1. Click the **TACACS+** tab and select **TACACS+**. The following page displays.

The screenshot shows the LANTRONIX SLB884 configuration interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'User Authentication' tab is selected, and the 'TACACS+' sub-tab is active. The page title is 'TACACS+' and there is a 'Help?' link.

The main configuration area is divided into two sections: 'TACACS+' and 'User Rights'.

**TACACS+ Section:**

- Enable TACACS+:
- TACACS+ Server #1:
- TACACS+ Server #2:
- TACACS+ Server #3:
- Secret:
- Encrypt Messages:
- Custom Menu:
- Escape Sequence:
- Break Sequence:
- Data Ports:
- Listen Ports:
- Clear Port Buffers:
- Access Outlets:

**User Rights Section:**

- Group:  Default Users,  Power Users,  Administrators
- Full Administrative:
- Networking:
- Services:
- SecureLinux Network:
- Date/Time:
- Local Users:
- Remote Authentication:
- SSH Keys:
- User Menus:
- Web Access:
- Reboot & Shutdown:
- Firmware & Configuration:
- Diagnostics & Reports:
- Device Ports:
- PC Card:
- Power Outlets:

Additional text on the right side of the 'User Rights' section: "All TACACS+ users are members of a group which has predefined user rights associated with it. Additional rights which are not defined by the group can be added."

An 'Apply' button is located at the bottom center of the configuration area.

## 2. Enter the following:

<b>Enable TACACS+</b>	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.
<b>TACACS+ Servers 1-3</b>	IP address or host name of up to three TACACS+ servers.
<b>Secret</b>	Shared secret for message encryption between the SLB branch office manager and the TACACS+ server. Enter an alphanumeric secret of up to 127 characters.
<b>Encrypt Messages</b>	Select the checkbox to encrypt messages between the SLB device and the TACACS+ server. Selected by default.
<b>Custom Menu</b>	If custom menus have been created (see <i>the User Guide</i> ), you can assign a default custom menu to TACACS+ users.
<b>Escape Sequence</b>	<p>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.)</p> <p>A suggested value is <b>Esc+A</b> (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as <b>\x1bA</b>, which is hexadecimal (<b>x</b>) character 27 (<b>1B</b>) followed by an <b>A</b>.</p> <p>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 <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p>
<b>Break Sequence</b>	<p>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 <b>Esc+B</b> (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as <b>\x1bB</b>, which is hexadecimal (<b>x</b>) character 27 (<b>1B</b>) followed by a <b>B</b>.</p>
<b>Data Ports</b>	The ports users are able to monitor and interact with using the <code>connect direct</code> command. <b>U</b> and <b>L</b> denote the upper and lower slots of the PC Card.
<b>Listen Port</b>	The ports users are able to monitor using the <code>connect listen</code> command.
<b>Clear Port Buffers</b>	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.
<b>Access Outlets</b>	The power outlets users may monitor and configure.

3. In the **User Rights** section, select the user group to which TACACS+ users will belong.

<b>Group</b>	<p>Select the group to which the TACACS+ users will belong:</p> <p><b>Default Users:</b> This group has only the most basic rights. You can specify additional rights for the individual user.</p> <p><b>Power Users:</b> This group has the same rights as Default Users plus <b>Networking, Date/Time, Reboot &amp; Shutdown,</b> and <b>Diagnostics &amp; Reports.</b></p> <p><b>Administrators:</b> This group has all possible rights.</p>
--------------	---

4. Select or clear the checkboxes for the following rights:

<b>Full Administrative</b>	Right to add, update, and delete all editable fields.
<b>Networking</b>	Right to enter Network settings.
<b>Services</b>	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
<b>Secure Lantronix Network</b>	Right to view and manage secure IT management units (e.g., SLP power managers, Spiders, SLB branch office managers) on the local subnet.
<b>Date/Time</b>	Right to set the date and time.
<b>Local Users</b>	Right to add or delete local users on the system.
<b>Remote Authentication</b>	Right to assign a remote user to a user group and assign a set of rights to the user.
<b>SSH Keys</b>	Right to set SSH keys for authenticating users.
<b>User Menus</b>	Right to create a custom user menu for the CLI for TACACS+ users.
<b>Reboot &amp; Shutdown</b>	Right to use the CLI or shut down the SLB device and then reboot it.
<b>Firmware &amp; Configuration</b>	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects <b>Reboot &amp; Shutdown.</b>
<b>Diagnostics &amp; Reports</b>	Right to obtain diagnostic information and reports about the unit.
<b>Web Access</b>	Right to access Web Manager.
<b>Device Ports</b>	Right to enter device port settings.
<b>PC Card</b>	Right to enter modem settings for PC cards.
<b>Power Outlets</b>	Right to configure power outlets.

5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

## TACACS+ Commands

These commands for the command line interface correspond to the web page entries described above.

---

### To configure the SLB branch office manager to use TACACS+ to authenticate users who log in via the Web, SSH, Telnet, or the console port:

```
set tacacs+ <one or more parameters>
```

#### Parameters:

```
accessoutlets <Outlet List>
breakseq <1-10 Chars>
clearports <Port List>
dataports <Port List>
encrypt <enable|disable>
escapeseq <1-10 Chars>
listenports <Port List>
secret <TACACS+ Secret>
server1 <IP Address or Name>
server2 <IP Address or Name>
server3 <IP Address or Name>
state <enable|disable>
```

---

### To set user group and permissions for TACACS+ users:

```
set tacacs+ group <default|power|admin>
```

---

### To set permissions for TACACS+ users not already defined by the user rights group:

```
set tacacs+ permissions <Permission List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

---

### To set a default custom menu for TACACS+ users:

```
set tacacs+ custommenu <Menu Name>
```

---

### To view TACACS+ settings:

```
show tacacs+
```

---

## 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 device 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 branch office manager configuration, and the administrator has the option of retaining the SSH keys during a reset to factory defaults.

The SLB device 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 branch office manager, 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 device can generate SSH keys for SSH connections out of the SLB for any SLB user. The SLB branch office manager retains both the private and public key on the SLB device, 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 branch office manager to use SSH keys to authenticate users:**

1. From the main menu, select **User Authentication – SSH Keys**. The following page displays.

**LANTRONIX<sup>®</sup> SLB884**

Logout User: sysadmin Select port for  configuration or  WebSSH (Device Port only)

Network Services **User Authentication** Devices Maintenance Quick Setup

Authentication Methods Local/Remote Users NIS LDAP RADIUS Kerberos TACACS+ SSH Keys

### SSH Keys [Help ?](#)

[SSH Server/Host Keys >](#)

**Imported Keys (SSH In)**

Host & User Associated with Key  
(not required if host and SLB Local User login are declared in imported key file; ignored if file contains multiple keys)

Host:   
User:

Host & Login for Import

Import via:    
Filename:   
Host:   
Path:   
Login:   
Password:   
Retype Password:

User	Host	Type	
sysadmin	slm02-tpham17	RSA, 1024 bits	<input type="radio"/>
michaell	172.18.0.65	DSA, 1024 bits	<input type="radio"/>
sysadmin	slm01_glenn17	RSA, 1024 bits	<input type="radio"/>
sysadmin	slm01_glenn19	RSA, 1024 bits	<input type="radio"/>
sysadmin	slm02_tpham17	RSA, 1024 bits	<input type="radio"/>
sysadmin	slm02_glenn19	RSA, 1024 bits	<input type="radio"/>

**Exported Keys (SSH Out)**

Export:  New Key for User  
 All Previously Created Keys

User:   
Key Name:

Key Type:  RSA  DSA

Number of Bits:    
Passphrase:   
Retype Passphrase:

SECSH Format:

Public Key Filename:

Host & Login for Export

Export via:    
Host:   
Path:   
Login:   
Password:   
Retype Password:

2. Enter the following:

### 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 AAAAB3NzaC1yc2EAAAABIwAAAEEApUHCX9EWsHt+jmUGXa1YC3us
ABYxIXUhSU1N+NU9HNaUADUFfd8LYz8/gUnUSH4Ksm8GRT7/8/Sn9jCVfGPh
UQ== asallaway@winserver
```

<b>Host</b>	Host name or IP address from which the SSH connections to the SLB branch office manager will be made.
<b>User</b>	The User ID of the user being given secure access to the SLB device.

### Host & Login for Import

<b>Import via</b>	Select <b>SCP</b> or <b>FTP</b> as the method for importing the SSH keys. <b>SCP</b> is the default.
<b>Filename</b>	Name of the public key file (for example, mykey.pub). May contain multiple keys.
<b>Host</b>	IP address of the remote server from which to SCP or FTP the public key file.
<b>Path</b>	Optional pathname to the public key file.
<b>Login</b>	User ID to use to SCP or FTP the file.
<b>Password/Retype Password</b>	Password to use to SCP or FTP the file.

### Exported Keys (SSH Out)

<b>Export</b>	Enables you to export created public keys. Select one of the following: <b>New Key for User:</b> Enables you to create a new key for a user and export the public key in a file.. <b>All Previously Created Keys:</b> Does not create any keys, but exports all previously created public keys in one file.
<b>User</b>	User ID of the person given secure access to the remote server.
<b>Key Name</b>	Name of the key. This will generate the public key filename (e.g., <keyname>.pub).
<b>Key Type</b>	Select either the <b>RSA</b> or the <b>DSA</b> encryption standard. <b>RSA</b> is the default.
<b>Number of Bits</b>	Select the number of bits in the key ( <b>512</b> or <b>1024</b> ). The default is <b>512</b> .
<b>Passphrase/Retype Passphrase</b>	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.
<b>SECSH Format</b>	Indicate whether the keys will be exported in <b>SECSH</b> format (by default the key is exported in <b>OpenSSH</b> format).
<b>Public Key Filename</b>	Filename of the public host key.

### Host and Login for Export

<b>Export via</b>	Select the method ( <b>SCP</b> , <b>FTP</b> , or <b>Cut and Paste</b> ) of exporting the key to the remote server. <b>Cut and Paste</b> , the default, requires no other parameters for export.
<b>Host</b>	IP address of the remote server to which the SLB branch office manager will SCP or FTP the public key file.
<b>Path</b>	Optional path of the file on the host to SCP or FTP the public key too.
<b>Login</b>	User ID to use to SCP or FTP the public key file.
<b>Password/Retype Password</b>	Password to use to SCP or FTP the public key file.

#### 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//0tTMEKkb3zrpPu0HHAXaiVXHAvv71Ate31VTpoXdLAXN0uCvuuJLf
aL/LvvGmoEWBubESu5051QHfL70ijxZW0EVTJGFqUQTSq8Ls3/v31kUJEX51n
2A1Qx0F40I5vNEC0+m3d5QE+FKc= sysadmin@DaveSLM
```

3. To delete the key, click the **Delete** button.

#### To view, reset, or import SSH RSA1, RSA, And DSA 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.

**LANTRONIX<sup>®</sup> SLB884**

User: **sysadmin**

Select port for  configuration or  WebSSH (Device Port only)

**Network Services User Authentication Devices Maintenance Quick Setup**

**Authentication Methods Local/Remote Users NIS LDAP RADIUS Kerberos TACACS+ SSH Keys**

**Fingerprint:**  
1024 71:3b:e3:69:5d:5f:83:36:12:06:a7:78:58:5f:64:37 ssh\_host\_key.pub

**Current Host RSA Public Key (Default Key)**

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzj7f6e1FfCKhOSJHcHMo4zrF7rI4mfUJT4BcyIPv6XPx
vFQ0906sVdYY/snmUNLOE81xKWG6OCPEwulIKfhiEx1yxFltXy2hng/AmZVdiwXeuGhKDS1pXg9aDq9/
fD6p3QEcTnhC5x320Gua6dbdIymzp9jqp15YbboY/fyUj9s= root@SLCXXY
```

**Fingerprint:**  
1024 19:44:90:37:be:04:c1:11:f2:1b:47:bb:83:04:8b:84 ssh\_host\_rsa\_key.pub

**Current Host DSA Public Key (Default Key)**

```
ssh-dss AAAAB3NzaC1kc3MAAACBPdQaAseWQDW44cCpESQs1EC47+cjKCUSpNx7VUCHPCNJ/sse28s
ObX8Bfx1/OmNZLQSHK056d/cc4wC+5vpaMn+WniwZ4Eo4AoEBoEYJIB1YXBeU+BM/OZYwY5bK6HBvsez
YCA561y5245RSF3uWV1Nz8mBgoLD6QMGMdMvMgtAAAAFQDiXI/DU1F3wbtYGnEBI5eF81WS3wAAAAIAD
MnF26Cgk72hcT12ov9SiNDhEA/AZ16SR+TLaj8ORCK903R8ewEp7KKUxCQV7Tg4IB8vHgDXIQ6K7T455
vLa5m24tKk8Qnj1FhasZygtMSQyTwY5B4zo6tcXVvrKFIGEWEoz1YOBkZbGLfMgShJYr77tfGAp9zdrR
Za5ThwTE8wAAAAIAJj3hMVIBKNGfzrzeTG8wF6920r9oARUNkwwUj76oi7Lm9A/17pwKwGTFc27AkJ28H
E9FaJWN5qnE/6x/IAxfhKsbILorMCSRH49Onzb/gezvTrRKswiyKQMlrtOnGYzZFXamB3SCYzj0QQSkw
viewZqOtul7wg0QrjCj7xeywRg== root@ (none)
```

**Fingerprint:**  
1024 55:a6:d4:e1:ba:8d:2f:8c:2a:06:12:4d:f7:7f:1d:ef ssh\_host\_dsa\_key.pub

Reset to Default Host Key:  All Keys  RSA1  RSA  DSA

**Note:** changing a host key requires a reboot for the update to take effect.

Import Host Key:

Type: **RSA1** (dropdown)

Import via: **SCP** (dropdown)

Host:

Path:

Login:

Public Key Filename:

Password:

Private Key Filename:

Retype Password:

[Back to SSH Keys](#)

2. View or enter the following:

<b>Reset to Default Host Key</b>	Select the <b>All Keys</b> checkbox to reset all default key(s), or select one or more checkboxes to reset defaults for <b>RSA1</b> , <b>RSA</b> , or <b>DSA</b> keys. All checkboxes are unselected by default.
<b>Import Host Key</b>	To import a site-specific host key, select the checkbox. Unselected by default.
<b>Type</b>	From the drop-down list, select the type of host key to import.
<b>Import via</b>	From the drop-down list, select the method of importing the host key (SCP or SFTP). The default is <b>SCP</b> .

<b>Public Key Filename</b>	Filename of the public host key.
<b>Private Key Filename</b>	Filename of the private host key.
<b>Host</b>	Host name or IPAddress of the host from which to import the key.
<b>Path</b>	Path of the directory where the host key will be stored.
<b>Login</b>	User ID to use to SCP or SFTP the file.
<b>Password &amp; Retype Password</b>	Password to use to SCP or SFTP the file.

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 Commands

These commands for the command line interface correspond to the web page entries described above.

### To import an SSH key:

```
set sshkey import <ftp|scp> <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>
```

**To export a key:**

```
set sshkey export <ftp|scp|coppypaste> <one or more parameters>
```

*Parameters:*

```
[format <openssh|secsh>]
[host <IP Address or Name>]
[login <User Login>]
[path <Path to Copy Key>]
bits <512|1024>
keyname <SSH Key Name>
keyuser <SSH Key User>
type <rsa|dsa>
```

---

**To export the public keys of all previously created SSH keys:**

```
set sshkey all export <ftp|scp|coppypaste> [pubfile <Public Key
File>] [host <IP Address or Name>] [login <User Login>] [path
<Path to Copy Keys>]
```

---

**To delete a key:**

```
set sshkey delete <one or more parameters>
```

*Parameters:*

```
keyhost <SSH Key Host>
keyname <SSH Key Name>
keyuser <SSH Key User>
```

**Note:** Specify the key user and key host to delete an imported key; specify the keyuser and keyname to delete an exported key.

---

**To import an SLB host key or to reset a SLB host key to the default:**

```
set sshkey server import type <rsal|rsa|dsa> via <sftp|scp>
    pubfile <Public Key File> privfile <Private Key File>
    host <IP Address or Name> login <User Login> [path
    <Path to Key File>]
```

---

**To reset defaults for all or selected host keys:**

```
set sshkey server reset [type <all|rsal|rsa|dsa>]
```

---

**To display SSH keys that have been imported:**

```
show sshkey import <one or more parameters>
```

*Parameters:*

```
[keyhost <SSH Key IP Address or Name>]
[keyuser <SSH Key User>]
[viewkey <enable|disable>]
```

---

**To display SSH keys that have been exported:**

```
show sshkey export <one or more parameters>
```

*Parameters:*

```
[keyhost <SSH Key IP Address or Name>]
[keyuser <SSH Key User>]
[viewkey <enable|disable>]
```

---

**To display host keys (public key only):**

```
show sshkey server [type <all|rsa1|rsa|dsa>]
```

---

6. Click the **Apply** button. New entries display in the Imported SSH Keys table and Exported SSH Keys table, as applicable.

## Custom User Menus

Local and remote users can have a custom user menu as their command line interface rather than the standard command set. Instead of typing each command, the user enters the number associated with the command. Each command can also have a nickname that can display in the menu instead of the command.

From the current menu, a user can display another menu, thus allowing menus to be nested. The special command `showmenu <Menu Name>` displays a specified menu. The special command `returnmenu` redisplay the parent menu if the current menu was displayed from a `showmenu` command.

The user with appropriate rights creates and manages custom user menus from the command line interface, but can assign a custom user menu to a user from either the command line or the web interface.

### 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.)

---

**To assign a custom user menu to a local or remote user:**

```
set localusers add|edit <User Login> menu <Menu Name>
```

---

**To create a new custom user menu or add a command to an existing custom user menu:**

```
set menu add <Menu Name> [command <Command Number>]
```

---

**To change a command or nickname within an existing custom user menu:**

```
set menu edit <Menu Name> command <Command Number>
set menu edit <Menu Name> nickname <Command Number>
```

---

**To set the optional title for a menu:**

```
set menu edit <Menu Name> title <Menu Title>
```

---

**To enable or disable the display of command nicknames instead of commands:**

```
set menu edit <Menu Name> shownicknames <enable|disable>
```

---

**To enable or disable the redisplay of the menu before each prompt:**

```
set menu edit <Menu Name> redisplaymenu
<enable|disable>
```

---

**To delete a custom user menu or one command within a custom user menu:**

```
set menu delete <Menu Name> [command <Command Number>]
```

---

**To view a list of all menu names or all commands for a specific menu:**

```
show menu <all|Menu Name>
```

---

## Example

The system administrator creates two custom user menus, with menu1 having a nested menu (menu2):

```
[SLB]> set menu add menu1
Enter optional menu title (<return> for none): Menu1 Title
Specify nickname for each command? [no] y
Enter each command, up to 50 commands ('logout' is always the last command).
Press <return> when the menu command set is complete.

Command #1: connect direct deviceport 1
Nickname #1: connect Port-1
Command #2: connect direct deviceport 2
Nickname #2: connect Port-2
Command #3: showmenu menu2
Warning: menu 'menu2' does not exist.
Nickname #3: menu2
Command #4:
Command #4: logout
Nickname #4: log off
Custom User Menu settings successfully updated.
[SLB]> set menu add menu2
Enter optional menu title (<return> for none): Menu2 Title
Specify nickname for each command? [no]
Enter each command, up to 50 commands ('logout' is always the last command).
Press <return> when the menu command set is complete.

Command #1: connect direct deviceport 3
Command #2: connect direct deviceport 4
Command #3: show datetime
Command #4: returnmenu
Command #5:
Command #5: logout
Custom User Menu settings successfully updated.
[SLB]> show menu all
___Custom User Menus
menu1      menu2
[SLB]> show menu menu1
___Custom User Menus
Menu: menu1
Title: Menu1 Title
Show Nicknames: enabled
Redisplay Menu: disabled
Command  1: connect direct deviceport 1
Nickname 1: connect Port-1
Command  2: connect direct deviceport 2
Nickname 2: connect Port-2
Command  3: showmenu menu2
Nickname 3: menu2
Command  4: logout
Nickname 4: log off
[SLB]> show menu menu2
_
```



```

__Custom User Menus__
Menu: menu2
Title: Menu2 Title
Show Nicknames: disabled
Redisplay Menu: disabled
Command 1: connect direct deviceport 3
Nickname 1: <none>
Command 2: connect direct deviceport 4
Nickname 2: <none>
Command 3: show datetime
Nickname 3: <none>
Command 4: returnmenu
Nickname 4: <none>
Command 5: logout
Nickname 5: <none>

```

The system administrator 4 configures local user 'john' to use custom menu 'menu1':

```

[SLB]> set localusers edit john custommenu menu1
Local users settings successfully updated.
[SLB]> show localusers user john
__Current Local Users Settings__
Login: john
Password: <set> UID: 101
Listen Ports: 1-32
Data Ports: 1-32
Clear Ports: 1-32
Escape Sequence: \x1bA Break Sequence: \x1bB
Custom Menu: menu1
Allow Dialback: disabled
Dialback Number: <none>

```

User 'john' logs into the command line interface, initially sees menu1, executes the command to jump to nested menu menu2, and then returns to menu1:

```

Welcome to the SLB Branch Office Manager
Model Number: SLB32
For a list of commands, type 'help'.

[Enter 1-4]> help
-----
Menu1 Title
-----
1) connect Port-1          3) menu2
2) connect Port-2          4) log off
[Enter 1-4]> 3
Executing: showmenu menu2

[Enter 1-5]> help
Menu2 Title
-----
1) connect direct deviceport 3
2) connect direct deviceport 4
3) show datetime
4) returnmenu
5) logout
[Enter 1-5]> 3
Executing: show datetime
Date/Time: Tue Sep 7 19:13:35 2004
Timezone: UTC
[Enter 1-5]> 4
Executing: returnmenu

[Enter 1-4]> help

```

```
Menu1 Title
-----
1) connect Port-1      3) menu2
2) connect Port-2      4) log off
[Enter 1-4]> 4
Executing: logout
Logging out...
```

## 12: Maintenance and Operation

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.

### SLB Maintenance

The 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.)
- ◆ Set up the location or method that will be used to save or restore configurations (default, FTP, SFTP, NFS, CIFS, or PCCARD). Update the version of the firmware running on the SLB branch office manager.
- ◆ Save a snapshot of all settings on the SLB device (save a configuration).
- ◆ Restore the configuration, either to a previously saved configuration, or to the factory defaults.
- ◆ View and terminate current web sessions.
- ◆ Import a site-specific SSL certificate
- ◆ For dual boot SLB devices, 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.
- ◆ Enable an iGoogle gadget that displays the status of ports on multiple SLB branch office managers.

#### To configure settings:

1. Click the **Maintenance** tab. The Firmware & Configurations page displays.

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'Maintenance' tab is active. Below the navigation bar, there's a 'Firmware & Configurations' section with a 'Help?' link. The main content area is divided into several sections:

- General:** Includes 'Reboot' and 'Shutdown' checkboxes. There are input fields for 'Welcome Banner', 'Login Banner', and 'Logout Banner'. A 'Web Timeout' section has radio buttons for 'No' and 'Yes, minutes (5-120):' with a value of '30'. There are links for 'Web Sessions' and 'SSL Certificate'.
- SLB Firmware:** Shows 'Current Version: 5.3'. There's an 'Update Firmware' checkbox and a 'Firmware Update Log' link. 'Load Firmware via:' is set to 'FTP' with an 'Upload File' link. There are input fields for 'Firmware Filename' and 'Key'.
- FTP/SFTP/TFTP Server:** Includes fields for 'Server' (172.18.0.85), 'Path' (/export/home/share), 'Login' (backup), 'Password', and 'Retype Password'.
- Boot Banks:** Shows 'Bank 1: 5.3 (current)', 'Bank 2: 5.2a', and 'Next Boot Bank: 1'. There are checkboxes for 'Switch to Bank 2', 'Copy configuration from Bank 1 to Bank 2 during firmware update', and 'Copy contents of Bank 1 to Bank 2'.
- Configuration Management:** Has radio buttons for 'No Save/Restore', 'Save Configuration', 'Restore Factory Defaults', and 'Restore Saved Configuration'. There are checkboxes for 'SSH Keys', 'SSL Certificate', and 'Preserve Configuration after Restore' with sub-options for Networking, Date/Time, Services, Remote Auth, Local Users, Device Ports, PC Card, and Power Outlets. There are also dropdown menus for 'Configuration Name to Save To or Restore From', 'Location for Save, Restore or Manage', and 'Saved Configurations' for FTP Server, NFS Mounted Directory, CIFS Share, and PC Card.

An 'Apply' button is located at the bottom right of the configuration area.

2. Enter the following:

**General**

<p><b>Reboot</b></p>	<p>Select this option to reboot the SLB branch office manager immediately. The default is <b>No</b>.</p> <p><b>Note:</b> The front panel LCD displays the “Rebooting the SLB” message, and the normal boot sequence occurs.</p>
<p><b>Shutdown</b></p>	<p>Select this option to shut down the SLB device. The default is <b>No</b>.</p>
<p><b>Welcome Banner</b></p>	<p>The text to display on the command line interface before the user logs in. <b>Welcome to the SLB</b> is the default.</p> <p><b>Note:</b> To create more lines use the <b>\n</b> character sequence.</p>

<b>Login Banner</b>	<p>The text to display on the command line interface after the user logs in. Default is blank.</p> <p><b>Note:</b> To create more lines, use the <b>\n</b> character sequence.</p>
<b>Logout Banner</b>	<p>The text to display on the command line interface after the user logs out. Default is blank.</p> <p><b>Note:</b> To create more lines use, the <b>\n</b> character sequence.</p>
<b>Web Timeout</b>	<p>Number of minutes (5-120) after which the SLB web session times out. The default is <b>5</b>. To avoid timeouts, select <b>No</b>.</p> <p>If the session times out, refresh the browser page and enter your user id and password to open another web session.</p> <p><b>Note:</b> If you close the browser without logging off the SLB branch office manager first, you will have to wait for the timeout time to expire. You can also end a web session by using the <i>admin web terminate</i> command at the CLI or by asking your system administrator to terminate your active web session.</p> <p>To view or terminate current web sessions, click the <b>Web Sessions</b> link. (See <a href="#">Firmware &amp; Configurations – Web Sessions</a> on page 184.)</p> <p>To view, import, or reset the SSL Certificate, click the <b>SSL Certificate</b> link. (See <a href="#">Firmware &amp; Configurations – Web Sessions</a> on page 184.)</p>
<b>Enable iGoogle Gadget Web Content</b>	<p>Select the check box to enable an SLB iGoogle gadget. The iGoogle gadget allows an iGoogle user to view the port status of many SLB devices on one web page. (See <a href="#">iGoogle Gadgets</a> on page 186.)</p>

### SLB Firmware

<b>Update Firmware</b>	<p>To update the SLB firmware, select the checkbox. If you select this option, the SLB reboots after you apply the update.</p> <p>To view a log of all prior firmware updates, click the <b>Firmware Update Log</b> link.</p> <p><b>Note:</b> For dual boot SLB branch office managers, 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.</p>
<b>Load Firmware via</b>	<p>From the drop-down list, select the method of loading the firmware. Options are <b>FTP</b>, <b>TFTP</b>, <b>HTTPS</b> and <b>SFTP (Secure FTP)</b>. <b>FTP</b> is the default.</p> <p>If you select <b>HTTPS</b>, the <b>Upload File</b> link becomes active. Select the link to open a popup window that allows you to browse to a firmware update file to upload.</p>
<b>Firmware Filename</b>	<p>The name of the firmware update file downloaded from the Lantronix web site.</p>
<b>Key</b>	<p>A key for validating the firmware file. The key is provided with the firmware file (32 hex characters).</p>

## Boot Banks

<b>Bank 1</b>	Version of SLB firmware in bank 1. <b>Note:</b> The word "current" displays next to the bank the SLB branch office manager booted from.
<b>Bank 2</b>	Version of SLB firmware in bank 2.
<b>Next Boot Bank</b>	Current setting for bank to boot from at next reboot.
<b>Switch to Bank</b>	If desired, select the alternate bank to boot from at next reboot.
<b>Copy configuration from Bank 1 to Bank 2 during firmware update</b>	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.
<b>Copy contents of Bank 1 to Bank 2</b>	If checked, enables you to copy the current boot bank to the alternate boot bank. This process takes a few minutes to complete.

## FTP/TFTP/SFTP

<b>Server</b>	The IP address or host name of the server used for obtaining updates and saving or restoring configurations. May have up to 64 alphanumeric characters; may include hyphens and underscores.
<b>Path</b>	The default path on the server for obtaining firmware update files and getting and putting configuration save files.
<b>Login</b>	The userid for accessing the FTP server. May be blank.
<b>Password /Retype Password</b>	The FTP user password.

## Configuration Management

<b>Configuration Management</b>	<p>From the option list, select one of the following:</p> <p><b>No Save/Restore:</b> Does not save or restore a configuration.</p> <p><b>Save Configuration:</b> Saves all settings to file, which can be backed up to a location that is not on the SLB branch office manager.</p> <p><b>Restore Factory Defaults:</b> Restores factory defaults. If you select this option, the SLB device reboots after you apply the update. Select the <b>Save SSH Keys</b> checkbox to save any imported or exported SSH keys. Select the <b>Save SSL Certificate</b> checkbox to save any imported certificate. Disabled by default.</p> <p><b>Restore Saved Configuration:</b> Returns the SLB settings to a previously saved configuration. If you select this option, the SLB branch office manager reboots after you apply the update.</p>
<b>Configuration Name to Save to or Restore From</b>	If you selected to save or restore a configuration, enter a name for the configuration file (up to 12 characters).

<b>Location for Save, Restore, or Manage</b>	<p>If you selected to save or restore a configuration, select one of the following options:</p> <p><b>Default – Saved Configurations:</b> If restoring, select a saved configuration from the drop-down list.</p> <p><b>FTP Server:</b> The FTP server specified in the FTP/SFTP/TFTP section. If you select this option, select FTP or SFTP to transfer the configuration file.</p> <p><b>NFS Mounted Directory:</b> Local directory of the NFS server for mounting files.</p> <p><b>CIFS Share – Saved Configurations:</b> If restoring, select a saved configuration from the drop-down list.</p> <p><b>PC Card:</b> If a PC Card Compact Flash is loaded into one of the PC Card slots on the front of the SLB branch office manager, and properly mounted, the configuration can be saved to or restored from this location.</p> <p>If you select this option, select the slot (upper or lower) in which the PC Card Compact Flash is mounted, and then select a saved configuration from the drop-down list.</p> <p><b>Manage:</b> The <b>Manage</b> option allows you to view and delete all configurations saved to the selected location. This feature is available for the default, CIFS Share, and PC Card locations. (See page <a href="#">183</a>.)</p>
<b>Preserve Configuration after Restore</b>	<p>Allows the user to keep a subset of the current configuration after restoring a configuration or resetting to factory defaults.</p> <p>Select the checkbox for each part of the current configuration you want to keep, for example, Networking, Services, or Device Ports.</p>

3. Click **Apply**.

**Note:** If you selected an option that forces a reboot (restore configuration, update firmware, or reset factory defaults), the SLB branch office manager automatically reboots at the end of the process.

#### To manage configuration files:

The **Manage** option on the 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 PC Card locations.

1. On the Firmware and Configurations page, click the **Manage** link. The following page displays the name and the time and date the file was saved:

The screenshot shows the LANTRONIX SLB884 web interface. The user is logged in as 'sysadmin'. The page title is 'Firmware & Configurations - Manage Configuration Files'. Below the title is a 'Back to Firmware & Configurations' link. The main content area contains a table titled 'Configurations - Default location' with a 'Delete' button. The table has the following data:

Name	Date/Time Saved	SSH Keys	SSL Certificate
slmsls	04/25/08 00:26:45	N	N

- To delete files, select one or more files and click the **Delete** button.

## Firmware & Configurations – Web Sessions

The Firmware & Configurations - Web Sessions page enables you to view and terminate current web sessions.

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

- On the Firmware & Configurations page, click the **Web Sessions** link. The following page displays:

The screenshot shows the LANTRONIX SLB884 web interface. The user is logged in as 'sysadmin'. The page title is 'Firmware & Configurations - Web Sessions'. Below the title is a 'Back to Firmware & Configurations' link. The main content area contains a table titled 'Current Web Sessions' with a 'Terminate' button. The table has the following data:

Id	User	Login Time	Idle Time
1	sysadmin	04/29/08 09:38	0:00:00:00

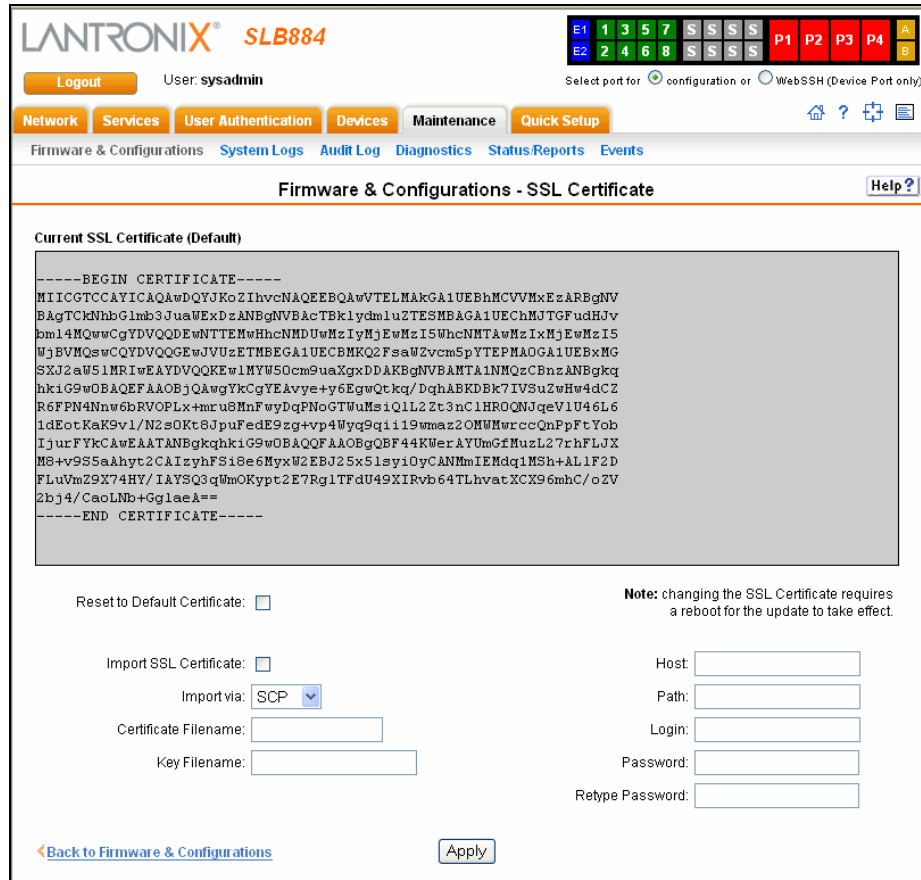
## Firmware & Configurations – SSL Certificate

The Firmware & Configurations – SSL Certificate 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, if desired.

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

- On the Firmware & Configurations page, click the **SSL Certificate** link. The following page displays the current SSL certificate.





2. If desired, enter the following:

<b>Reset to Default Certificate</b>	To reset to the default certificate, select the checkbox to reset to the default certificate. Unselected by default.
<b>Import SSL Certificate</b>	To import your own SSL Certificate, select the checkbox. Unselected by default.
<b>Import via</b>	From the drop-down list, select the method of importing the certificate (SCP or SFTP). The default is <b>SCP</b> .
<b>Certificate Filename</b>	Filename of the certificate.
<b>Key Filename</b>	Filename of the private key for the certificate.
<b>Host</b>	Host name or IP address of the host from which to import the file.
<b>Path</b>	Path of the directory where the certificate will be stored.
<b>Login</b>	User ID to use to SCP or SFTP the file.
<b>Password &amp; Retype Password</b>	Password to use to SCP or SFTP the file.

3. Click the **Apply** button.

**Note:** You must reboot the SLB device for the update to take effect.

4. To return to the Back to Firmware & Configurations page, click the link at the bottom of the page.

## iGoogle Gadgets

You can create an iGoogle gadgets that enables you to view the status of the ports of many SLB branch office managers on one web page.

Anyone with a Google email account (gmail.com) can create an iGoogle gadget for viewing web pages. There are two types of iGoogle gadgets: public gadgets and private gadgets. The public gadgets are listed for import on iGoogle web pages. The SLB gadget is a private gadget, whose location is not publicly advertised.

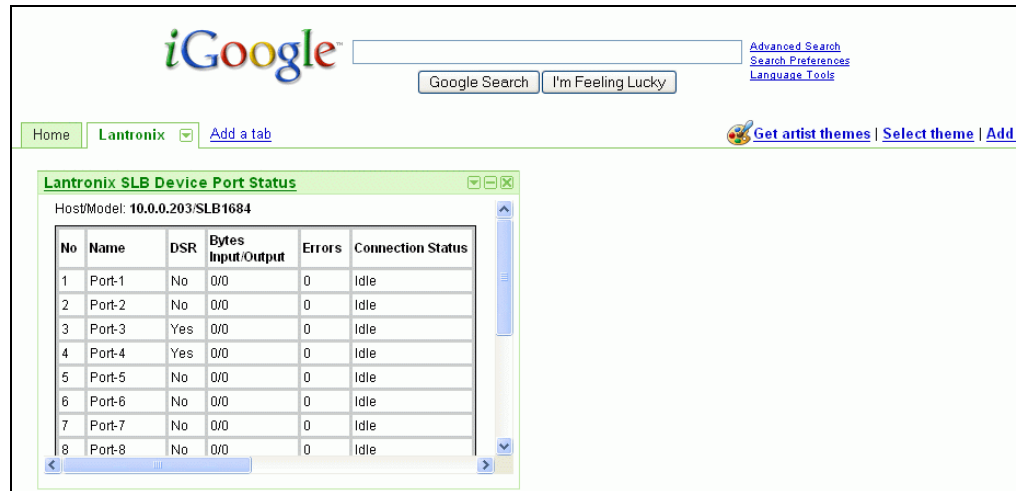
### To set up an SLB iGoogle gadget:

1. Load the following XML code on a web server that is accessible over the Internet. This code describes how to retrieve information and how to format the data for display.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Module>
  <ModulePrefs title="__UP_model__ Devport Status"
    title_url="http://www.lantronix.com"
    directory_title="SLC/SLB Status" description="Devport
    status and counters" scrolling="true" width="400"
    height="360" />
- <UserPref name="model" display_name="Model" datatype="enum"
  default_value="slc">
  <EnumValue value="SLC" display_value="SLC" />
  <EnumValue value="SLB" display_value="SLB" />
  </UserPref>
  <UserPref name="ip" display_name="IP Address" required="true"
  />
- <UserPref name="rate" display_name="Refresh Rate"
  datatype="enum" default_value="10">
  <EnumValue value="1" display_value="1 second" />
  <EnumValue value="5" display_value="5 seconds" />
  <EnumValue value="10" display_value="10 seconds" />
  <EnumValue value="30" display_value="30 seconds" />
  <EnumValue value="60" display_value="1 minute" />
  <EnumValue value="300" display_value="5 minutes" />
  <EnumValue value="600" display_value="10 minutes" />
  </UserPref>
  <Content type="url" href="http://__UP_ip__/devstatus.htm" />
</Module>
```

2. On the iGoogle web page, click the **Add stuff** link.
3. On the new page, click the **Add feed or gadget** link.
4. In the field that displays, type the URL of the gadget location.
5. Return to the gadget viewing page and complete the SLB gadget configuration fields.

You should see an iGoogle gadget similar to the following:



## Administrative Commands

These commands for the command line interface correspond to the web page entries described above.

### To copy the boot bank from the currently booted bank to the alternate bank (for dual-boot SLB branch office managers):

```
admin firmware copybank
```

### To reboot the SLB device:

```
admin reboot
```

**Note:** The front panel LCD displays the "Rebooting the SLB" message, and the normal boot sequence occurs.

### To add welcome, login, and logout banners:

```
admin banner login <Banner Text>
```

```
admin banner logout <Banner Text>
```

```
admin banner welcome <Banner Text>
```

**Note:** To go to the next line, type **\n** and press **Enter**.

### To display banners:

```
admin banner show
```

### To prepare the SLB branch office manager to be powered off:

```
admin shutdown
```

**Note:** When you use this command to shut down the SLB device, the LCD front panel displays "Shutting down the SLB," followed by a pause, and then "Shutdown complete." When "Shutdown complete" displays, it is safe to power off the SLB branch office manager. This command is not available on the Web page.

**To enable or disable iGoogle Gadget web content:**

```
admin web gadget <enable|disable>
```

---

**To configure the timeout for web sessions:**

```
admin web timeout <disable|5-120>
```

Timeouts are measured in minutes.

---

**To terminate a web session:**

```
admin web terminate <web session id>
```

---

**To view current timeout and all active web sessions:**

```
admin web show
```

---

**To list current hardware and firmware information:**

```
admin version
```

---

**To update SLB firmware to a new revision:**

**Note:** The firmware file should be accessible via the settings displayed by `admin ftp show`. The SLB branch office manager automatically reboots after successful update.

```
admin firmware update <ftp|tftp|sftp> file <Firmware File> key  
<Checksum Key>
```

---

**To set the boot bank to be used at the next SLB reboot:**

```
admin firmware bootbank <1|2>
```

Applies to dual-boot SLB devices only.

---

**To list the current firmware revision:**

```
admin firmware show [viewlog <enable|disable>]
```

Lists the current firmware revision, the boot bank status (for dual-boot SLB branch office managers), and optionally displays the log containing details about firmware updates.

---

**To lock or unlock the LCD keypad:**

**Note:** If the keypad is locked, users can scroll through settings but not change them.

```
admin keypad <lock|unlock>
```

---

**To change the Restore Factory Defaults password used at the LCD to return the SLB branch office manager to the factory settings:**

```
admin keypad password <Password>
```

Must be 6 digits.

---

**To view keypad settings:**

```
admin keypad show
```

**To set the FTP/TFTP/SFTP server used for firmware updates and configuration save/restore:**

```
admin ftp server <IP Address or Hostname> [login <User Login>]
[path <Directory>]
```

**To view FTP settings:**

```
admin ftp show
```

**To set the FTP server password and prevent it from being echoed:**

```
admin ftp password
```

**To restore the SLB device to factory default settings:**

```
admin config factorydefaults [savesshkeys <enable|disable>]
[savesSLBert <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	lu - Local Users
sv - Services	dp - Device Ports
dt - Date/Time	pc - PC Card
po - Power Outlets	

**To restore a saved configuration to the SLB branch office manager:**

```
admin config restore <Config Name> location
<default|ftp|sftp|nfs|cifs|pccard> [nfsdir <NFS Mounted Dir>]
[pccardslot <upper|lower>] [keepconfig <Config Params to Keep>]
[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	lu - Local Users
sv - Services	dp - Device Ports
dt - Date/Time	pc - PC Card
po - Power Outlets	

**To save the current SLB configuration to a selected location:**

```
admin config save <Config Name> location
<default|ftp|sftp|nfs|cifs|pccard> [nfsdir <NFS Mounted Dir>]
[pccardslot <upper|lower>]
```

**To delete a saved configuration:**

```
admin config delete <Config Name> location <default|cifs|pccard>
[pccardslot <upper|lower>]
```

---

**To list the configurations saved to a location:**

```
admin config show <default|ftp|sftp|nfs|cifs|pccard> [nfsdir <NFS
Mounted Dir>] [pccardslot <upper|lower>]
```

---

**To run the quick setup script:**

```
admin quicksetup
```

---

**To import an SSL certificate, or reset the web server certificate to the default:**

```
admin web certificate import via <sftp|scp> certfile <Certificate File>
privfile <Private Key File> host <IP Address or Name>
login <User Login> [path <Path to Files>]
```

---

**To reset a web certificate:**

```
admin web certificate reset
```

---

**To show a web certificate:**

```
admin web certificate show
```

---

**To restart the program that controls the LCD:**

```
admin lcd reset
```

---

## System Logs

The System Logs page allows you to view various system logs. (See [7: Services](#) 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:



2. Enter the following:

<b>Log</b>	Select the type(s) of log you want to view.
<b>Level</b>	Select the alert level you want to view for the selected log.
<b>Starting at</b>	Select the starting point of the range you want to view: <b>Beginning of Log:</b> Beginning of the log. <b>Date:</b> Specific start date and time of the log.
<b>Ending at</b>	Select the endpoint of the range you want to view: <b>End of Log:</b> The end of the log. <b>Date:</b> Specific end date and time of the log.

3. Click the **View Log** button. The log displays. For example, if you select the type **All** and the level **Error**, the SLB device displays a log similar to this:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there's a status bar with various indicators (E1-E2, 1-8, S, P1-P4, A, B). Below that, a navigation menu includes 'Network', 'Services', 'User Authentication', 'Devices', 'Maintenance', and 'Quick Setup'. The 'Maintenance' tab is active, showing 'System Logs'. The 'Log: All - Error Level' is selected. There's an 'Email Output' button and a form with fields for 'Comment', 'to' (with a radio button selected), and 'Case Number'. A note on the right says: 'Note: A valid case number is required to submit an e-mail to Tech Support. Contact Lantronix Tech Support to receive a case number.' Below the form is a scrollable log window showing system messages from August 21, 2007, including kernel errors and device status reports.

4. To email the system log to an individual:
  - a) In the **Comment** field, enter a comment (if desired).
  - b) Select **to** and enter the person's email address.
  - c) Press the **Email Output** button.
5. To email the system log to Lantronix Technical Support:
  - a) In the **Comment** field, enter a comment (if desired).
  - b) Select **to: Lantronix Tech Support**.
  - c) Call Lantronix Tech Support and obtain a case number.
 

**Note:** For contact information, click the **Lantronix Tech Support** link.
  - d) Enter the number in **Case Number**.
  - e) Press the **Email Output** button.
6. A message asks for confirmation. Click **OK**.

#### To clear system logs:

1. From the main menu, select **SLB Maintenance – System Logs**.
2. Select the logs you want to clear and click the **Clear Log** button.



## System Log Command

The following command for the command line interface corresponds to the web page entries described above.

---

### To view the system logs containing information and error messages:

```
show syslog [<parameters>]
```

#### Parameters:

```
[email <Email Address>]
level <error|warning|info|debug>
log <all|netlog|servlog|authlog|devlog|diaglog|genlog>
display <head|tail> [numlines <Number of Lines>]
startingtime <MMDDYYhhmm [ss]
endtime <MMDDYYhhmm [ss]
```

**Note:** The level and time parameters cannot be used simultaneously.

---

### To clear one or all of the system logs:

```
show syslog clear
<all|netlog|servlog|authlog|devlog|diaglog|genlog>
```

---

## Audit Log

The Audit Log web page displays a log of all actions that have changed the configuration of the SLB branch office manager. The audit log is disabled by default. Use the Services web page ([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 reboots.**

1. Click the **Maintenance** tab and select the **Audit Log** option. The following page displays:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there is a status bar with various indicators (E1-E2, 1-8, S, P1-P4, A, B) and a user login section for 'User: sysadmin'. Below this is a navigation menu with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'Maintenance' tab is selected, and the 'Audit Log' page is displayed. The log shows a list of events sorted by Date/Time, with columns for Date/Time, User, and Command/Action. The events include SSH authentication success, user logouts, and SSH key management actions (delete, import, copy/paste) performed by the sysadmin user.

Sorted by: Date/Time	Sort by User	Sort by Command	Clear Log
Feb 12 18:42:50 2008		SSH Authentication Success for user sysadmin	
Feb 12 18:42:51 2008		User sysadmin logged off of SSH session	
Feb 12 18:42:51 2008	sysadmin	set sshkey delete keyuser sysadmin keyhost slm01_glenn17	
Feb 12 18:42:51 2008	sysadmin	set sshkey import import copy/paste	
Feb 12 18:44:17 2008		SSH Authentication Success for user sysadmin	
Feb 12 18:44:17 2008	sysadmin	set sshkey delete keyuser sysadmin keyhost slm02_tpham17	
Feb 12 18:44:18 2008		User sysadmin logged off of SSH session	
Feb 12 18:44:18 2008	sysadmin	set sshkey import import copy/paste	
Feb 12 18:45:17 2008		SSH Authentication Success for user sysadmin	
Feb 12 18:45:18 2008	sysadmin	set sshkey delete keyuser sysadmin keyhost slm01_glenn19	
Feb 12 18:45:18 2008	sysadmin	set sshkey import import copy/paste	
Feb 12 18:45:19 2008		User sysadmin logged off of SSH session	
Feb 12 18:47:45 2008		SSH Authentication Success for user sysadmin	
Feb 12 18:47:45 2008	sysadmin	set sshkey delete keyuser sysadmin keyhost slm02_tpham19	
Feb 12 18:47:45 2008	sysadmin	set sshkey import import copy/paste	
Feb 12 18:47:46 2008		User sysadmin logged off of SSH session	
Feb 27 12:08:36 2008		SSH Authentication Success for user sysadmin	
Feb 27 12:08:37 2008		User sysadmin logged off of SSH session	
Feb 27 12:08:37 2008	sysadmin	set sshkey delete keyuser sysadmin keyhost slm02-tpham17	
Feb 27 12:08:37 2008	sysadmin	set sshkey import import copy/paste	

- To select a sort option (by Date/Time, User, Command/Action, click the appropriate button:
  - ◆ To sort by date and time, click the **Sort by Date/Time** button. (This is the default.)
  - ◆ To sort by user, click the **Sort by User** button.
  - ◆ To sort by command/action, click the **Command** button.
- To clear the log, click the **Clear Log** button.

## Diagnostics

The Diagnostics web 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.

- Click the **Maintenance** tab and select the **Diagnostics** option. The following page displays:



2. Enter the following:

<b>Select Diagnostics</b>	Select one or more diagnostic methods you want to run, or select <b>All</b> to run them all.
<b>ARP Table</b>	Address Resolution Protocol (ARP) table used to view the IP address-to-hardware address mapping.
<b>Netstat</b>	Displays network connections. If you select the checkbox, select a protocol or select <b>All</b> for both protocols to control the output of the Netstat report.
<b>Host Lookup</b>	If you enter a host name in the corresponding <b>Hostname</b> field, verifies that the SLB branch office manager can resolve the host name into an IP address (if DNS is enabled).
<b>Ping</b>	If you enter a host name in the corresponding <b>Hostname</b> field, verifies that the host is up and running.

---

<b>Send Packet</b>	<p>This option sends an Ethernet packet out one of the Ethernet ports, mainly as a network connectivity test.</p> <p>Enter the following:</p> <p><b>Protocol:</b> Select the type of packet to send.</p> <p><b>Hostname:</b> Specify a host name or IP address of the host to send the packet to.</p> <p><b>Port:</b> Specify a <b>TCP</b> or <b>UDP</b> port number of the host to send the packet to.</p> <p><b>String:</b> 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).</p> <p><b>Count:</b> The count is the number of times the string is sent.</p> <p>For UDP, the number of times the string is sent is equal to the number of packets sent.</p> <p>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.</p>
--------------------	--

3. Click the **Run Diagnostics** button. The Diagnostics report page displays.

LANTRONIX® SLB884

Logout User: sysadmin Select port for  configuration or  WebSSH (Device Port only)

Network Services User Authentication Devices Maintenance Quick Setup

Firmware & Configurations System Logs Audit Log Diagnostics Status/Reports Events

### Diagnostics [Help ?](#)

Diagnostic Output: [Arp Table](#) [Netstat \(All\)](#) [SLB Internals](#)  Comment:

to:

to: **Lantronix Tech Support**

Case Number:

**Note:** A valid case number is required to submit an e-mail to Tech Support. Contact [Lantronix Tech Support](#) to receive a case number.

#### Arp Table

Address	HWtype	HWaddress
172.18.100.26	ether	00:01:02:4F:D6:D5
172.18.100.29	(incompl	eth0
172.18.21.68	ether	00:40:05:35:F0:6E
172.18.21.68	ether	00:40:05:35:F0:6E

#### Netstat (All)

```

Ip:
1262989 total packets received
22 with invalid headers
0 forwarded
0 incoming packets discarded
1256160 incoming packets delivered
47793 requests sent out
66 reassemblies required
33 packets reassembled ok
32 fragments received ok

Icmp:
11840 ICMP messages received
11338 input ICMP message failed.
ICMP input histogram:
destination unreachable: 11840
11841 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
destination unreachable: 11841

Tcp:
5 active connections openings

```

4. To view a report, click the link for that report.
5. To email the report(s) to an individual:
  - a) In the **Comment** field, enter a comment (if desired).
  - b) Select **to** and enter the person's email address.
  - c) Press the **Email Output** button.
6. To email the report(s) to Lantronix Technical Support:
  - a) In the **Comment** field, enter a comment (if desired).
  - b) Select **to: Lantronix Tech Support**
  - c) Call Lantronix Tech Support and obtain a case number.

**Note:** For contact information, click the **Lantronix Tech Support** link.

  - d) Enter the number in **Case Number**.
  - e) Press the **Email Output** button.

## Diagnostic Commands

The following CLI commands correspond to the web page entries described above.

---

### To display the ARP table of IP address-to-hardware address mapping:

```
diag arp [email <Email Address>]
```

*You can optionally email the displayed information.*

---

### To display a report of network connections:

*You can optionally email the displayed information.*

```
diag netstat [protocol <all|tcp|udp>] [email <Email Address>]
```

---

### To resolve a host name into an IP address:

*You can optionally email the displayed information.*

```
diag lookup <Hostname> [email <Email Address>]
```

---

### To test a device port by transmitting data out the port and verifying that it is received correctly:

```
diag loopback <Device Port Number or Name> [<parameters>]
```

*Parameters:*

```
test <internal|external>
```

```
xferdatasize <Size In Kbytes to Transfer>
```

*Default is 1 Kbyte.*

**Note:** A special loopback cable comes with the SLB branch office manager. 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.

---

### To display the route that packets take to get to a network host:

```
diag traceroute <IP Address or Hostname>
```

---

### To verify that the host is up and running:

```
diag ping <IP Address or Name> [<parameters>]
```

*Parameters:*

```
count <Number of Times to Ping>
```

*The default is 5.*

```
packetsize <Size in Bytes>
```

*The default is 64.*

---

### To display performance statistics for an Ethernet port or a device port (averaged over the last 5 seconds):

```
diag perfstat [ethport <1|2>] [deviceport <Device Port # or Name>]
```

---

**To generate and send Ethernet packets:**

```
diag sendpacket host <IP Address or Name> port <TCP or UDP Port
Number> [string <Packet String>] [protocol <tcp|udp>] [count
<Number of Packets>]
```

*The default is 1.*

---

**To display all network traffic, applying optional filters:**

**Note:** *This command is not available*

```
diag nettrace <one or more parameters>
```

*Parameters:*

```
ethport <1|2>
host <IP Address or Name>
numpackets <Number of Packets>
protocol <tcp|udp|icmp>
verbose <enable|disable>
```

---

**To display information on the internal memory, storage and processes of the SLB branch office manager:**

```
diag internals
```

**Note:** *This command is available in the CLI but not the web.*

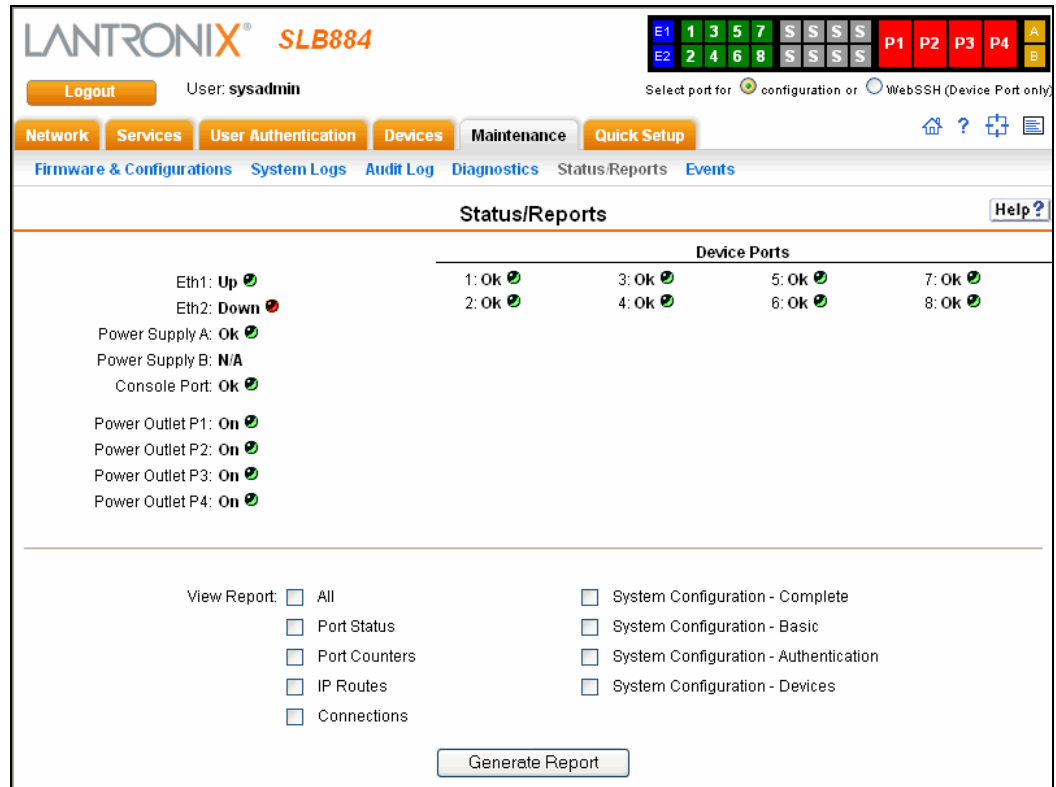
---

## 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:



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. Enter the following:

### View Report

<b>View Report</b>	<p>Select as many of the reports as desired, or select <b>All</b>.</p> <p><b>Port Status:</b> Displays the status of each device port: mode, user, any related connections, and serial port settings.</p> <p><b>Port Counters:</b> Displays statistics related to the flow of data through each device port.</p> <p><b>IP Routes:</b> Displays the routing table.</p> <p><b>Connections:</b> Displays all active connections for the SLB branch office manager: Telnet, SSH, TCP, UDP, device port, and modem.</p> <p><b>System Configuration – Complete:</b> Displays a complete snapshot of the SLB settings.</p> <p><b>System Configuration – Basic:</b> Displays a snapshot of the SLB device's basic settings (for example, network, date/time, routing, services, console port).</p> <p><b>System Configuration – Authentication:</b> Displays a snapshot of authentication settings only (including a list of all localusers).</p> <p><b>System Configuration - Devices:</b> Displays a snapshot of settings for each device port and (each PC Card slot) for a PC Card.</p>
--------------------	---

3. Click the **Generate Report** button. In the upper left, the report page displays a list of reports generated.



The screenshot shows the SLB884 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. Below this is a sub-menu with links for Firmware & Configurations, System Logs, Audit Log, Diagnostics, Status/Reports, and Events. The main content area is titled 'Status/Reports' and contains an 'Email Output' button, a 'Comment' field, and radio buttons for selecting the recipient: 'to:' (selected) and 'to: Lantronix Tech Support'. A 'Case Number' field is also present. A note on the right states: 'Note: A valid case number is required to submit an e-mail to Tech Support. Contact [Lantronix Tech Support](#) to receive a case number.'

Port Status			
Device Port:	1	DSR/CD:	No
Name:	Port-1	DTR:	Yes
Mode:	Idle	CTS:	No
		RTS:	Yes
Device Port:	2	DSR/CD:	No
Name:	Port-2	DTR:	Yes
Mode:	Idle	CTS:	No
		RTS:	Yes
Device Port:	3	DSR/CD:	No
Name:	Port-3	DTR:	Yes
Mode:	Idle	CTS:	No
		RTS:	Yes
Device Port:	4	DSR/CD:	No
Name:	Port-4	DTR:	Yes
Mode:	Idle	CTS:	No
		RTS:	Yes
Device Port:	5	DSR/CD:	No

4. To view a report, click the link for that report.
5. To email the report(s) to Lantronix Technical Support:
  - a) In the **Comment** field, enter a comment (if desired).
  - b) Select **to: Lantronix Tech Support**
  - c) Call Lantronix Tech Support and obtain a case number.  
*Note: For contact information, click the **Lantronix Tech Support** link.*
  - d) Enter the number in **Case Number**.
  - e) Press the **Email Output** button.
6. To email the report(s) to an individual:
  - a) In the **Comment** field, enter a comment (if desired).
  - b) Select **to:** and enter the person's email address.
  - c) Press the **Email Output** button.

## Status Commands

These commands for the command line interface correspond to the web page entries described above.

---

### To display device port modes and states for one or more ports:

*You can optionally email the displayed information.*

```
show portstatus [deviceport <Device Port List or Name>] [email <Email Address>]
```

---

### To display a snapshot of configurable parameters:

*You can optionally email the displayed information.*

```
show sysconfig [display <basic|auth|devices>] [email <Email Address>]
```

Displays a report of all configurable parameters or a shorter report with basic system settings, authentication settings, or device settings.

---

### To generate a report for one or more ports:

*You can optionally email the displayed information.*

```
show portcounters [deviceport <Device Port List or Name>] [email <Email Address>]
```

---

### To display the overall status of all SLB devices:

*You can optionally email the displayed information.*

```
show sysstatus [email <Email Address>]
```

---

### To display a list of all current connections:

*You can optionally email the displayed information.*

```
show connections [email <Email Address>]
```

---

### To provide details, e.g., endpoint parameters and trigger, for a specific connection:

*You can optionally email the displayed information.*

```
show connections connid <Connection ID> [email <Email Address>]
```

**Note:** Use the basic `show connections` command to obtain the Connection ID.

---

## Events

On this page, you can define what action you want to take for events that may occur in the SLB branch office manager.

1. Click the **Maintenance** tab and select the **Events** option. The following page displays:

The screenshot shows the LANTRONIX SLB884 web interface. At the top, there is a navigation menu with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. Below the navigation menu, there are links for Firmware & Configurations, System Logs, Audit Log, Diagnostics, Status/Reports, and Events. The main content area is titled "Events" and contains a configuration form. The form includes the following fields and options:

- Event Trigger:
- Action:
- Ethernet:  Eth1  Eth2
- Modem Connection on:  Upper PC Card Slot  Lower PC Card Slot  Device Port:
- NMS/Host to forward trap to:
- SNMP Community:
- SNMP Trap OID:
- Email Address:

At the bottom of the form, there are buttons for "Add Event", "Edit Event", and "Delete Event". To the right of these buttons, there is a note: "To edit or delete an event, select the radio button in the right column below." Below the form, there is a table with the following columns: "Id", "Event Trigger", "Action/Alarm", and "Options". An "Apply" button is located at the bottom center of the page.

2. Enter the following:

<b>Event Trigger</b>	From the drop-down list, select the type of incident that triggers an event. Currently, the options are: <b>Receive Trap</b> <b>Temperature Over/Under Limit:</b> For Sensorsoft devices. <b>Humidity Over/Under Limit:</b> For Sensorsoft devices.
<b>Action</b>	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.
<b>Ethernet</b>	For actions that require an Ethernet connection (for example, <b>Forward All Traps to Ethernet</b> ), select the Ethernet port to use.
<b>Modem Connection on</b>	For actions that require a modem connection (for example, <b>Forward All Traps to a Modem Connection</b> ), select which device port or PC Card slot with a modem connection to use.
<b>NMS/Host to forward trap to</b>	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.
<b>SNMP Community</b>	Forwarded traps are sent with this SNMP community value There is no default.

<b>SNMP Trap OID</b>	Enter a unique identifier for an SNMP object. (An SNMP object is anything that can hold a value and can be read using an SNMP "get" action.) The OID consists of a string of numbers separated by periods (for example, 1.1.3.2.1). Each number is part of a group represented by the number on its left.
----------------------	---

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 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

To manage the response to events that occur in the SLB branch office manager:

```
admin events add <trigger> <response>
```

<trigger> is one of:

```
|receivetraps|templimit|humidlimit|overcurrent|
```

<response> is one of:

```
action <syslog>
```

```
action <fwdalltrapseth|fwdseltrapeth> ethport <1|2>
nms <SNMP NMS> community <SNMP Community> [oid <SNMP
OID>]
```

```
action <fwdalltrapsmodem|fwdseltrapmodem> deviceport
<Device Port # or Name> nms <SNMP NMS> community
<SNMP Community> [oid <SNMP Trap OID>]
```

```
action <fwdalltrapsmodem|fwdseltrapmodem> pccardslot
<upper|lower> nms <SNMP NMS> community <SNMP
Community> [oid <SNMP Trap OID>]
```

```
action <emailalert> emailaddress <destination email
address>
```

---

**To update event definitions:**

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>  
pccardslot <upper|lower>

---

**To delete an event:**

admin events delete <Event ID>

---

**To view events:**

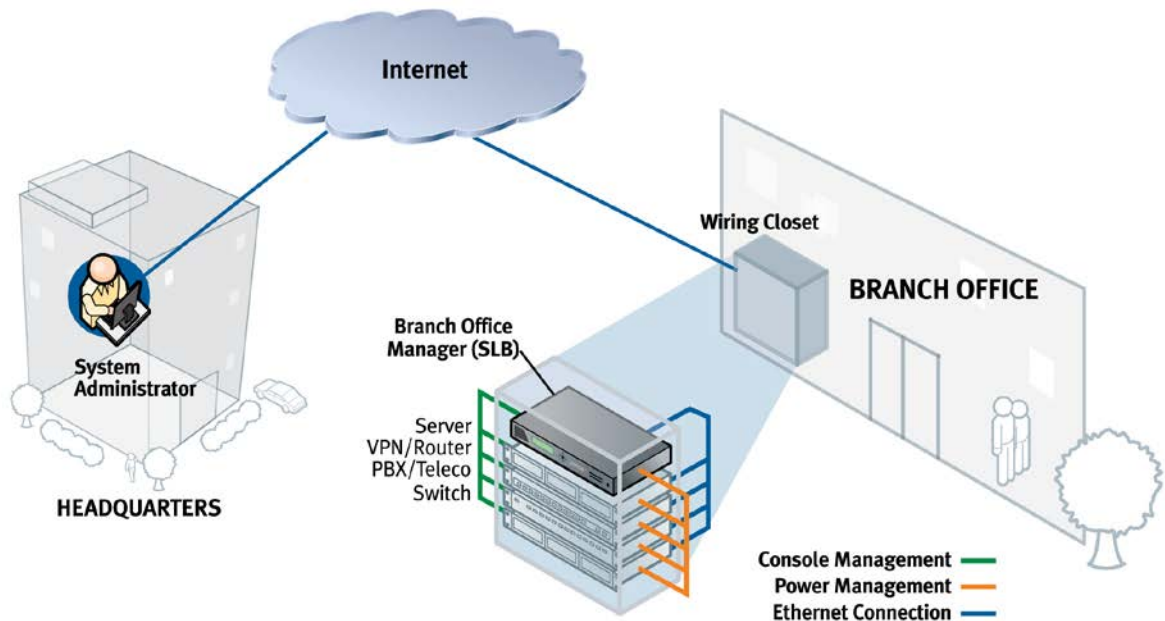
admin events show

---

## 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.

Figure 13-1. SLB Branch Office Manager Configuration

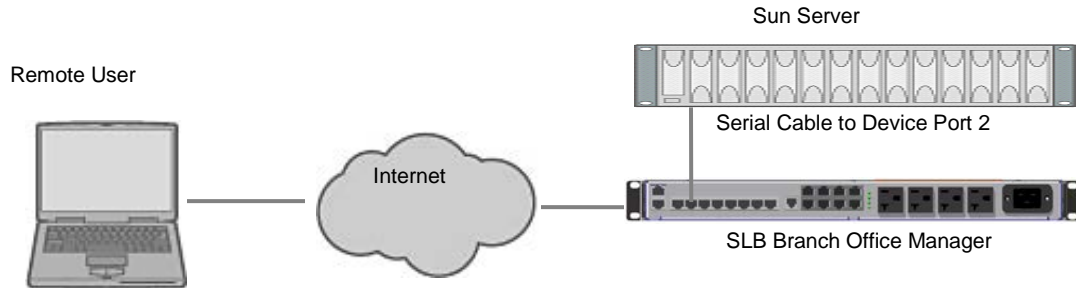


This chapter includes three typical scenarios for using the SLB branch office manager. The scenarios assume that the SLB device is connected to the network and has already been assigned an IP address. In the examples, we use the command line interface. You can do the same things using the web page interface except for directly interacting with the SLB branch office manager (`direct` command).

## Telnet/SSH to a Remote Device

The following figure shows a Sun server connected to port 2 of the SLB device.

**Figure 13-2. Remote User Connected to a SUN Server via the SLB Device**



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
Remote IP: negotiate       Flow Control: xon/xoff  IP: <none>
Authentication: PAP        Logins: disabled
CHAP Host: <none>          Break Sequence: \xlbB
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      PC Card 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:

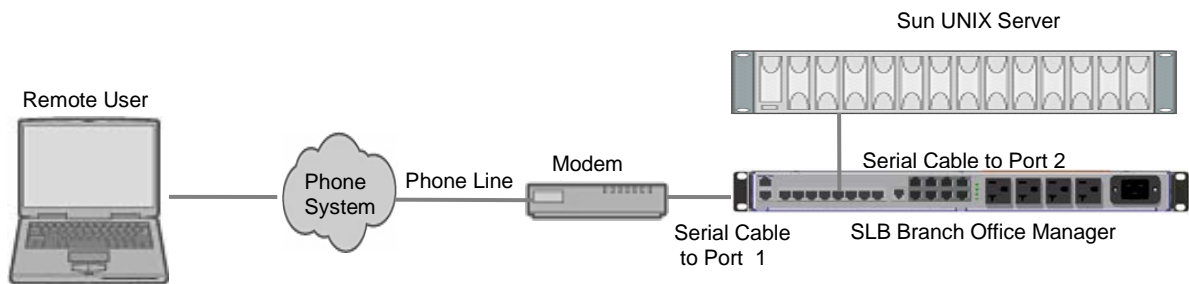
```
Mar 15 09:09:44 tssf280r sendmail[292]: [ID 702911 mail.info] starting daemon
(8.12.2+Sun): SMTP+queueing@00:15:00
Mar 15 09:09:44 tssf280r sendmail[293]: [ID 702911 mail.info] starting daemon
(8.12.2+Sun): queueing@00:15:00
Mar 15 14:44:40 tssf280r sendmail[275]: [ID 702911 mail.info] starting daemon
(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.)

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%COA"
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 device.

```
CONNECT 57600

Welcome to the SLB

login: sysadmin
Password:

Welcome to the SLB Branch Office Manager
Model Number: SLB48
For a list of commands, type 'help'.

[SLB]>
```

5. Connect to the SUN Unix server using the `direct` command.

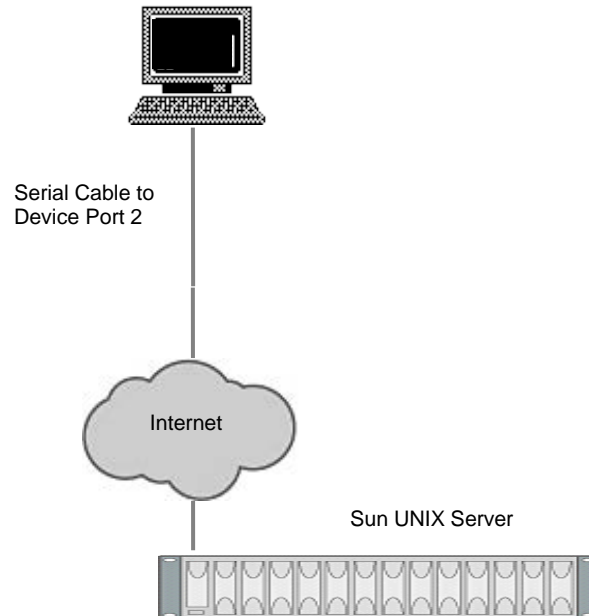
```
[SLB]> connect direct deviceport 2
SunOS 5.7

login: frank
Password:
Last login: Wed Jul 14 16:07:49 from computer
Sun Microsystems Inc. SunOS 5.7 Generic 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 branch office manager. 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 [10: Connections](#) for more information).



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
Remote IP: negotiate       Flow Control: xon/xoff IP: <none>
Authentication: PAP        Logins: disabled
CHAP Host: <none>          Break Sequence: \xlbB
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    PC Card 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, pccard, 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:

<code>&lt;parameter name&gt; &lt;aa   bb&gt;</code>	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.
<code>&lt;parameter name&gt; &lt;Value&gt;</code>	User must specify an appropriate value, for example, an IP address. The parameter values are in mixed case. Square brackets [ ] indicate optional parameters.

Table 14-1. Actions and Category Options

Action	Category
set	network   ipfilter   routing   datetime   ntp   services   nfs   cifs   menu   auth   hostlist   localusers   remoteusers   ldap   radius   kerberos   tacacs+   consoleport   deviceport   nis   slcnetwork   command   sshkey   password   history   cli   locallog   power
show	network   ipfilter   routing   datetime   ntp   services   nfs   cifs   menu   auth   hostlist   localusers   nis   ldap   radius   kerberos   tacacs+   consoleport   deviceport   locallog   sysstatus   syslog   auditlog   portstatus   sysconfig   portcounters   connections   slcnetwork   sshkey   history   cli   user   remoteusers   power
connect	direct   listen   bidirection   unidirection   terminate
diag	ping   loopback   traceroute   arp   lookup   netstat   perfstat   sendpacket   nettrace   internals
pccard	storage   modem
admin	reboot   shutdown   ftp   config   firmware   version   banner   keypad   quicksetup   web   events   lcd
logout	Terminates CLI session.

## 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.

## Administrative Commands

### `admin banner login`

#### Syntax

```
admin banner login <Banner Text>
```

#### Description

Configures the banner displayed after the user logs in.

**Note:** To go to the next line, type `\n` and press **Enter**.

### `admin banner logout`

#### Syntax

```
admin banner logout <Banner Text>
```

#### Description

Configures the banner displayed after the user logs out.

**Note:** To go to the next line, type `\n` and press **Enter**.

### `admin banner show`

#### Syntax

```
admin banner show
```

#### Description

Displays the welcome, login, and logout banners.

### `admin banner welcome`

#### Syntax

```
admin banner welcome <Banner Text>
```

#### Description

Configures the banner displayed before the user logs in.

**Note:** To go to the next line, type `\n` and press **Enter**.

**admin config delete****Syntax**

```
admin config delete <Config Name> location <default|cifs|pccard>
[pccardslot <upper|lower>]
```

**Description**

Deletes a configuration.

**admin config factorydefaults****Syntax**

```
admin config factorydefaults [savesshkeys <enable|disable>]
[savesSLBert <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	lu - Local Users
sv - Services	dp - Device Ports
dt - Date/Time	pc - PC Card
po - Power Outlets	

**Description**

Restores the SLB branch office manager to factory default settings.

**admin config restore****Syntax**

```
admin config restore <Config Name> location
<default|ftp|sftp|nfs|cifs|pccard> [nfsdir <NFS Mounted Dir>]
[pccardslot <upper|lower>] [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	lu - Local Users
sv - Services	dp - Device Ports
dt - Date/Time	pc - PC Card
po - Power Outlets	

**Description**

Restores a saved configuration to the SLB device.

**admin config save****Syntax**

```
admin config save <Config Name> location
<default|ftp|sftp|nfs|cifs|pccard> [nfsdir <NFS Mounted Dir>]
[pccardslot <upper|lower>]
```

**Description**

Saves the current SLB configuration to a selected location.

**admin config show**

**Syntax**

```
admin config show <default|ftp|sftp|nfs|cifs|pccard> [nfsdir <NFS Mounted Dir>] [pccardslot <upper|lower>]
```

**Description**

Lists the configurations saved to a location.

**admin firmware bootbank**

**Syntax**

```
admin firmware bootbank <1|2>
```

**Description**

Sets the boot bank to be used at the next SLB reboot. Applies to dual-boot SLB branch office managers only.

**admin firmware copybank**

**Syntax**

```
admin firmware copybank
```

**Description**

Copies the boot bank from the currently booted bank to the alternate bank (for dual-boot SLB devices).

**admin firmware show**

**Syntax**

```
admin firmware show [viewlog <enable|disable>]
```

**Description**

Lists the current firmware revision, the boot bank status (for dual-boot SLB branch office managers), and optionally displays the log containing details about firmware updates.

**admin firmware update**

**Syntax**

```
admin firmware update <ftp|tftp|sftp|> file <Firmware File> key <Checksum Key>
```

**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 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.

**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 device 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 quicksetup**

**Syntax**

admin quicksetup

**Description**

Runs the quick setup script.

**admin reboot**

**Syntax**

admin reboot

**Description**

Reboots the SLB branch office manager.

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 device, 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 branch office manager. This command is not available on the Web page.

**admin version**

**Syntax**

admin version

**Description**

Displays current hardware and firmware information.

**admin web certificate****Syntax**

```
admin web certificate import via <sftp|scp> certfile <Certificate File>
    privfile <Private Key File> host <IP Address or Name>
    login <User Login> [path <Path to Files>]
```

**Description**

Imports an SSL certificate.

**admin web certificate reset****Syntax**

```
admin web certificate reset
```

**Description**

Resets a web certificate.

**admin web certificate show****Syntax**

```
admin web certificate show
```

**Description**

Displays a web certificate.

**admin web gadget****Syntax**

```
admin web gadget <enable|disable>
```

**Description**

Enables or disables iGoogle Gadget web content.

**admin web timeout****Syntax**

```
admin web timeout <disable|5-120>
```

**Description**

Configures the timeout for web sessions.

**admin web terminate****Syntax**

```
admin web terminate <Session ID>
```

**Description**

Terminates a web session.

**admin web show****Syntax**

```
admin web show
```

**Description**

Displays the current sessions and their ID.

Add 'admin web certificate' commands

## 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.

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**

```
accessoutlets <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 228 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 branch office manager to use Kerberos to authenticate users who log in via the Web, SSH, Telnet, or the console port.

```
show kerberos
```

### Syntax

```
show kerberos
```

### Description

Displays Kerberos settings.

## LDAP Commands

```
set ldap
```

### Syntax

```
set ldap <one or more parameters>
```

### Parameters

```
accessoutlets <Outlet List>
```

```
adsupport <enable|disable>
```

```
base <LDAP Base>
```

```
bindname <Bind Name>
```

```
bindpassword <Bind Password>
```

```
clearports <Port List>
```

```
custommenu <Menu Name>
```

```
dataports <Port List>
```

```
breakseq <1-10 Chars>
```

```
escapeseq <1-10 Chars>
```

```
encrypt <enable|disable>
```

```
group <default|power|admin>
```

```
listenports <Port List>
```

```
permissions <Permission List>
```

```
port <TCP Port>
```

```
server <IP Address or Hostname>
```

```
state <enable|disable>
```

Default is **389**.

**Note:** See [User Permissions Commands](#) on page 228 for information on groups and user rights.

### Description

Configures the SLB device to use LDAP to authenticate users who log in via the Web, SSH, Telnet, or the console port.

**show ldap****Description**

Displays LDAP settings:

**Syntax**

```
show ldap
```

## Local Users Commands

**set localusers add|edit****Syntax**

```
set localusers add|edit <User Login> <one or more parameters>
```

**Parameters**

accessoutlets <Outlet List>

allowdialback <enable|**disable**>

breakseq <1-10 Chars>

changenextlogin <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>

passwordexpires <enable|disable>

permissions <Permission List>

**Note:** See [User Permissions Commands](#) on page 228 for information on groups and user rights.

**Description**

Configures local accounts (including sysadmin) who log in to the SLB branch office manager by means of the Web, SSH, Telnet, or the console port.

**set localusers allowreuse****Syntax**

```
set localusers allowreuse <enable|disable>
```

**Description**

Sets whether a login password can be reused.

**set local users complexpasswords****Syntax**

```
set localusers complexpasswords <enable|disable>
```

**Description**

Sets whether a complex login password is required.

**set localusers state****Syntax**

```
set localusers state <enable|disable>
```

**Description**

Enables or disables authentication of local users.

**set localusers delete****Syntax**

```
set localusers delete <User Login>
```

**Description**

Deletes a local user.

**set localusers lifetime****Syntax**

```
set localusers lifetime <Number of Days>
```

**Description**

Sets the number of days the login password may be used. The default is 90 days.

**set localusers maxloginattempts****Syntax**

```
set localusers maxloginattempts <Number of Logins>
```

**Description**

Sets the maximum number of login attempts before the account is locked. Disabled by default.



**set localusers password****Syntax**

```
set localusers password <User Login>
```

**Description**

Sets a login password for the local user.

**set localusers periodlockout****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.

**set localusers periodwarning****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.

**set localusers reusehistory****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.

**set localusers state****Syntax**

```
set localusers state <enable|disable>
```

**Description**

Enables or disables authentication of local users.

**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 228 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 device to use NIS to authenticate users who log in via the Web, SSH, Telnet, or the console port.

### 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 228 for information on groups and user rights.

```
timeout <enable|1-30>
```

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.

### show radius

#### Syntax

```
show radius
```

#### Description

Displays RADIUS settings.

## TACACS+ Commands

### set tacacs+

#### Syntax

```
set tacacs+ <one or more parameters>
```

#### Parameters

```
accessoutlets <Outlet List>
```

```
clearports <Port List>
```

```
custommenu <Menu Name>
```

```
dataports <Port List>
```

```
encrypt <enable|disable>
```

```
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 228 for information on groups and user rights.

```
secret <TACACS+ Secret>
```

```
server1 <IP Address or Name>
```

```
server2 <IP Address or Name>
```

```
server3 <IP Address or Name>
```

```
state <enable|disable>
```

#### Description

Configures the SLB branch office manager to use TACACS+ to authenticate users who log in via the Web, SSH, Telnet, or the console port.

### 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 local users unlock <User Login>
```

**Description**

Blocks (locks) a user's ability to login.

```
set localusers unlock
```

**Syntax**

```
set local users 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,
  pc, 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>
```

```
group <default|power|admin>
```

```
permissions <Permissions List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, pc, 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

**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, pc, 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>
```

**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
```

**Syntax**

```
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

```
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>
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 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

```
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**

```
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**

```
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>]
```

#### 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.

## 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>
```

```
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.

## 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.

```
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 *power manager* uses to restart itself.

```
slp outletcontrol state <on|off|cyclepower> [outlet <Outlet #>][tower <A|B>]
```

Outlet # is 1-8 for SLP8 power manager and 1-16 for SLP16 power manager. 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 power manager.

```
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 lowest 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 and Sensorsoft devices.

## Device Port Commands

```
set deviceport port
```

### Syntax

```
set deviceport port <Device Port List or Name> <one or more device port parameters>
```

**Example:** set deviceport port 2-5,6,12,15-16 baud 2400

### Parameters

```
auth <pap|chap>
```

```
banner <Banner Text>
```

```
baud <300-115200>
```

```
breakseq <1-10 Chars>
```

---

```

calleridcmd <Modem Command String>
calleridlogging <enable| disable>
chaphost <CHAP Host or User Name>
chapsecret <CHAP Secret or User Password>
The user defines the secret.
checkdsr <enable|disable>
closedsr <enable|disable>
databits <7|8>
device <none|slp8|slp16>
dialbacknumber <username|Phone Number>
dialoutlogin <User Login>
dialoutnumber <Phone Number>
dialoutpassword <Password>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
dodchapsecret <CHAP Secret or User Password>
flowcontrol <none|xon/xoff|rts/cts>
gsmautodns <enable|disable>
gsmbearerservice <GSM Bearer Service>
gsmcompression <enable|disable>
gsmcontext <GPRS Context Id>
gsmdialoutmode <gprs|gsm>
gsmpin <GSM/GPRS PIN Number>
initscript <Initialization Script>
A script that initializes a modem.
Note: We recommend preceding the initscript with AT and include E1 V1 x4 Q0 so that the SLB
branch office manager may properly control the modem.
ipaddr <IP Address>
localipaddr <negotiate|IP Address>
logins <enable|disable>
modemmode <text|ppp>
modemstate <disable|dialout|dialin|dialback|dialondemand|
dialin+dialondemand>
modemtimeout <disable|1-9999 seconds>
name <Port Name>
nat <enable|disable>
parity <none|odd|even>

```



```
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
slp infeedstatus
Displays the infeed status and load of the SLP power manager.
ssshauth <enable|disable>
sshin <enable|disable>
sshport <TCP Port>
stopbits <1|2>
telnetauth <enable|disable>
telnetin <enable|disable>
telnetport <TCP Port>
timeoutlogins <disable or 1-30>
webcolumns <Web SSH/Telnet Cols>
webrows <Web SSH/Telnet Rows>
```

### Description

Configures a single port or a group of ports.

### **set deviceport global**

#### Syntax

```
set deviceport global <one or more parameters>
```

#### Parameters

```
sshport <TCP Port>
telnetport <TCP Port>
tcpport <TCP Port>
maxdirect <1-10>
```

### Description

Configures settings for all or a group of device ports.

### **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 branch office manager.

**Note:** This command is available in the CLI but not the web.

**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.

**diag nettrace****Syntax**

```
diag nettrace <one or more parameters>
```

**Parameters**

```
ethport <1|2>
```

```
host <IP Address or Name>
```

```
numpackets <Number of Packets>
```

```
protocol <tcp|udp|icmp>
```

```
verbose <enable|disable>
```

**Description**

Displays all network traffic, applying optional filters. This command is not available on the web page.

**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 branch office manager. 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.

## diag traceroute

### Syntax

```
diag traceroute <IP Address or Hostname>
```

### Description

Displays the route that packets take to get to a network host:

## 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 power manager.

```
slp outletcontrol state <on|off|cyclepower> [outlet <Outlet #>]
```

Outlet # is 1-8 for SLP8 power manager and 1-16 for SLP16 power manager. 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 power manager uses to restart itself.

```
slp system
```

Displays system information for the SLP power manager.

### 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 power manager.

## Events Commands

### **admin events add**

#### **Syntax**

```
admin events add <receivetraps> <response>
```

<response> is one of:

```
action <fwdalltrapseth|fwdseltrapeth> ethport <1|2> nms <SNMP NMS> community <SNMP Community> [oid <SNMP OID>]
```

```
action <fwdalltrapsmodem|fwdseltrapmodem> deviceport <Device Port # or Name> nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
```

```
action <fwdalltrapsmodem|fwdseltrapmodem> pccardslot <upper|lower> 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>
```

```
pccardslot <upper|lower>
```

#### **Description**

Edits event definitions.

**admin events show**

### Syntax

admin events show

### Description

Displays event definitions.

## 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
```

**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>  
pccardslot <upper|lower> state <disable>  
pccardslot <upper|lower> 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**

```
emaildelay <Email Delay>
emaillogging <disable|bytecnt|charstr>
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>
pccardlogging <enable|disable>
pccardmaxfiles <Max # of Files>
pccardmaxsize <Size in Bytes>
pccardslot <upper|lower>
```



```
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 [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 [11: User Authentication](#)).

## Network Commands

```
set network
```

### Syntax

```
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.

**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|gprs|default>  
alternate <IP Address>  
pingip <IP Address>  
ethport <1 or 2>  
pingdelay <1-250 seconds>  
failedpings <1-250>
```

**Description**

Sets default and alternate gateways. The alternate gateway is used if an IP address usually accessible through the default gateway fails to return one or more pings.

**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>]
```

**Description**

Configures Ethernet port 1 or 2.

**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 branch office manager.

**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 <one or more parameters>

**Parameters**

locdir <Directory>

```
mount <enable|disable>
remdir <Remote NFS Directory>
rw <enable|disable>
Enables or disables read/write access to remote directory.
```

### 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.

```
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.

**Note:** 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`).

```
show cifs
```

### Syntax

```
show cifs
```

### Description

Displays SMB/CIFS settings.

**show nfs**

**Syntax**

show nfs

**Description**

Displays NFS share settings.

## PC Card Storage Commands

**pccard storage dir**

**Syntax**

pccard storage dir <upper|lower>

**Description**

Views a directory listing of a Compact Flash card.

**pccard storage format**

**Syntax**

pccard storage format <upper|lower> [filesystem <ext2|fat>]

**Description**

Formats a Compact Flash card.

**pccard storage mount**

**Syntax**

pccard storage mount <upper|lower>

**Description**

Mounts a Compact Flash card in the SLB device for use as a storage device.

The Compact Flash card must be formatted with an ext2 or FAT file system before you mount it.

**pccard storage unmount**

**Syntax**

pccard storage unmount <upper|lower>

**Description**

Unmounts a Compact Flash card. Enter this command before ejecting the card.

## PC Card Modem Commands

### pccard modem

#### Syntax

pccard modem <upper|lower> <parameters>

#### Parameters

auth <**pap**|chap>

baud <300-115200>

**9600** is the default.

calleridcmd <Modem Command String>

calleridlogging <enable| **disable**>

chaphost <CHAP Host or User Password>

chapsecret <CHAP Secret or User Password>

databits <7|**8**>

dialbacknumber <username|Phone Number>

dialoutlogin <User Login>

dialoutnumber <Phone Number>

dodauth <pap|chap>

dodchaphost <CHAP Host or User Name>

dodchapsecret <CHAP Secret or User Password>

dialoutpassword <Password>

flowcontrol <**none**|xon/xoff|rts|cts>

gsmautodns <**enable**|disable>

gsmbearerservice <GSM Bearer Service>

gsmcompression <enable|**disable**>

gsmcontext <GPRS Context Id>

gsmdialoutmode <**gprs**|gsm>

gsmpin <GSM/GPRS PIN Number>

initscript <Initialization Script>

isdnchannel <1|2>

isdnumber <Phone Number>

localipaddr <negotiate|IP Address>

modemmode <**text**|ppp>

modemstate <**disable**|dialout|dialin|dialback|dialondemand|  
dialin+dialondemand>

modemtimeout <disable|1-9999 seconds>

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>

```

**Description**

Configures a currently loaded PC Card.

**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>
wakeuptime <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.

## Routing Commands

**set routing****Syntax**

```
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**

```
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.



## Services Commands

### set services

#### Syntax

```
set services <one or more services parameters>
```

#### Parameters

```
alarmdelay <1-6000 Seconds>
```

```
auditlog <enable|disable>
```

```
auditsize <Size in Kbytes>
```

Limit is 1-500 Kbytes

```
authlog <off|error|warning|info|debug>
```

```
clicommands <enable|disable>
```

```
contact <Admin contact info>
```

```
devlog <off|error|warning|info|debug>
```

```
diaglog <off|error|warning|info|debug>
```

```
genlog <off|error|warning|info|debug>
```

```
includesyslog <enable|disable>
```

```
location <Physical Location>
```

```
netlog <off|error|warning|info|debug>
```

```
nms <IP Address or Name>
```

```
phonehome <enable|disable>
```

```
phoneip <IP Address>
```

```
portssh <TCP Port>
```

```
rocommunity <Read-Only Community Name>
```

```
rwcommunity <Read-Write Community Name>
```

Sets a password for an SNMP manager to access the read-only data the SLB SNMP agent provides and to modify data where permitted.

```
servlog <off|error|warning|info|debug>
```

```
smtserver <IP Address or Hostname>
```

```
snmp <enable|disable>
```

```
ssh <enable|disable>
```

```
syslogserver1 <IP Address or Name>
```

```
syslogserver2 <IP Address or Name>
```

```
telnet <enable|disable>
```

```
timeoutssh <disable or 1-30>
```

```
timeouttelnet <disable or 1-30>
```

```
traps <enable|disable>
```

```

trapcommunity <Trap Community>
vlssh <enable|disable>
v3password <Password for v3 auth>
v3user <User for v3 auth>
v3user <V3 RO User>
v3password <V3 RO User Password>
v3phrase <V3 RO User Passphrase>
v3rwuser <V3 RW User>
v3rwpassword <V3 RW User Password>
v3rwphrase <V3 RW User Passphrase>
v3security <noauth|auth|authencrypt>
v3auth <md5|sha>
v3encrypt <des|aes>
webssh <enable|disable>
webtelnet <enable|disable>

```

**Description**

Configures services (system logging, SSH and Telnet access, SSH and Telnet timeout, SNMP agent, email (SMTP) server, and audit log):

```
show services
```

**Syntax**

```
show services
```

**Description**

Displays current services.

## SLB 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 SLB devices 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|coppaste> [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|coppaste> <one or more parameters>
```

**Parameters**

[format <openssh|secsh>]

[host <IP Address or Name>]

[login <User Login>]

```
[path <Path to Copy Key>]
bits <512|1024>
keyname <SSH Key Name>
keyuser <SSH Key User>
type <rsa|dsa>
```

### Description

Exports an sshkey.

```
set sshkey import
set sshkey import <ftp|scp> <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 <rsa1|rsa|dsa> 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|rsa1|rsa|dsa>]
```

### 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**

show connections connid <Connection ID> [email <Email Address>].

**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**

```
show syslog [<parameters>]
```

**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**

```
show syslog clear <all|netlog|servlog|authlog|devlog|diaglog|genlog>
```

**Description**

Clears one or all of the system logs.

## A: Bootloader

The SLM management appliance provides a bootload command interface. This interface is only accessible through the SLB branch office manager's console port.

### Accessing the Bootloader

#### To access the bootloader CLI:

To access the bootloader command line interface

1. Power up the SLB branch office manager.
2. Type **x15** within 10 seconds of power up. The bootloader halts the boot procedure and displays a **Lantronix** command prompt.

### Bootload Commands

#### User Commands

`help`

Lists and prints the command list and online help.

`?`

An alias for `help`.

`boot`

Boot default (runs `bootcmd`).

`bootcheck`

Checks boot bank information.

`bootinfo`

Displays boot bank information.

`bootset 1|2`

Selects boot bank 1 or boot bank 2.

`IDE`

Accesses the IDE sub-system.

`mtest`

Performs a simple test of the RAM.

`su cust|admin`

Switches to another user: from `cust` (customer) to `adm` (administrator) and vice versa.

`version`

Prints the bootloader version.

`whoami`



Displays information about the current user.

## Administrator Commands

In addition to the commands that the user can issue, the administrator can issue the following commands:

`imagecopy`

Copies an image of the drive from the lower PCMCIA device to the internal CF card.

`passwd`

Provides a new password for user `admin`. The default password for user `admin` is `admin`. User `cust` does not have a password.

`ping`

Sends a ping request to the network host.

`printenv`

Prints bootloader variables.

`setenv`

Sets environment variables.

## 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 device, 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 branch office manager may be secure, but the path from the SLB device to the end device may not be secure.
- ◆ With the right tools, a person having physical access to open the SLB branch office manager 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 device will attempt to service all requests and will not filter out potential denial-of-service attacks.

## C: Safety Information

### 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 branch office manager.
- ◆ Install the SLB device near an AC outlet that is easily accessible.
- ◆ Always connect any equipment used with the product to properly wired and grounded power sources.
- ◆ 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

- ◆ This SLB branch office manager may have more than one power supply source. Disconnect all power supply sources before servicing to avoid electric shock.
- ◆ Check nameplate ratings to assure there is no overloading of supply circuits that could affect over current protection and supply wiring.

#### Grounding

- ◆ Maintain reliable grounding of this product.
- ◆ Pay particular attention to supply connections when connecting to power strips, rather than directly to the branch circuit.
- ◆ Install DC-rated equipment only under the following conditions:
  - Connect the equipment to a DC supply source that is electrically isolated from the AC source and reliably connected to ground, or connect it to a DC (SELV) source.

- Install only in restricted access areas (dedicated equipment rooms, equipment closets or the like) in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
- Route and secure input wiring to terminal block in such a manner that it is protected from damage and stress. Do not route wiring past sharp edges or moving parts.
- Incorporate a readily accessible disconnect device, with a 3 mm minimum contact gap, in the fixed wiring.
- Provide a listed circuit breaker suitable for protection of the branch circuit wiring and rated 60 VDC minimum.

### Fuses

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

### Rack

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

- ◆ Do **not** install the SLB branch office manager 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 (T<sub>ma</sub>) inside the rack may be greater than the room ambient temperature. Make sure to install the SLB device in an environment with an ambient temperature less than the maximum operating temperature of the SLB branch office manager. (See [Technical Specifications](#) on page 23.)
- ◆ 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 device, make sure the SLB branch office manager 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).

## D: Adapters and Pinouts

The serial device ports of the SLB branch office manager products match the RJ45 pinouts of the console ports of many popular devices found in a network environment. The SLB device 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 branch office manager 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.

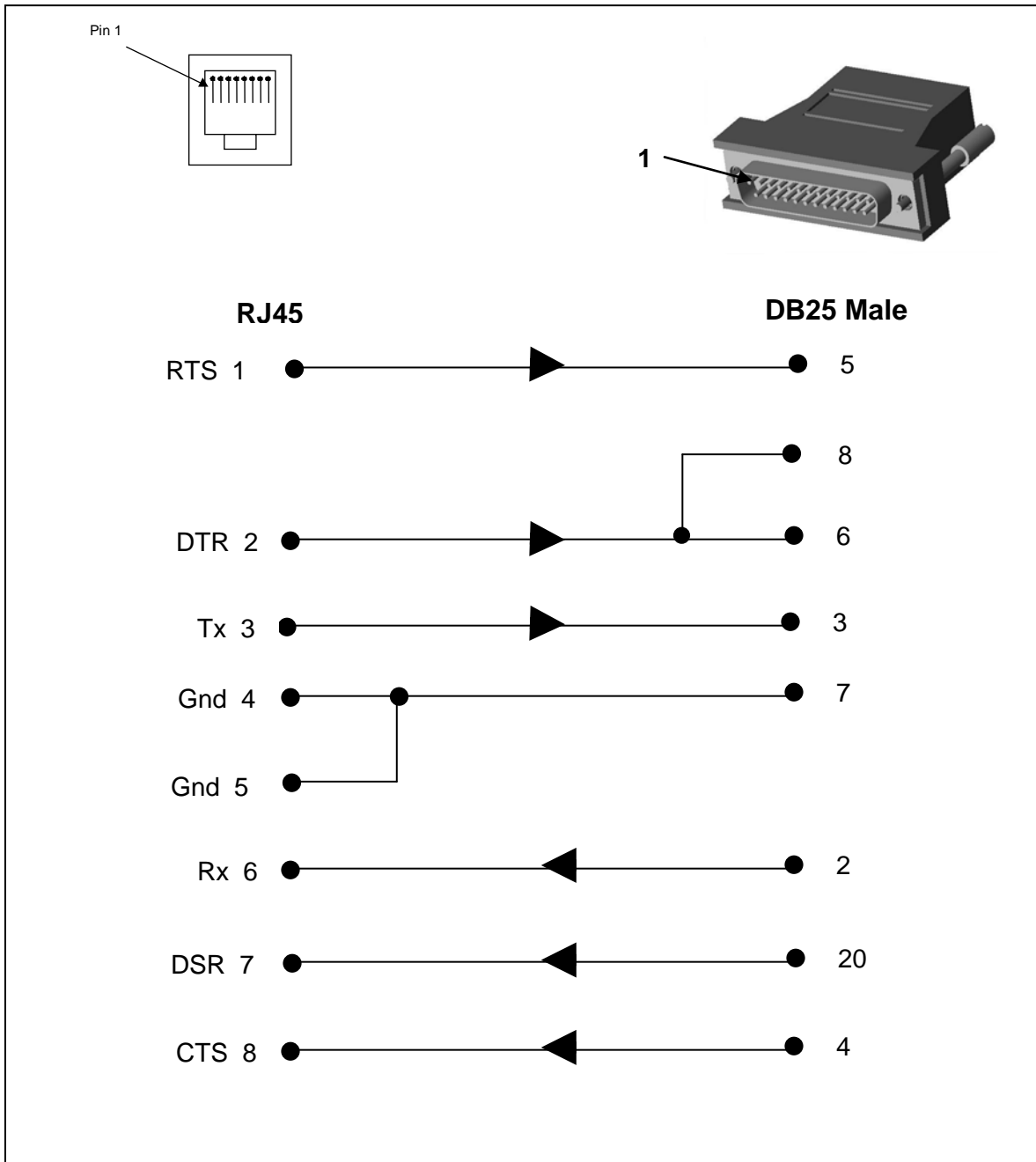
Please check the cabling database on the Lantronix website at <http://www.lantronix.com> for suggested cables and adapters for commonly used serial devices.

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 pushbuttons on the front panel, the Console Port web page, or the command line interface **show console port** and **set consoleport** commands.

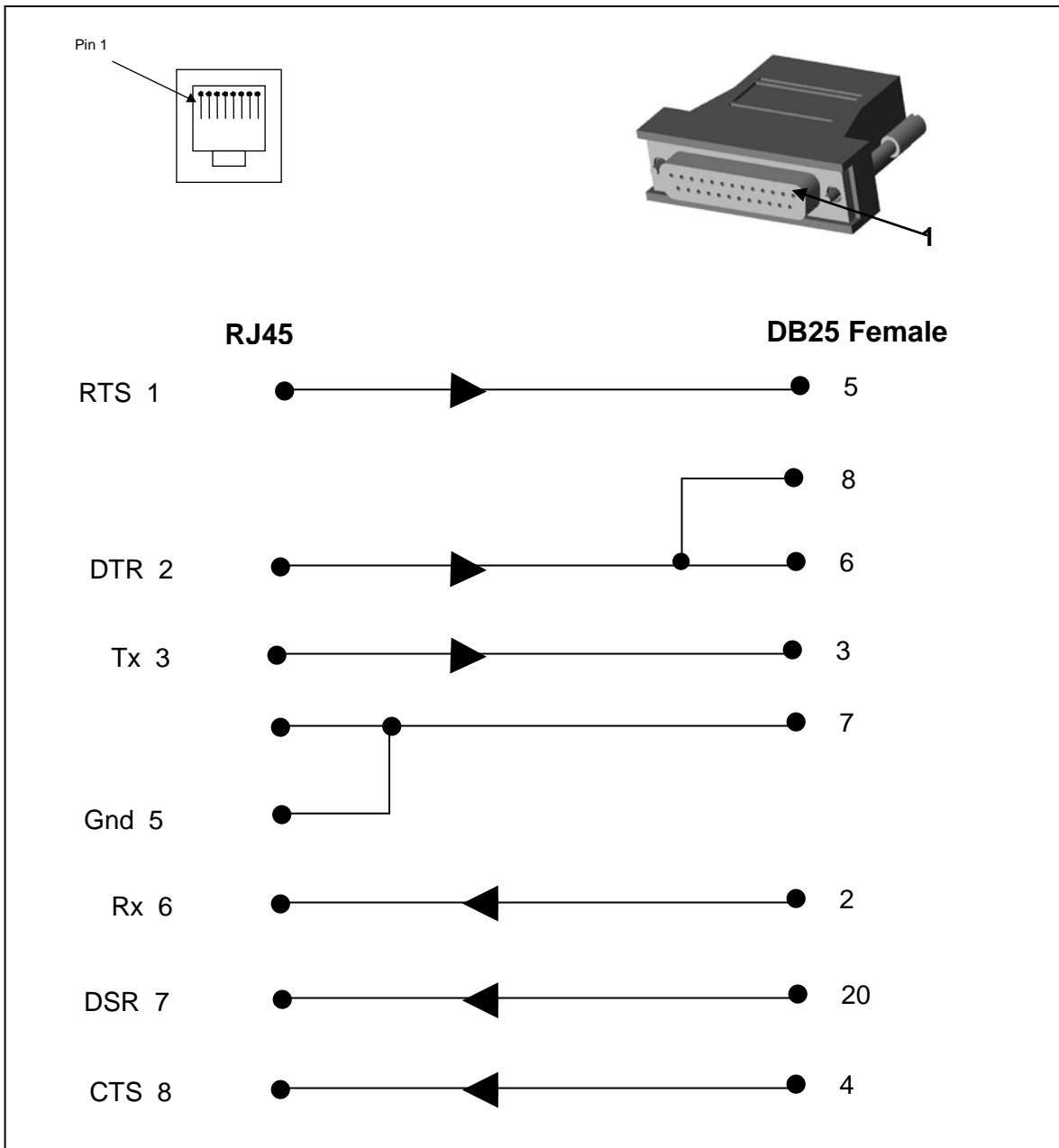
The adapters illustrated below are compatible with the Lantronix SLB models.

**RJ45 Receptacle to DB25M DCE Adapter for the SLB Device (PN 200.2066A)**

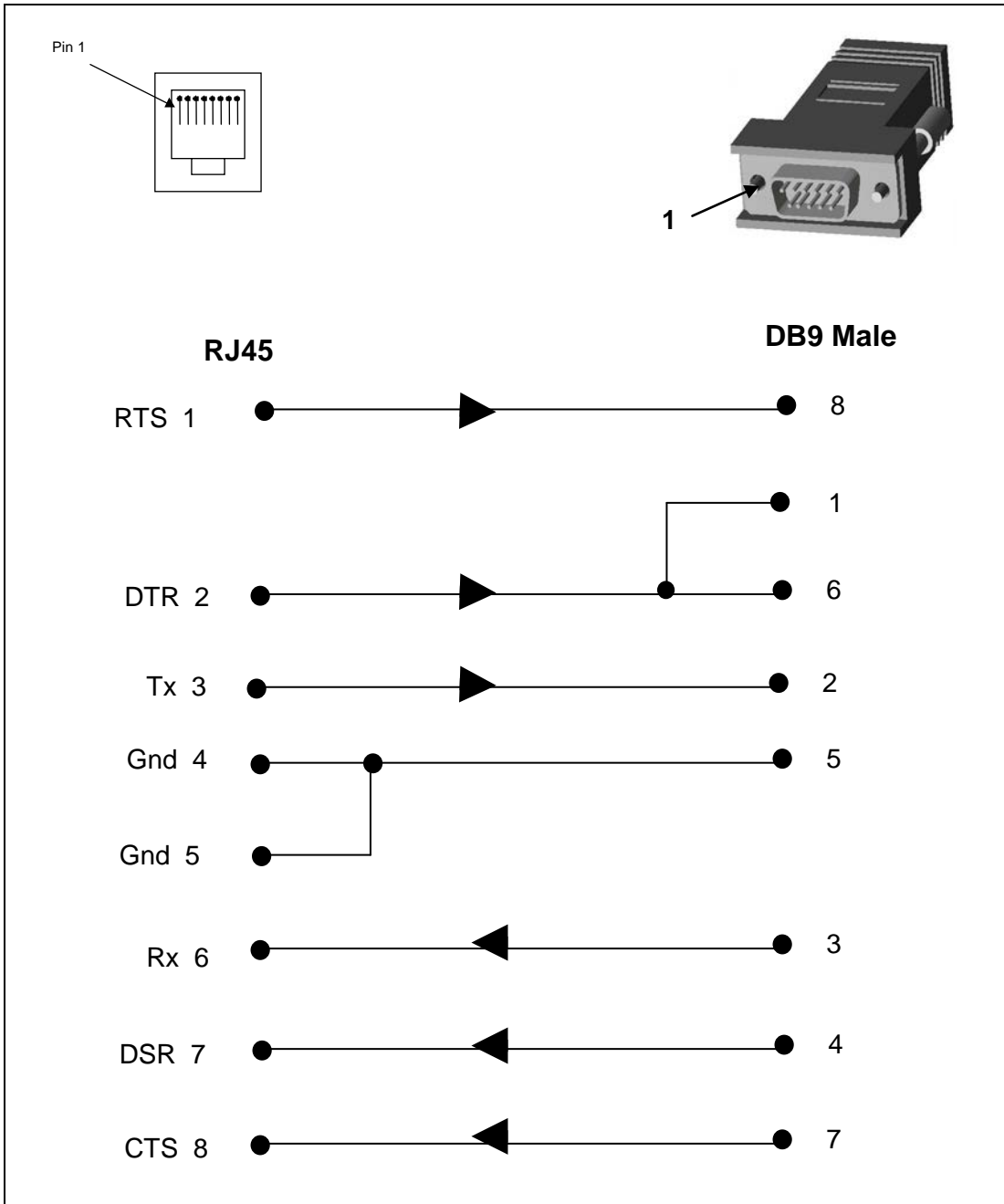


Use PN 200.2066A adapter with a dumb terminal or with many SUN applications.

RJ45 Receptacle to DB25F DCE Adapter for the SLB Device (PN 200.2067A)

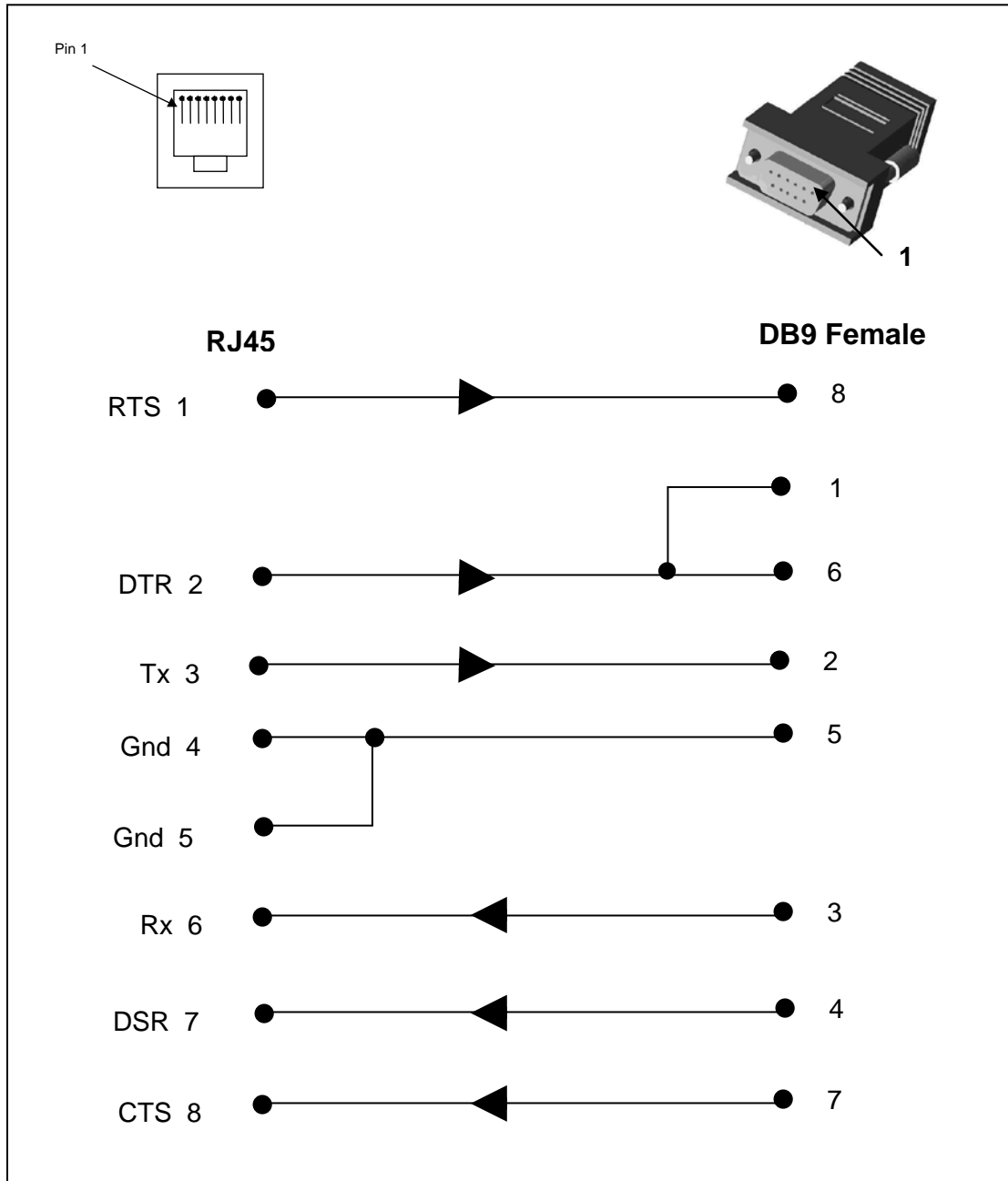


RJ45 Receptacle to DB9M DCE Adapter for the SLB Device (PN 200.2069A)





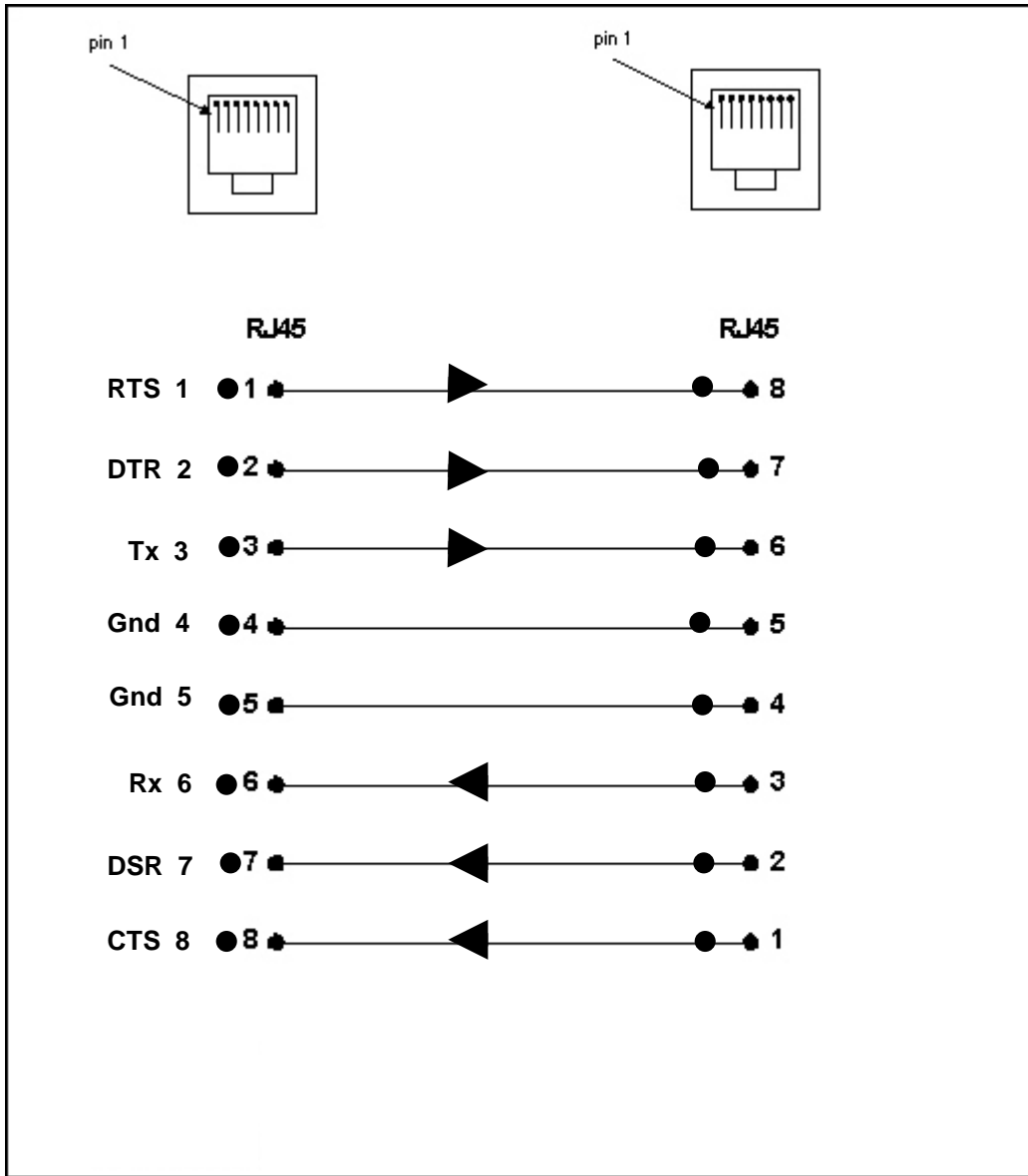
**RJ45 Receptacle to DB9F DCE Adapter for the SLB Device (PN 200.2070A)**



Use PN 200.2070A adapter with a PC's serial port.

**RJ45 to RJ45 Adapter for Netra/Sun/Cisco and SLP Device (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 the SLP power manager, Netra/SUN/CISCO, and others.

## **E: 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.

### **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.

## ***F: Compliance Information***

### **Manufacturer's Name & Address:**

Lantronix, Inc., 167 Technology Drive, Irvine, CA 92618 USA

### ***Declares that the following product:***

Product Name(s): **SLB Branch Office Manager (SLB Series)**

### ***Conforms to the following standards or other normative documents:***

#### **SAFETY:**

- UL 60950-1
- CAN/CSA-C22.2 No. 60950-1-03
- EN 60950-1 (2001), Low Voltage Directive (73/23/EEC)

### **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.

### **CE NOTICE (European Union Only)**

Marking by the symbol  indicates compliance of this information technology device to the EMC Directive and the Low Voltage Directive of the European Union. Such marking is indicative that this system meets the following technical standards:

- EN 55022 — “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment.”
- EN 55024 — “Information technology equipment - Immunity characteristics - Limits and methods of measurement.”
- EN 61000-3-2 — “Electromagnetic compatibility (EMC) - Part 3: Limits - Section 2: Limits for harmonic current emissions (Equipment input current up to and including 16 A per phase).”
- EN 61000-3-3 — “Electromagnetic compatibility (EMC) - Part 3: Limits - Section 3: Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current up to and including 16 A.”
- EN 60950 — “Safety of Information Technology Equipment.”

### **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
- NIST-certified implementation of AES as specified by FIPS 197 (uses SLC-SSH algorithm)

**RoHS Notice:**

All Lantronix products in the following families are China RoHS-compliant and free of the following hazardous substances and elements:

- Lead (Pb)
- Mercury (Hg)
- Polybrominated biphenyls (PBB)
- Cadmium (Cd)
- Hexavalent Chromium (Cr (VI))
- Polybrominated diphenyl ethers (PBDE)

Product Family Name	Toxic or hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr (VI))	Polybrominated biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
UDS1100 and 2100	0	0	0	0	0	0
EDS	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
XPress DR & XPress-DR+	0	0	0	0	0	0
SecureBox 1101	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
UBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
SLC	0	0	0	0	0	0
XPort	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLP	0	0	0	0	0	0
SCS	0	0	0	0	0	0
SLS	0	0	0	0	0	0

O: toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

X: toxic or hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T11363-2006.

**Manufacturer's Contact:**

Lantronix Inc.

167 Technology Drive

Irvine, CA 92618, USA

Toll Free: 800-526-8766

Phone: 949-453-3990

Fax: 949-453-3995